Chapter 4

Personnel Movement Control

Perimeter barriers, intrusion detection devices and protective lighting provide physical security safeguards; however, they alone are not enough. A positive personnel movement control system must be established and maintained to preclude unauthorized entry, and to facilitate authorized entry at personnel control points. Access lists, personal recognition, security identification cards and badges, badge exchange procedures, and personnel escorts contribute to the effectiveness of movement control systems.

The best control is provided when systems incorporate all these elements. Simple, understandable, and workable identification and movement control procedures should be used to achieve security objectives without impeding efficient operations. Properly organized and administered, a personnel and movement control system provides a means not only of positively identifying those who have the right and need to enter or leave an area, but also of detecting unauthorized personnel who attempt to gain entry.

Identification of Personnel — Section I

4-1 Purpose of Movement Control and Identification

a. Prevent introduction of harmful devices, materiel, or components.

b. Prevent misappropriation, pilferage, or compromise of materiel or recorded information by means of:

- Package
- Materiel
- Property Movement Control.

c. This prevention is accomplished through:

(1) Initially determining who has a valid requirement to be in an area.

(2) Limiting access to those persons who have that valid requirement.

(3) Establishing procedures for positive identification of persons within, and of persons authorized access into, areas.

(4) Issuing special identification cards or badges to personnel authorized access into restricted areas.

(5) Using access lists.

(6) Using identification codes.

(7) Using duress codes

4-2 Employee Screening

a. Screening job applicants and employees to eliminate potential espionage and sabotage agents and other security risks is important in peacetime and is extremely important in time of a national defense emergency. For such screening to be most effective, it should be incorporated into standard personnel policies for peacetime as well as for times of emergency.

b. Personnel Security Survey Questionnaire. The use of a personnel security questionnaire is essential in the investigation of both applicants and employees. The security questionnaire should be screened for completeness and, in the case of applicants, obvious undesirables eliminated from further consideration. A careful investigation should be conducted to assure that the applicant's or employee's character, associations, and suitability for employment are satisfactory.

c. Sources of Data. The following

sources may be helpful in securing employment investigative data:

(1) State and local police, to include national and local police in overseas areas.

(2) Former employers.

(3) References (including those not furnished by applicant or employee. These are known as throw-offs, and their names are obtained during interviews of references furnished by applicants or employees).

(4) Public records.

(5) Credit agencies.

(6) Schools (all levels).

(7) Others as appropriate. (These may include the FBI, the US Army Criminal Records Repository, etc.). In requesting investigative data from any of the above sources, enough information should be furnished to properly identify the applicant or employee and avoid error in identity.

4-3 Identification System

a. An identification (ID) system should be established at each installation or facility to provide a means of identifying all military personnel, civilian employees, and visitors. The system should provide for the use of security identification cards or badges to aid in control and movement of personnel into, within, and out of specified areas or activities.

b. The standard identification media, DD Form 2A (Military) or DA Form 1602 (Civilian Employee), may be prescribed for personnel by installation or facility commanders as valid identification for access to areas that are basically administrative in nature, contain no security interest, and are not in the restricted area category.

c. Personnel requiring access to restricted areas should be issued a security identification card or badge as prescribed in AR 606-5. The identification card or badge should be designed as simply as possible and still provide for adequate control of the movement of personnel.

d. Provisions for identification by card or badge control at an installation or facility should be included as part of the physical security plan.

4-4 Use of Identification Media

a. Designation of the various areas where media are required.

b. Description of the various types in use plus authorizations and limitations placed upon the holder.

c. Required presentation at times of entering and leaving each area, including nonoperational hours.

d. Details, of where, when, and how worn, displayed, or carried.

e. Procedures to be followed in case of loss or damage.

f. Disposition on termination of employment or as a result of investigations and personnel actions.

g. Prerequisites for reissue.

4-5 Types of Systems

Most Common Identification Systems

□ Single card or badge

□ Card or badge exchange

□ Multiple cards or badges

4-6 Card and Badge System

a. A security identification card or badge system should be established to admit and control the movement of all persons admitted to restricted areas employing 30 or more persons per shift. However, the commander may at his discretion authorize a card or badge system in restricted areas where less than 30 persons per shift are employed.

b. Of the several identification systems used in access control, three of the most commonly used are the **single card or badge system,** the **card or badge exchange system,** and the **multiple card or badge system.** These ID systems may be used either for cards carried on the person or for cards or badges worn on outer clothing.

c. A system may be established (in an appropriate situation) for issuance of identification cards or badges at the main entrance to an installation. Such a system can be used for visitors and similar personnel.

4-7 Single Card or Badge

a. With this system, permission to enter specific areas is shown by letters, numerals, or colors. It has a major limitation-loose control. The opportunity for alteration or duplication is high.

b. This system gives comparatively loose control and is not recommended for security areas. Permission to enter does not always go with the need to know, and the fact that ID cards and badges frequently remain in the bearer's possession during off duty or off post hours gives the opportunity for alteration or duplication.

4-8 Card or Badge Exchange

a. In this system, two items contain identical photographs but different background colors, or one item has an overprint. One is presented at the entrance to a specific area and exchanged for the other, which is carried or worn while in that area. Individual possession upon issuance is only in the area, to **decrease the possibility of forgery or alteration.**

b. This method provides extra security by having both photographs identical. In this type of system, the second badge or card is kept in the security area and never leaves the area.

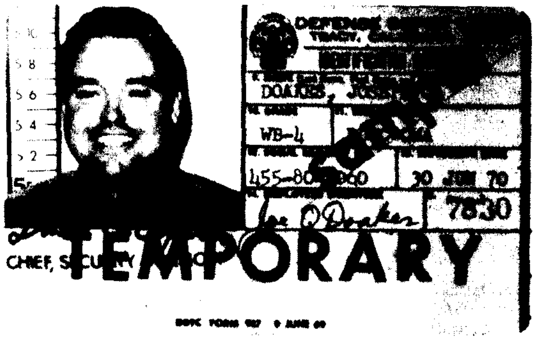
4-9 Multiple Card or Badge

a. Instead of having specific markings on the ID card or badge denoting permission to enter various restricted areas, the multiple card or badge system makes an exchange at the entrance to each security area within the installation. Exchange cards or badges are kept at each area for only those individuals who have the appropriate card or badge. By virtue of the localized and controlled exchange requirements, this is the most secure and effective system.

b. Card and badge data are identical and must be so to allow comparisons.

4-10 Card and Badge Specifications

a. Security ID cards and badges should be of a type of design and construction which will make them, for all practical purposes, tamperproof, and which will meet the requirements of AR 606-5.



DOAKES, JOS

WB-4

455-80 960

30 JUN 70

7830

TEMPORARY

CHIEF, S CU Y

b. Security ID card and badge inserts should be prenumbered to avoid any possibility of reissuing any number. Acquisition, storage, and control of card and badge components and all engraved plates must be accomplisher as prescribed in AR 606-5.

c. Issuance and Accountability:

(1) Identification card or badge issuance, accuntability, and control should be accomplished at a central office, preferably the office of the provost marshal or physical security office, so a minimum of time me elapses between change in the status of a card or badge and noti fication of the security forces.

(2) A duplicate of each issued card or badge and a file on each hearer should be kept including, in addition to the data entered on the card or badge, the bearer's residential address and telephone number.

(3) Why such strict control?

(a) Because any ID card or badge may be altered or reproduced by a person having the time and sufficient skill in printing. engraving and photocopying, the makeup, issuance, and accountability of cards and badges must be fully controlled.

(b) Because control commences with the manufacturer or supplier.

(c) When inserts or complete cards or badges are secured commerically, verification should be made that adequate control is exercised by the supplier. This is especially important when engraving or special paper is concerned.

4-11 Enforcement Measures

The most vulnerable link in any identification system is its enforcement. Perfunctory performance of duty by the security forces in comparing the bearer with the card or badge may weaken or destroy the effects of the most elaborate system. Positive enforcement measures should be prescribed to insure effective operation of the personnel and identification system. These should include, but not be limited to the following:

a. Security personnel designated for duty at entrance control points should be chosen for their alertness, quick perception, tact, and good judgment.

b. Formalized, standard procedures for conducting assemblies, posting, and relief of personnel, and frequent inspection of personnel on post at irregular times are effective means to preclude posting of unqualified personnel and perfunctory performance of duty.

c. A uniform method of handling or wearing security ID cards or badges should be prescribed. If carried on the person, the card must be removed from the wallet or other container and handed to security personnel. A badge should be worn in a con spicuous position to expedite inspection and recognition from a distance.

d. Entrances and exits of restricted areas should be arranged so that arriving and departing personnel arc forced to pass in a single file in front of security personnel. In some instances, the use of turnstiles may be advisable to assist in maintaining positive control of entrance and exit.

e. Artificial lighting at the control points should be arranged so that it illuminates the arriving and departing personnel and should be of sufficient intensity to enable security personnel to compare and identify the bearer with the ID card or badge.

f. Enforcement of access control systems rests primarily on the installation security forces. However, it is essential that they have the full cooperation of the employees, who should be educated and encouraged to assume this security responsibility. Employees should be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where access is limited to particular zones, employees should report movement of individuals to unauthorized zones.

g. Identification card and badge racks or containers used at control points for an exchange system should be positioned so they are accessible only to guard personnel.

h. A responsible custodian should be appointed by competent authority to accomplish control procedures required by AR 606-5 for issue, turn in, recovery, or expiration of security ID cards and badages, The degree of compromise tolerable in the identification system is in direct proportion to the degree of security required or indicated. The following control procedures are recommended for preserving the integrity of a card and badge system:

(1) Maintenance of an accurate written record or log listing, by serial number, all cards and badges, showing those on hand, to whom issued, and disposition (lost, mutilated, or destroyed).

(2) Authentication of records and logs by the custodian.

(3) Periodic inventory of records by a commissioned officer.

(4) Prompt invalidation of lost cards and badges.

(5) Conspicuous posting at security control points of current lists of lost or invalidated cards and badges.

(6) Establishment of controls within re stricted areas to enable security personnel on duty to determine promptly and accurately the number of persons within the area at any time.

(7) Establishment of a two-man rule when required.

(8) Establishment of procedures to control movement of visitors to security areas. A visitor control record should be maintained and located where positive controls can be exercised.

4-12 Visitor Identification And Control

a. Physical security precaution against pilferage, espionage, and sabotage requires screening, identification, and control of visitors. Visitors are generally in the following categories:

(1) Persons with whom every installation or facility must have dealings in connection with the conduct of its business, such as representatives of suppliers, customers, licensers or licensee, insurance inspectors or adjusters, government inspectors (national, state, and local), service industry representatives, contractors, employees, etc.

(2) Individuals or groups who desire to visit an installation or facility for a purpose not essential to, or necessarily in furtherance of, the operations of the installation or facility concerned. Such visits may be desired, for example, by business, educational, technical, or scientific organizations and individuals or groups desiring to further their particular interests.

(3) Individuals or groups specifically sponsored by government agency organizations such as foreign nationals visiting under technical cooperation programs and similar visits by US nationals. Requests for visits by foreign nationals should be processed in accordance with AR 380-25.

(4) Individuals and groups who the government generally encourages but does not specifically sponsor, because of the contribution they make to economic and technical progress or to defense production in the United States and/or in friendly nations.

(5) Guided tour visits to selected portions of installations in the interest of public relations.

(6) Further information concerning requirements and procedures for visits will be found in AR 381-130 and AR 550-50.

b. Arrangements for identification and control of visitors may include the following:

(1) Positive methods of establishing the authority for admission of visitors, as well as any limitations relative to access.

(2) Positive ID of visitors by means of personal recognition, visitor permit, or other identifying credentials. The employee, supervisor or officer in charge should be contacted to ascertain the validity of the visit.

(3) Availability and use of visitor registration forms and records that will provide a record of identity of the visitor, time and duration of his visit, and other pertinent control data.

(4) Availability and use of visitor ID cards or badges. Such identification media should be numbered serially and indicate the following:

(a) Bearer's name.
(b) Area or areas to which access is authorized.
(c) Escort requirements, if any.
(d) Time limit for which issued.
(e) Signature (or facsimile).
(f) Photograph, if desired and available.

(5) Procedures which will insure supporting personal identification in addition to check of visitor cards or badges at restricted area entrances.

(6) Procedures for escorting visitors having limitations relative to access through areas where an uncontrolled visitor, even though conspicuously identified, could acquire information for which he is not authorized. Foreign national visitors should be escorted at all times.

(7) Controls which will recover visitor ID cards or badges on expiration, or when no longer required.

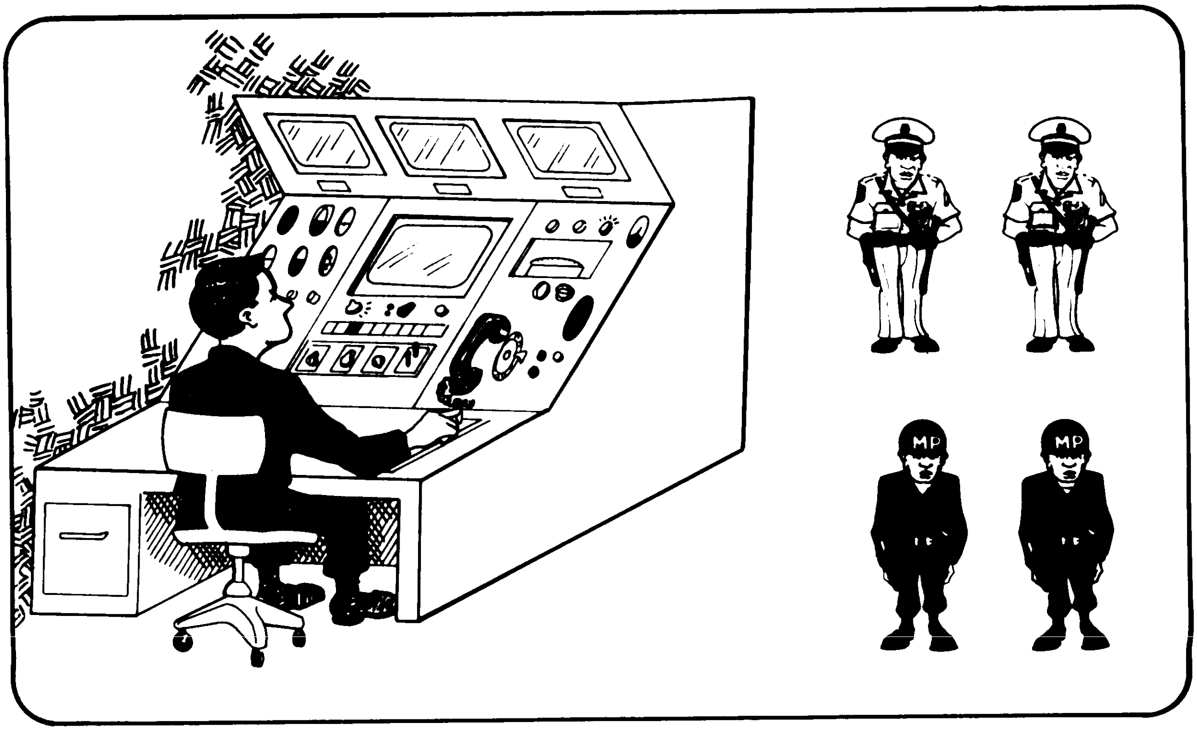
(8) Twenty-four hour advance approval when possible. Where appropriate, the installation should prepare an agenda for the visit and designate an escort officer.

4-13 Sign/Countersign And Codeword

This additional measure to verify identity is primarily used in tactical maneuvers and during Army Training and Evaluation Programs (ARTEP). The sign/countersign or codeword procedure should be checked and tested to insure immediate change if. compromised.

4-14 Duress Code

This is a simple word or phrase used during normal conversation. It alerts other security personnel that an authorized person has been forced to vouch for an unauthorized individual. A viable duress code requires preplanning to insure appropriate response. And it is changed frequently to minimize compromise.



Equipment And/Or Manpower

This system assists in the control of entry and departure of personnel to and from these areas and provides a strict control and identification system within the area.

4-15 Use of Escorts

Escorts must be chosen because of their ability to accomplish tasks properly and effective y and their knowledge of areas to be visited, to include all security requirement.

a. Each should be a representative of the person or activity visited.

b. Escort personnel should be other than military police or civilian guards.

c. Whether or not the escort remains with such visitor during the time he is within the restricted area is determined by local regulations. Personnel listed on the access list may be admitted to restricted areas without escort, depending upon local policy.

4-16 Entry Roster

Admission of unit or installation personnel to restricted areas should be granted only to those positively identified and whose names appear on a properly authenticated roster of all persons authorized by competent authority to enter.

a. Each time a permanent addition or deletion is made, this correction can initially be accomplished by pen and ink.

b. Changes may be published in the same manner as the original roster.

c. Rosters should be maintained at access control points to facilitate positive control and be kept current, verified, authenticated, and accounted for by an individual designated by the commander. Admission of persons other than those on the authorized roster should be subject to specific approval by the installation or facility commander, or his designated representative. Such persons will be escorted or supervised.

4-17 Two-man Rule

a. At least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and who are familiar with applicable safety and security requirements, will be present during any operation that affords access to sensitive weapons.

b. The rule is designed to prohibit access to sensitive weapons by a lone individual. Two authorized persons will be considered to be present when they are in a physical position from which they can positively detect incorrect or unauthorized procedures with respect to the task and/or operation being performed. When application of the two-man rule is required, it will be enforced constantly by the persons who constitute the team while they are accomplishing the task or operation assigned and until they leave the area in which it is required.

c. The two-man rule should not, however, be considered applicable only in the cited situations. It can, and should, be applied in many other aspects of physical security operations, such as the following:

(1) When uncontrolled access to vital machinery, equipment, or materiel might provide opportunity for intentional or unintentional damage which could affect the mission or operation of the installation or facility.

(2) Where uncontrolled access to funds could provide opportunity for diversion by falsification of accounts.

(3) When uncontrolled delivery or receipt for materials could provide opportunity for pilferage through “short” deliveries and false receipts.

(4) When uncontrolled access to an arms or ammunition storage room could provide an opportunity for theft. Keys should be issued so as to require the presence of at least two men to unlock the three locks required under provisions of AR 190-11. (This is analogous to the safe deposit box system, which requires two keys in the possession of two different persons.)

d. The foregoing are only a few examples the listing is virtually limitless. The important point to be stressed is that the provost marshal and the physical security manager should explore every possible aspect of physical security operations in which the two-man rule would provide additional security and assurance, and include all appropriate recommendations and provisions in the overall physical security plan.

4-18 Additional Procedures For Specific Groups

a. Visitors— Entrance prerequisites:

(1) Verify identity.

(2) Contact person or activity to be visited to insure identity and validity of visit.

(3) Record visitor information.

(a) Issue visitor badges.
(b) Use registration forms.

b. VIPs and foreign nationals, special consideration— Coordination with protocol office:

(1) Twenty-four hour advance notice desirable.

(2) Agenda for visit and designation of escort officer, if appropriate.

c. Civilians working on jobs under government contract— The security manager should:

- Coordinate with procurement office to determine applicable provisions of contract.
- Identify procedures to control the movement of those employees.
- Insure that protection of the construction site is accomplished with available resources.

d. Supervisors using cleaning teams should seek technical advice from the physical security office on internal controls for each specific building.

e. Public utility and commercial service representatives:

(1) Entrance prerequisites same as for visitors.

(2) Designated activity personnel check on authority to remove equipment for maintenance.

f. DOD employees in work areas after normal operational hours:

□ Supervisors establish internal controls, based on coordination with the security manager.

□ Notify security personnel of workers' presence and expected duration of work.

4-19 Security Personnel At Entry and Exit Points

The security manager responsible for these individuals must insure that the personnel:

a. Are alert, very perceptive, tactful, and capable of exercising sound judgment in executing their duties and responsibilities.

b. Conduct frequent, irregular checks of their assigned areas during periods of inactivity (holidays, weekends, after-duty hours, etc.). (Also, see chapter 5.)

4-20 Mechanized/Automated Systems

Identification and access control systems base their identification judgment factor on a remote capability through a routine discriminating device for positive ID, as opposed to the manual system's using a guard force member to conduct identification based on access rosters and personal recognition.

a. In a mechanized identification system, the following actions occur within the machine:

(1) Receives physical ID data from an individual.

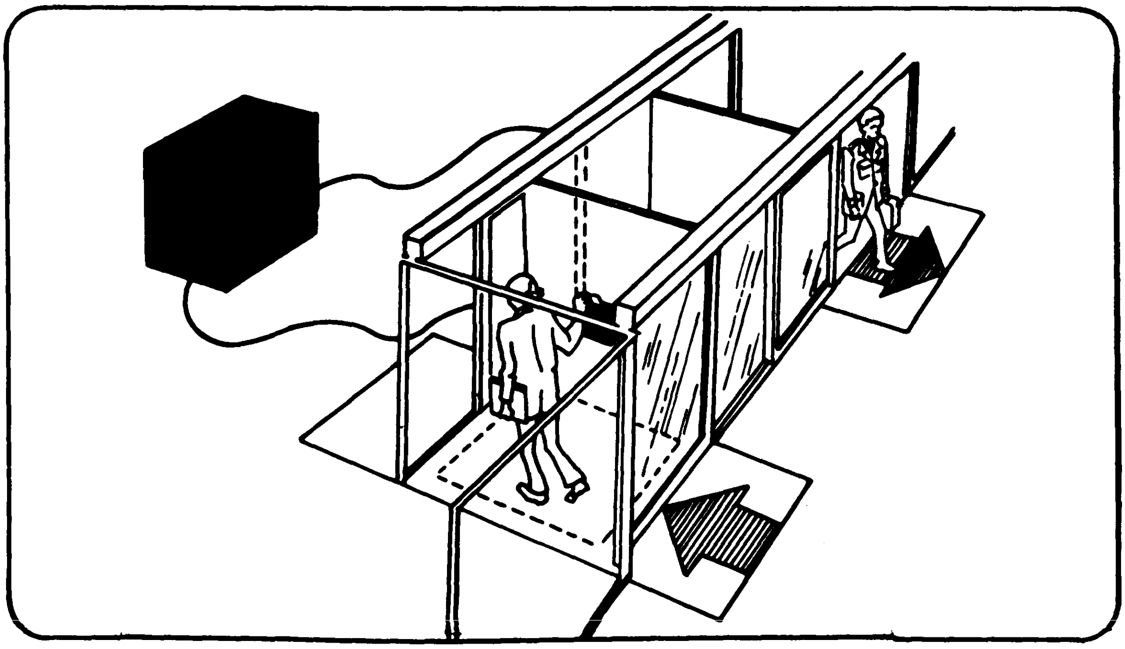
(2) Encodes this data for use.

(3) Compares this data to stored data.

(4) Makes ago or no go decision based on the comparison.

(5) Translates the results into readable form.

b. Several mechanical devices add to the security posture and are expanding in popu-



Computer makes go or no go decision based on data received.

larity and use. Such devices use the following techniques:

(1) Magnetic coding.

(2) Embossing.

(3) Optical characters.

(4) Dielectric coding.

c. Specialized mechanical systems are ideal for highly sensitive situations because these systems use a controlled process in a controlled environment to establish the required data base and accuracy.

(1) One innovative technique with application to identification and admittance procedures involves dimension comparisons. The dimension of a person's full hand is compared to previously stored data to determine entry authorization. Another specialized machine reader can scan a single fingerprint and provide positive identification of anyone attempting entry. (Good for semiremote environment.)

(2) The voiceprint technique is being widely used as an identification means and features rapid processing with accuracy.

d. An all-inclusive automated ID and access control system reinforces the security indepth ring through its easy and rapid change capability. The computer is able to do this through its memory, stored on magnetic tape or disc. Changes can be made by remote use of specific code numbers. The big advantage for this system is that changes do not require wiring or media alterations.

e. The commercial security market has a wide range of mechanized and automated hardware-software systems interfacing for the enhancement of any security posture. Assessment of security needs and use of the planning, programing and budgeting procedures outlined in chapter 2 will greatly assist a security manager in improving the overall security posture.

Designation of Restricted Areas

Section III

4-21 Restricted Areas

The term "restricted area" as used here, is defined (AR 380-20) as "Any area, access to which is subject to special restrictions or controls for reasons of security or safeguarding of property or material."

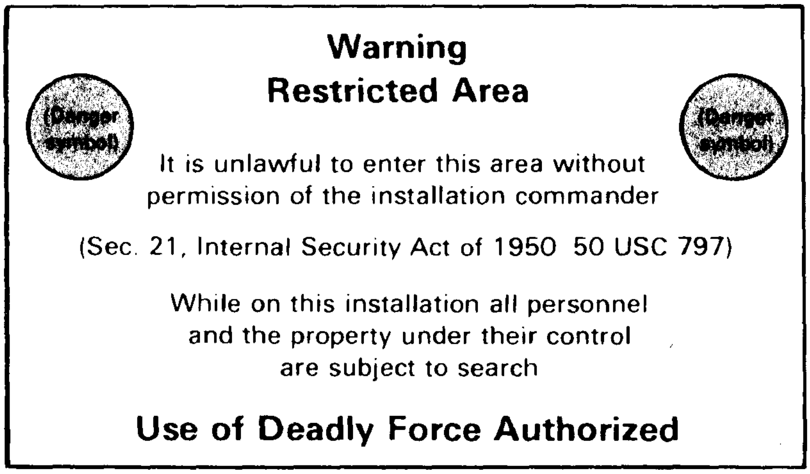
a. Designation and establishment of restricted areas is the responsibility of the military commander of the installation or facility. His authority is derived from Department of Defense Directive No. 5200.8, dated 20 August 1954, which was issued pursuant to the provisions of section 21, Internal y y Act of 1950. Within the Army, the DOD Directive was implemented by AR 380-20.

b. AR 380-20 states, "these regulations apply only to Army installations or activities within the continental United States. Oversea commanders may utilize these regulations for guidance in establishing local procedures."

c. The terms, "restricted area," "controlled area," "limited area," and "exclusion area," are described by AR 50-5 as standard terminology. The regulation states that these terms "will be employed wherever United States Army nuclear weapon material is involved." Such employment outside the continental United States would, however, require publication of an appropriate command directive, since AR 380-20 would not apply.

d. It is clearly the meaning and intent of these documents that the security protection afforded by a restricted area pertains particularly to subversive activities control, that is, protection against espionage, sabotage, or any such actions adversely affecting the national defense of the United States. Within this context, the designation "restricted area, " as defined, is not applicable to an area solely for protection against common pilferage or misappropriation of property or material which is not classified or not essential to the national defense. For example, an area devoted to the storage or use of classified documents, equipment or materials should be so designated to safeguard against espionage. An installation communications center should also be so designated, to safeguard against sabotage. On the other hand, a cashier's cage or an ordinary mechanic's toolroom should not be so designated, although the commander may impose controls on access thereto. This may be as simple a matter as posting a sign, "Off Limits to Unauthorized Personnel," or it may require the erection of fences, railings, etc. The responsibility for designation is, of course, the commanders. However, in furnishing advice to him, the provost marshal or physical security manager should consider carefully the foregoing guidance; evaluate the purpose of any proposed or necessary designation of a restricted area; coordinate with the intelligence officer and staff judge advocate; and formulate his recommendations accordingly.

e. To comply with the requirements of the Internal Security Act of 1950 and the provisions of implementing directives, and to



Warning
Restricted Area

(Danger symbol)

It is unlawful to enter this area without
permission of the installation commander

(Sec. 21, Internal Security Act of 1950 50 USC 797)

While on this installation all personnel
and the property under their control
are subject to search

Use of Deadly Force Authorized

(Danger symbol)

provide for proper procedures in cases of violation, a restricted area must be designated in writing as such by the military commander and must he posted with warning signs or notices of the type described in AR 380-20. 0-20.

f. The establishment of restricted areas improves security by providing defense in depth (see also paragraph 1- 3c) and increases efficiency by providing degrees of security compatible with operational requirements. These specially designated areas may also provide for economy of operation by reducing the need for stringent control measures for the installation or facility as a whole.

4-22 Types of Restricted Areas

a. The degree of security and controls required depends upon the nature, sensitivity. or importance of the security interest or other matter involved. Restricted areas may be established to provide the following:

(1) Effective application of necessary security measures and exclusion of unauthorized personnel.

(2) Intensified controls over those areas requiring special protection.

(3) Conditions for compartmentalization of classified information or critical equipment or materials, with minimum impact on operations.

b. Different areas involve different degrees of security interest, depending upon their purpose and nature of work, information, and/or materials concerned. For similar reasons, different areas within an installation may have varying degrees of importance. In some cases, the entire area of an installation may have a uniform degree of importance, requiring only one level of restriction and control. In others, differences in degrees of importance will require further segregation or compartmentalization of activities.

c. To meet these different levels of sensitivity and to provide for an effective and efficient basis for applying the varying degrees of restriction of access, control of movement, and type of protection required, restricted areas or portions thereof may be further administratively designated as "exclusion," "limited," or "controlled" areas. It must be understood that the term "restricted area" is in effect a legal designation (Internal Security Act of 1950), whereas the terms, "exclusion" and "limited" are administrative only (AR 380-20). The term "controlled area, " is not mentioned in either the Security Act or

AR 380-20, and is used only as a matter of convenience.

d. The primary criteria for administrative designation of exclusion, limited, and controlled areas is the degree of restriction or controls required to prevent compromise of the security interest or other matter therein. Characteristics of these areas are:

(1) Exclusion area— A restricted area containing one of the following:

(a) A security interest or other matter of such nature that access to the area constitutes, for all practical purposes, access to such security interest or matter.

(b) A security interest or other matter of such vital importance that proximity resulting from access to the area is treated as equivalent to **(a)** above.

(2) Limited area— A restricted area containing a security interest or other matter and in which uncontrolled movement will permit access to such security interest or matter, but within which access may be prevented by escort and other internal restrictions and controls. Individuals who have a legitimate reason for entering a limited area may do so if internal restrictions and controls are provided to prevent access to the security interest or other matter. These measures usually consist of escorts and other physical safeguards.

(3) Controlled area— An area, usually adjacent to or encompassing limited or exclusion areas. Access to a controlled area is restricted to those with a need for access. However, movement of authorized personnel within this area is not necessarily controlled, since mere access to the area does not provide access to the security interest or other matter within the exclusion or limited areas. The controlled area is provided for administrative control, safety, and/or as a buffer zone for depth in security for the exclusion or limited areas. The degree of control of movement within this area will, therefore, be as prescribed by the appropriate commander.

e. You can see from the foregoing that an installation may have varying degrees of security designation, or none at all. It maybe designated in its entirety as a restricted area, with no further degree of restrictions or controls. It may, however, provided that it is first designated as a restricted area, to bring it under the provisions of the Internal Security Act of 1950, be further administratively classified, in whole or in portions, as an exclusion area, limited area, or controlled area with specific clear zones (figures 6,7,8,9 and 10).

4-23 Other Considerations

a. There are other important considerations which should be kept in mind concerning restricted areas and their compartmentalization. Some of these are:

(1) Immediate and anticipated needs can be determined by survey and analysis of the installation or facility, its missions, and the security interests or other matters on hand which require protection. Anticipated needs can be determined from future plans.

(2) The **nature of the security interest** or other matter to be protected. Classified documents and small items may be protected by securing them in safes or locked containers, whereas large items may have to be placed within guarded enclosures.

(3) Some **security interests are more sensitive to compromise** than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.

(4) All security interests should be **evaluated according to their relative importance.** This may be indicated by a security classification such as TOP SECRET, SECRET, or CONFIDENTIAL, or by their criticality. That is, the effect their loss or compromise would have on national defense or the mission of the installation or facility.

b. Parking areas for privately owned vehicles must be established outside restricted areas, if at all possible. This is due to the fact that large amounts of articles can be readily concealed in vehicles, and would then be harder to detect than if they were on a person. Also, entrances should be kept at a minimum necessary for safe and efficient operation and control.

c. Establishment of restricted areas within an installation improves overall security by providing security in depth. Limited and exclusion areas serve as inner rings of security; the controlled area serves as a buffer zone. As a general rule, an increase in security results in some slowdown in operations. However, **without security there may be no operations.** The use of security areas makes it possible to have security compatible with operational requirements. Instead of establishing stringent control measures for the installation as a whole varying degrees of security can be provided as required and as conditions warrant. In this way, interference with overall operations is reduced to a minimum and operational efficiency can be maintained at a relatively high level.

d. Where required, adequate physical safeguards such as fences, gates, and window bars must be installed to deny entry of unauthorized persons into restricted areas. Except where such action would tend to advertise an otherwise concealed area, warning signs or notices must be posted in conspicuous and appropriate places, such as ordinary entrances or approaches to these areas, and on perimeter fences or boundaries of each area.

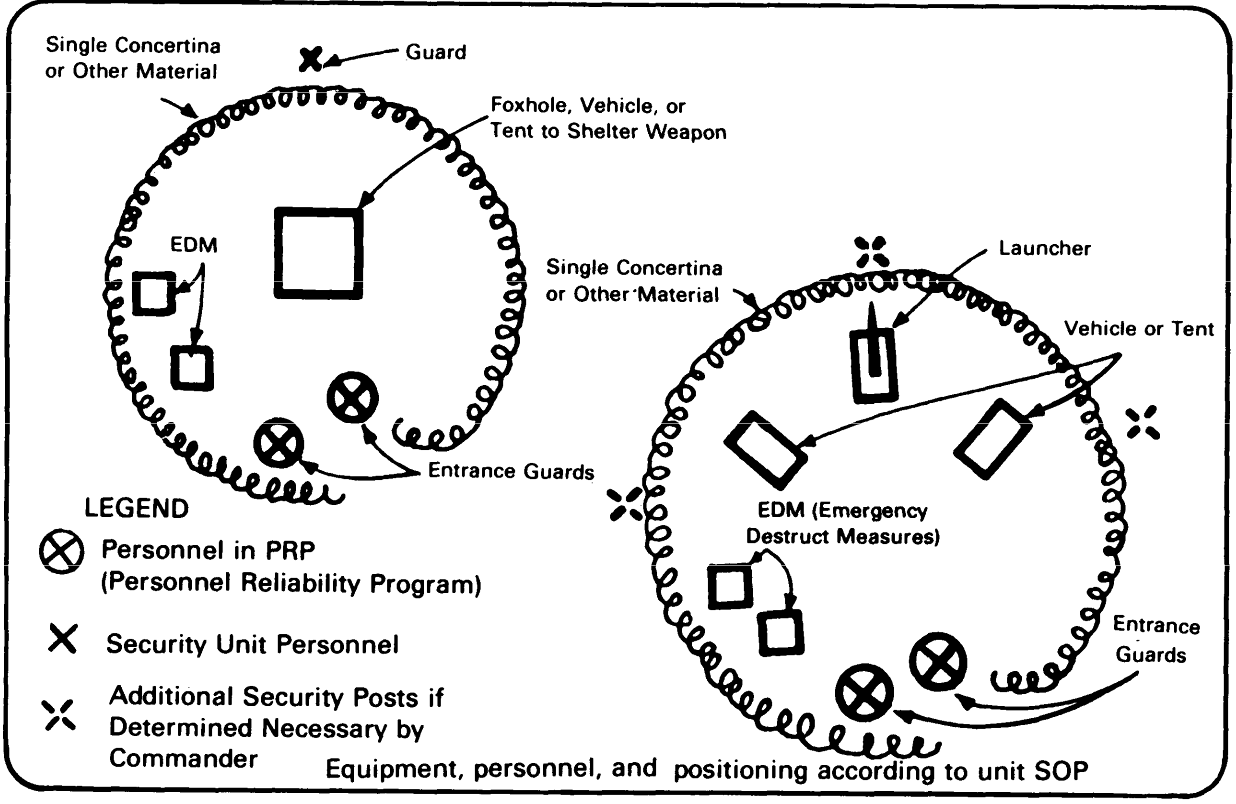
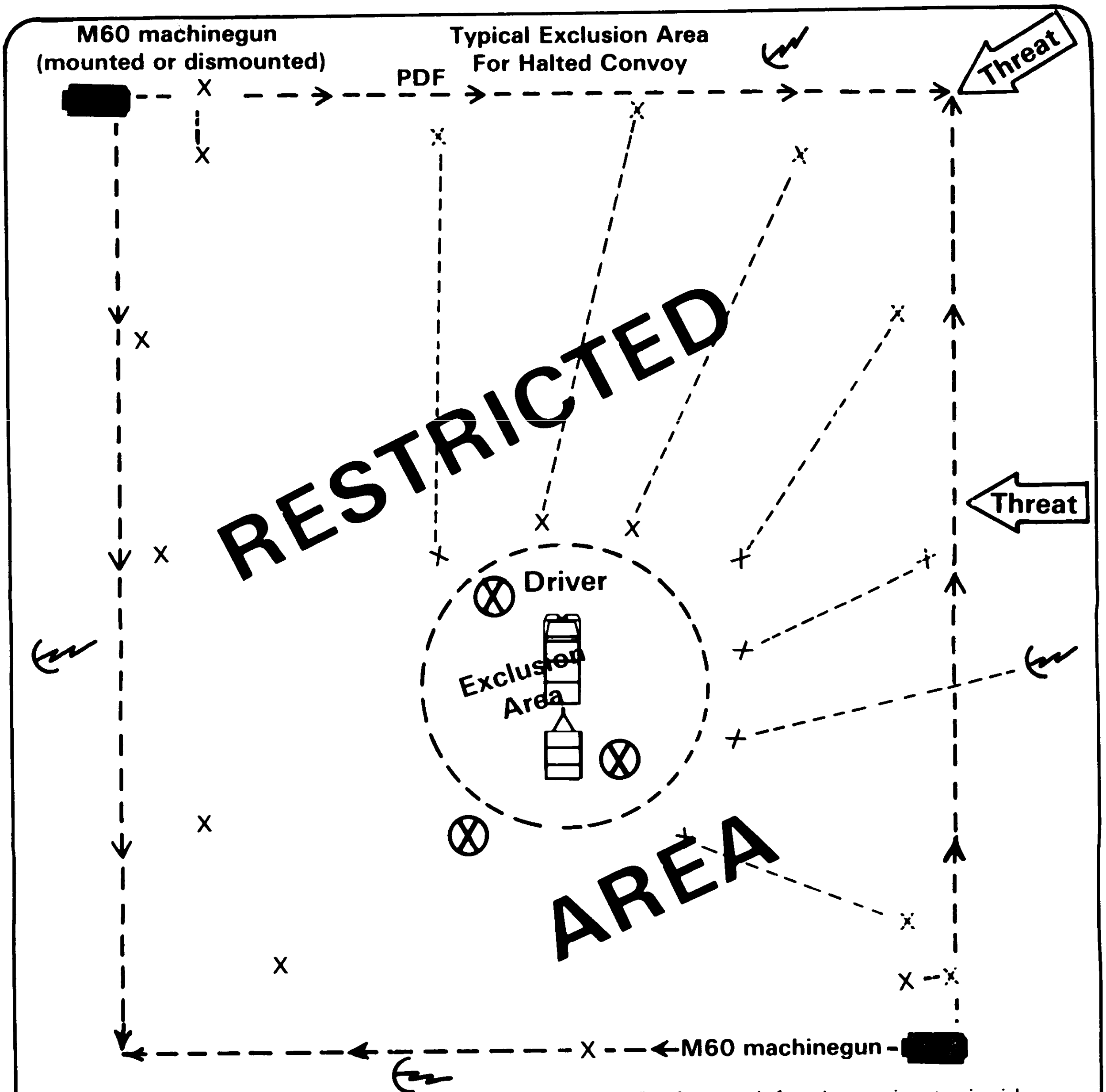

Single Concertina or Other Material
Guard
Foxhole, Vehicle, or Tent to Shelter Weapon
EDM
Single Concertina or Other Material
Launcher
Vehicle or Tent
Entrance Guards
LEGEND
⊗ Personnel in PRP (Personnel Reliability Program)
X Security Unit Personnel
Additional Security Posts if Determined Necessary by Commander
EDM (Emergency Destruct Measures)
Entrance Guards
Equipment, personnel, and positioning according to unit SOP

Figure 6—Sample layout of temporary tactical restricted areas.



Note: Other vehicles and personnel, to include the LPs, form a defensive perimeter inside the primary directions of fire of the M60 machineguns. During attack, alternate machinegun crews should be placed in the perimeter away from primary machineguns and be spaced so that if they are needed as replacements, large gaps do not appear in the perimeter.

Legend

X MP rifleman

⊗ PRP qualified (see AR 50-5)

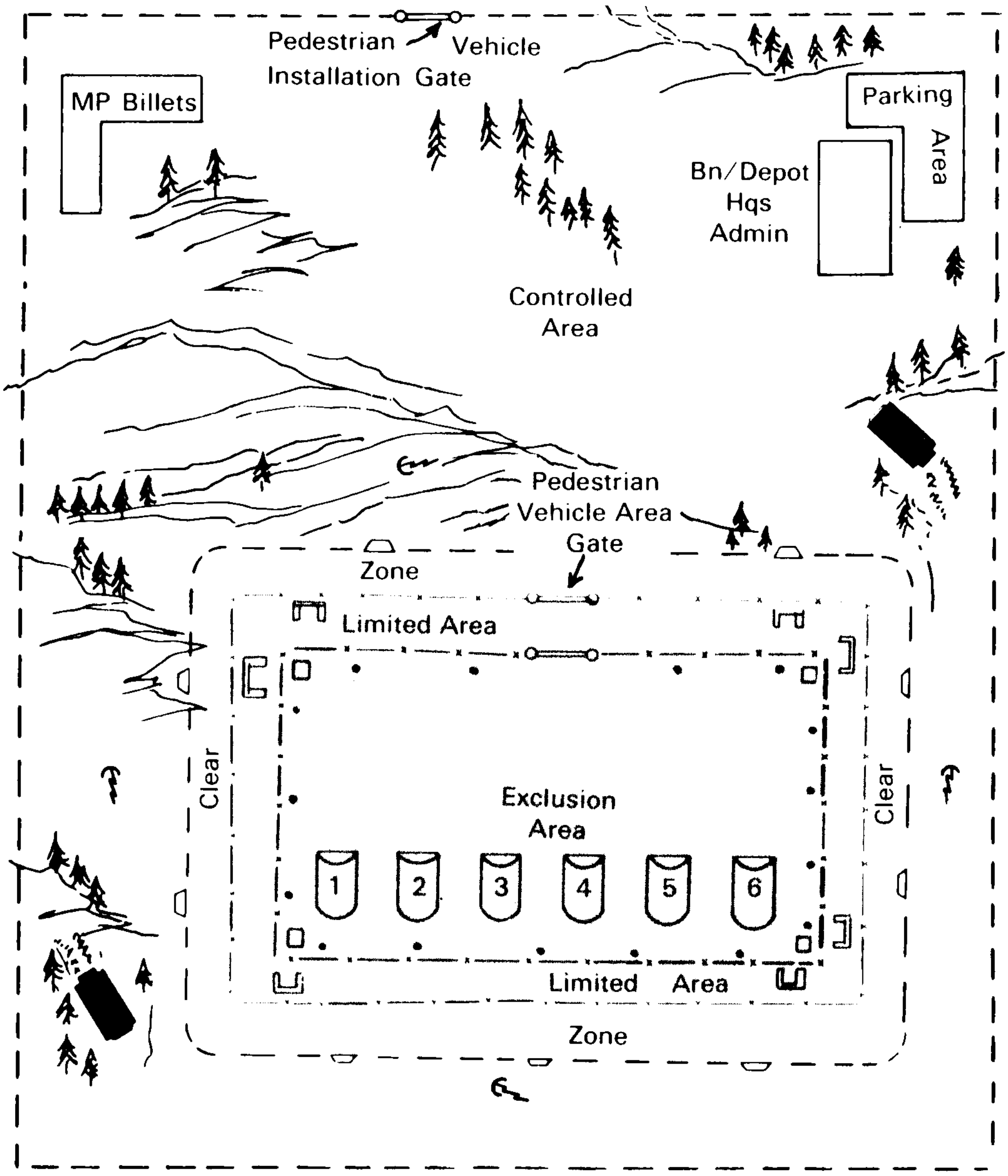
←—←— Principal direction of fire

◌ Temporary exclusion area (size depends on terrain and threat force)

Listening Post

Figure 7—Sample layout for temporary tactical exclusion area.

Depot Complex
(Restricted Area—Base Defense)



Legend

- - - - Chainlink fencing with top guard on perimeter of restricted area

□ Guard tower

▽ Restricted area warning signs

Listening post

● Protective lighting

Fighting position

MG Depending on direction of attack and terrain features, the MG teams may displace to establish final protective fires (FPF) or principal direction of fire (PDF).

Figure 8—Diagram of depot complex example.

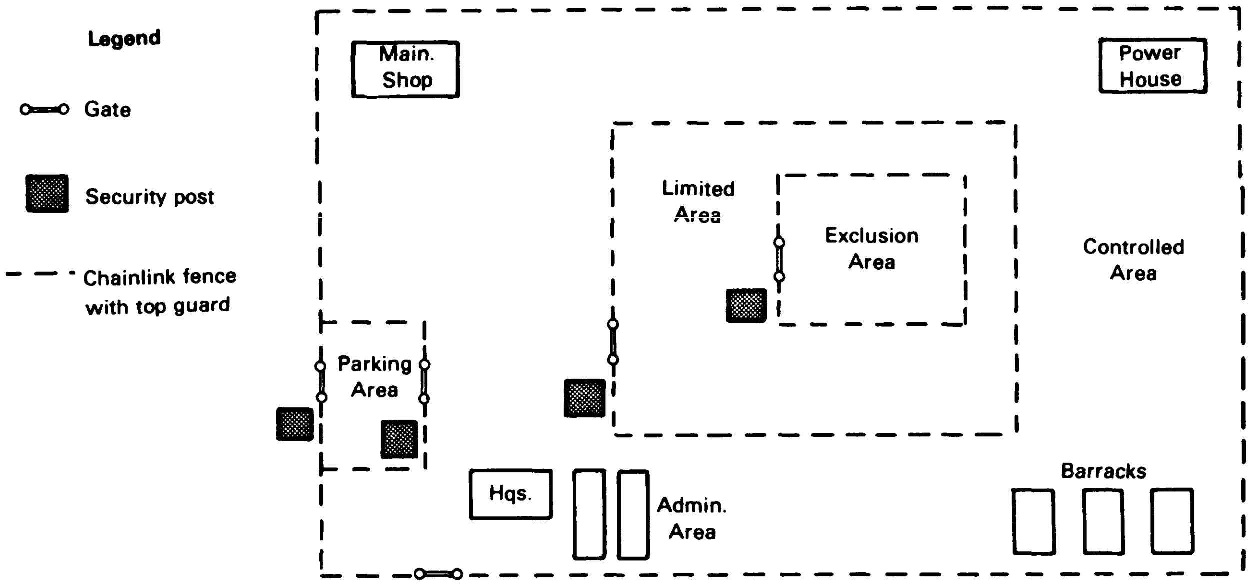


Figure 9—Schematic diagram of simplified restricted area and degrees of security.

Package, Materiel, and Property Control Section IV

4-24 Package Control

a. A good package control system helps prevent or minimize pilferage, sabotage and espionage. Only packages with proper authorization should be permitted into restricted areas without inspection.

b. A positive system should be established to control movement of packages, materiel, and property into and out of the installation.

c. A package checking system, using Individual Property Pass, DA Form 1818, or a similar form, may be used at the entrance gate for the convenience of employees and visitors. When practicable, inspect all outgoing packages except those properly authorized for removal. When 100 percent inspection is impracticable, conduct frequent unannounced spot checks.

4-25 Property Controls

a. Property controls must not be limited to packages carried openly; but must include control of anything that could be used to secret property or materiel of any type.

b. Persons should not be routinely searched except in unusual situations. When they are, it should be only in accordance with published command directives.

4-26 Vehicle Control

a. All privately owned/visitor-operated motor vehicles on the installation should be registered with the provost marshal or the installation physical security office. Requirement to display a tag or decal should be IAW AR 190-5 and AR 210-10.

b. Vehicles belonging to visitors should be identified by a temporary decal or identification media different from permanent registration to permit ready recognition by security personnel.

c. When authorized vehicles enter or exit a restricted area, each must undergo a **sys-**

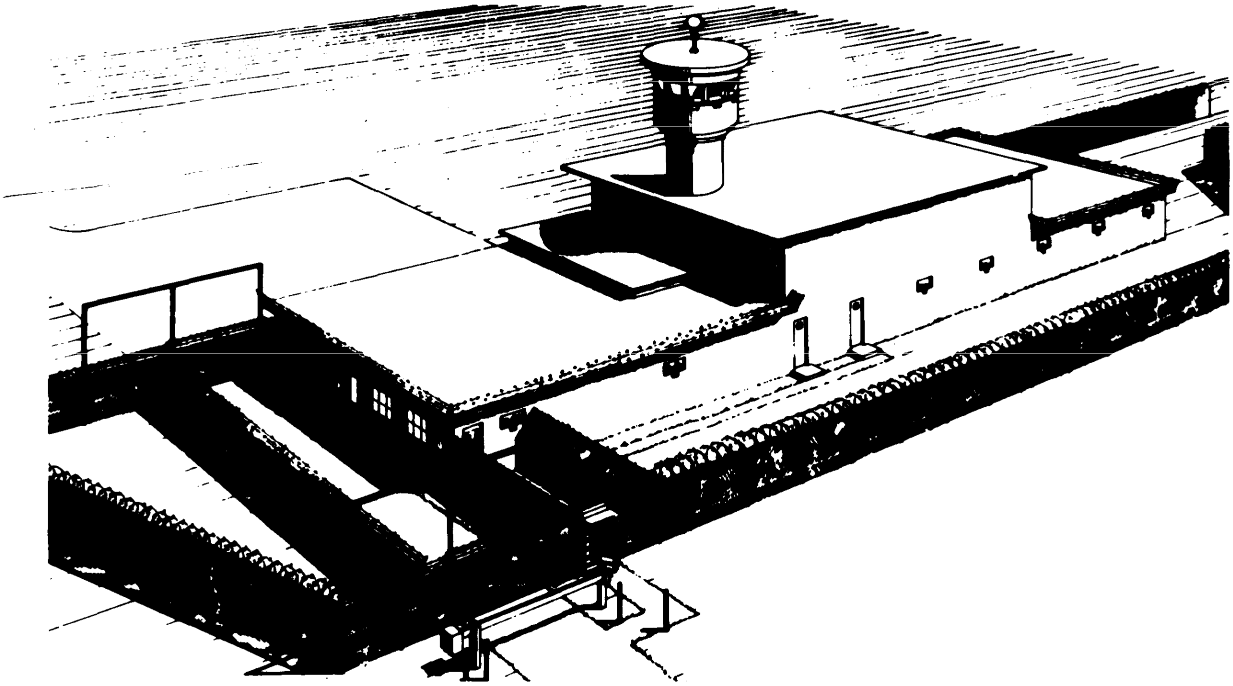


Figure 10—Drawing of standard physical security layout.

tematic search, including, but not limited to, the following areas:

- Interior of vehicle
- Engine compartment
- External air breathers
- Top of vehicle
- Battery box
- Cargo compartment
- Undercarriage.

4-27 Truck and Railroad Car Control

a. Movement of trucks and railroad cars into and out of installations or facilities should be supervised and each inspected to prevent the entry or removal of unauthorized persons or materiel. Inspectors should be especially watchful for explosives or incendiaries.

b. Truck and railroad entrances should be **controlled by locked gates** when not in use, and should be under security supervision when unlocked or opened for passage.

c. **Identification cards or badges** should be issued to operators of trucks and railroad engines to insure proper identification and registration of those entering and leaving the area. Such cards or badges should permit access only to specific loading and unloading areas.

d. All conveyances entering or leaving a protected area should be required to pass through a service gate manned by security forces. Drivers, helpers, passengers, and ve hicle contents should be carefully examined. The security check should include

- Appropriate entries in security log, date, operator's name, description of load, time entered and departed.
- License check of operator.
- Verify seal number with shipping document and examine seal for tampering.

e. Incoming **trucks and railroad cars must be assigned escorts before they are permitted to enter designated limited or exclusion areas.** Commanders should establish published procedures to control the movement of trucks and railroad cars that enter designated **restricted areas** to discharge or pick up cargo. Escorts should be provided when necessary.