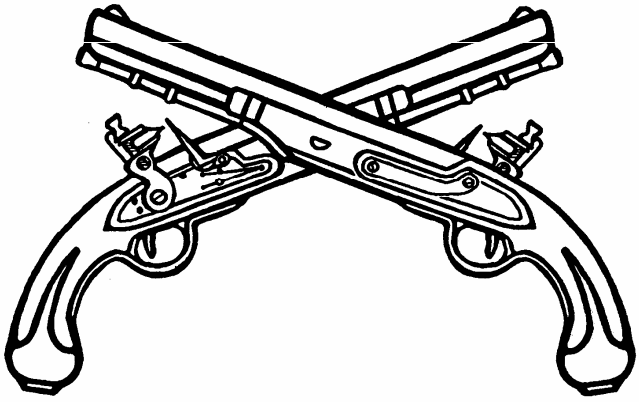
SUBCOURSE
MP1003

EDITION
C

MATERIEL CONTROL

MP



SETS THE STANDARD FOR EXCELLENCE

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM

AIPD

READINESS / PROFESSIONALISM

THRU GROWTH

MATERIEL CONTROL

Subcourse Number MP1003

EDITION C

United States Army Military Police School
Fort McClellan, Alabama 36205-5030

5 Credit Hours

Edition Date: May 1996

SUBCOURSE OVERVIEW

We designed this subcourse to teach you the basic materiel control measures to use in your physical security program and perform duties as a physical security specialist/supervisor.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time it was prepared. In your own work situation, always refer to the latest official publications.

Unless otherwise stated, the masculine gender of singular pronouns is used to refer to both men and women.

TERMINAL LEARNING OBJECTIVE

ACTION: You will learn the various measures used to control materiels as part of a physical security program.

CONDITION: You will have access to this subcourse, paper and pencil.

STANDARD: To demonstrate competency in this task, you must achieve a minimum of 70 percent on the subcourse examination.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont)

TABLE OF CONTENTS (Cont)

THIS PAGE INTENTIONALLY LEFT BLANK

LESSON 1

INSTALLATION PHYSICAL SECURITY

Critical Tasks: 191-386-0007

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to identify and implement the control measures required for packages, materiel, and vehicles on a post.

TERMINAL LEARNING OBJECTIVE:

ACTION: Identify and implement control measures required for packages, materiel, and vehicles on a post.

CONDITION: You will have this subcourse, pencil and paper.

STANDARD: Evaluation of your performance will be by successful completion of the examination (70 percent).

REFERENCES: The material contained in this lesson was derived from the following publication: FM 19-30, AR 190-51, AR 190-13, AR 190-11, and Physical Security Update 10-3.

INTRODUCTION

Millions of dollars each year are lost to pilferage. This is true in both the government and the private sector. Theft is often difficult to detect, hard to prove, and dangerous to ignore. Therefore, measures must be taken to counter such threats. Private businesses often deal with the high cost of petty pilferage. They mark up merchandise to absorb the loss; they implement physical security programs. Government, however, is not a profit making business, so its cost cannot be passed to individuals wanting a commodity. However, the public still pays the cost in the form of taxes. Security personnel are therefore entrusted with providing countermeasures to prevent property loss. Package materiel, and vehicle control is one means of minimizing loss at posts and facilities. When items of value are pilfered, or destroyed, the credibility of your security personnel suffer.

PART A - PURPOSE OF PACKAGE AND MATERIEL CONTROL

All posts and facilities can anticipate loss from theft. Type and amount of materiel and equipment influence this loss. Other influences are storage and processing facilities and number of employees.

Social and economic conditions in the surrounding communities also influence the actual loss from pilferage. Ignored, this loss would be impossible to determine. Accounting methods must be used for package and materiel to do the following:

a. Prevent introduction of contraband.

b. Prevent removal of unauthorized materiel.

c. Control and expedite authorized entry and removal of packages and materiel. This should be done without interruption of normal operations.

d. Prevent loss or damage by properly executing existing security measures.

PART B - PILFERAGE

1. The words "pilferage" and "shoplifting," as mentioned in other lessons, are included within the meaning of stealing, theft, larceny, and other such terms. All of these imply theft of any quantity or any item of materiel with a monetary value. Pilferage is theft of any kind of materiel by persons who are authorized within the facility or area. It is the threat best controlled by package, materiel and vehicle control. Therefore, discussion will be more in depth than in previous lessons.

a. A casual pilferer can be almost anyone. He steals if given the chance; he takes items for individual use. He requires no assistance and steals without prior planning. The size of the item is very important.

b. A systematic pilferer is a person or group of people who steal according to a preconceived plan or method. He has a motive of some form or seeks personal profit. He carefully plans his operation, steals for monetary value, and requires the aid of several people. The size of the item stolen is not important.

2. Reasons for Stealing. People steal for many reasons. Listed below are a few of the reasons and explanations.

a. Profit. The casual pilferer steals things he can use without paying for them. Most systematic pilferers steal for the money they hope to make by selling the items.

b. Excitement. They have little concern about the items they are stealing. They enjoy beating the system. If they are a success, they can turn systematic.

c. A kleptomaniac is a person who will take items without regard for value or use. They steal compulsively and often openly. They repeat even after several apprehensions, and they are generally nervous and shy.

d. A disaffectionate person steals to get back at the system or a person.

e. Temptation occurs when he is given the chance to take something of value with little or no risk of getting caught.

f. A person in debt will steal anything of value in order to get money to pay his debts.

g. A drug addict will hit and run to support his drug use.

3. Targets for Pilferage. Prime areas on an installation which are targets for pilferage:

a. Shipping and Receiving Areas. These areas are considered the most vulnerable to pilferage of items. It is in these areas that physical control of the item is the least apparent.

b. Theft Through Trash Channels. This is one of the favorite means of the systematic pilferer to transport his item from an area. The person is usually in coordination with trash pickup employees. He stashes the stolen item in a dumpster. The trash man empties the item in the trash truck, and removes the item from the post.

c. Theft through empty cargo trailers or CONEXES. This is the same principle as theft through trash channels. The item is loaded into an empty cargo trailer or CONEX and pulled off the post.

d. Parking of privately owned vehicles. This is one area often overlooked by the security officer at a post. Parking areas designated too close to a warehouse make the removal of items very easy.

4. Control Measures for Casual Pilferage. Specific measures for preventing theft must be based on careful analysis of the conditions at each post. The most practical and effective method is to establish psychological deterrents. This may be done in a number of ways.

a. One of the most common means of discouraging casual theft is to search persons and vehicles leaving the post at unannounced times and places. Sometimes a total inspection of package, materiel, and vehicles is impractical. If so, you should conduct frequent unannounced spot checks of these as they leave restricted areas.

(1) Spot searches may sometimes detect attempts of theft, but greater value is realized by bringing one fact to the attention of all personnel: they may be apprehended if they do try to illegally remove property. AR 210-10 states that the installation CO will establish rules governing the entry of persons to and exit from the post. This regulation also states that the installation CO sets rules regarding the search of persons and their possessions.

(2) The installation CO may directly authorize security personnel to search persons and possessions. This may be done entering, visiting, or leaving post facilities. These persons may be military or civilian personnel

or visitors. Such searches are authorized when based upon probable cause that an offense has been committed; searches may be authorized upon military necessity. Instructions of COs about such searches should be specific and complete. Security personnel should be taught that incoming personnel should not be searched over their objection, but they may be denied the right of entry upon refusal to consent to search. All persons entering facilities should be advised in advance of likely searches. A notice prominently displayed can fill this need. Persons should know they are liable to search upon entry, while on post, or upon exit.

(3) Care must be taken to ensure that personnel are not demoralized. Their legal rights should not be violated by oppressive physical controls or unethical security practices. Persons should not be routinely searched except in unusual cases.

b. An aggressive security education program is a good means of convincing employees that they have much more to lose than to gain by thieving. Case histories may be cited where personnel were discharged or prosecuted for pilferage. Care must be taken in discussing these cases: individuals involved should not be identified. This will avoid possible civil suits for defamation of character. It is generally poor policy to publicize derogatory information about a certain person. It is important for all employees to realize that pilferage is morally wrong; this is true, no matter how little the value of the items taken. It is particularly important for supervisory personnel to set a proper example. They must maintain a desirable moral climate for all subordinates. All personnel must be impressed with the fact that they have a duty to report any loss to proper authorities.

c. Adequate inventory and control measures should be instituted. These measures should account for all materiel, supplies, and equipment. Poor accountability, if it is commonly known, provides one of the greatest sources of temptations to the casual thief.

d. All tools and equipment should be identified by some mark or code (where feasible). This is necessary so that government property can be recognized. Government tools and equipment have counterparts in the civilian economy, and they cannot otherwise be identified as government property. Another control method is to require signing for all tools and equipment to be used. The use of signature control methods reduces the temptation to pocket the item. Proper documentation and accountability is the best method of controlling materiel.

5. Control Measures for Systematic Pilferage.

a. Package Control.

(1) A good package control system is an invaluable aid. It helps greatly to prevent or minimize pilferage, acts of sabotage, or espionage. No packages, except those with proper authorization, should be allowed into restricted areas without inspection.

(2) A positive system should be set up to control movement of packages, materiel, and property into and out of the post. Limitations should be included in the physical security plan. Such limitations may concern the types of property authorized, persons allowed to move it and approved points of entrance and exit.

(3) A package checking system may be done at entrance gates. DA Form 1818 (Individual Property Pass) or a similar form may be used. This system is used for the convenience of employees and visitors. When practicable, all outgoing packages should be inspected except those properly authorized for removal. When 100 percent inspection is impractical, frequent unannounced spot checks should be done.

(4) DD Form 577 (Signature Card) is used in physical security to verify signatures in support of DA Form 1818. Each activity or post CO should require that signature cards be prepared on persons authorized to allow property removal. Each card should be prepared in triplicate. The first is for the person authorizing release of the property. A second copy is filed at the local security office. The third copy goes to the security guard at the gate or control point for immediate reference.

(5) DA Form 1818 (Individual Property Pass) acts as a check and balance for authorized property removal. A property pass may be temporary or permanent with a valid use of 24 hours to 90 days. This depends on local policy. You should control the forms from one location, preferably the physical security office. Best accountability and control of forms can be maintained this way.

b. Vehicle Control. Each post CO should publish directives governing the registration and operation of motor vehicles on a post. Controls should be established to provide for the movement of vehicles into and out of the area. Directives should include, as a minimum, the following:

(1) Vehicle registration requirements.

(2) Speed limits.

(3) Parking procedures, limitations, and/or restrictions.

(4) Other local traffic control requirements as may be necessary.

(5) Procedures for reporting and investigating all traffic accidents.

(6) Disposition of traffic violation offenders.

(7) Assessment of points for violation of traffic regulations.

(8) Procedures for the safe handling of vehicles transporting explosive, combustible, or hazardous items.

c. Registration of Vehicles.

(1) Vehicles Privately Owned and Operated. All motor vehicles privately owned and operated by personnel should be registered. Registrations should be with the provost marshal or the physical security officer. These vehicles should also display a tag or decal (AR 210-10 and AR 190-5). Concerned vehicles are those used by personnel living on or employed on post. Also included are those vehicles used in making daily or frequent visits to the post. Prerequisites for registration normally include the following:

(a) Evidence of ownership and a state certificate of registration.

(b) Valid operator's license or permit issued by the state in which the vehicle is registered.

(c) Motor vehicle liability insurance.

(d) Vehicle inspection (where deemed necessary by the post CO).

(e) Issuance of decal.

(2) Additional Procedure. Vehicle registration and display of a decal is a must, but it does not excuse the driver from compliance with the normal personal identification and admittance procedures.

(3) Registration of Visitor's Vehicles. All visitor vehicles should be registered. Registration should include the make of vehicle, license number and name of driver. It should also include the destination, purpose of visit, time and date of entry and departure. Vehicles of visitors should be identified by a temporary decal or ID media. This should be different from permanent registrations to permit ready recognition by security guards. Visitors should be directed to parking areas. These should be specifically designated. Sometimes visitors are allowed entry after normal duty hours. If so, local regulations normally specify the conditions of entry. Other limitations are also spelled out to assure proper control at all times.

(4) Temporary Registration. At some posts it is advisable to issue temporary registration. This is especially so when there is a large turnover of permanent personnel. Temporary registration is only valid for 72 hours. This is enough time for personnel to see to permanent registration. It is also long enough for them to clear the post after permanent registration has been cancelled.

(5) Tags and Decals. State laws differ as to the type and placement allowed for other than state registrations tags. A check of the applicable laws should be made. This check should occur before planning for vehicle registration. It should also be done before the placement of tags of decals on the vehicle.

d. Vehicles in Restricted Areas.

(1) When authorized vehicles enter or exit a restricted area, each must undergo a systematic search. The search should include the following:

(a) Interior vehicle.

(b) Engine compartment.

(c) External air breathers.

(d) Top of vehicle.

(e) Battery box.

(f) Cargo compartment.

(g) Undercarriage.

(2) A restricted area is any place to which access is subject to special restrictions or controls. This is done for reasons of security or safeguarding of property or materiel.

(3) A restricted area must be designated in writing. It must be posted with warning signs or notices. These should be of the type described in AR 190-13 (See figure 1-1).

WARNING

This (fort, range, plant, etc.) has been declared a restricted area according to a Secretary of Defense directive issued 20 August 1954 under the provisions of section 21, Internal Security Act of 1950. Unauthorized Entry is prohibited.

All persons and vehicles entering hereon are liable to search. Photographing or making notes, drawings, maps, or graphic representations of this area or its activities is prohibited unless specifically authorized by the commander. Any such material found in the possession of unauthorized persons will be confiscated.

Figure 1-1. Restricted area warning sign.

e. Vehicle Parking Control.

(1) Whenever possible, parking areas for privately owned vehicles should be located outside the perimeter of restricted areas. Parking areas should be fenced and lighted. Entrances and exits to these areas should be separate from others. The method of parking should be clearly marked and strictly enforced.

(2) Sometimes it is found impractical to require that all cars be parked outside restricted areas. If so, then only employees should be allowed to park within the enclosure. In case of interior restricted area parking, the parking zone should be away from important facilities or processes. They should be separately fenced in such a way that occupants of vehicles must pass through a pedestrian gate before entering the facility. Security guard personnel should monitor movements of personnel to parking areas. This will prevent unauthorized removal of property.

(3) Enough parking space should be provided for visitors near access control points to prevent their entering other areas. Visitor parking areas should be under close watch of security guards. This will prevent unauthorized removal of government property.

f. Truck Control.

(1) A close inspection of all trucks entering or leaving a post should be required. An orderly system should be established to limit and control the movement of trucks and other conveyances within such areas. Where possible, loading and unloading platforms should be outside restricted areas. Sometimes, however, this is not possible. If not, turnaround areas for loading and unloading should be at, or as near to as possible, to the truck gates. This will help to eliminate theft by employees and truckers of items being loaded or unloaded.

(2) All trucks and conveyances entering a restricted area should be required to pass through a service gate manned by guards. Truck drivers, helpers, passengers, and vehicle contents should be carefully examined. The guard check at truck entrances should cover both incoming and outgoing trucks. They should also include the following:

(a) Appropriate entries on a truck register. This should include registration of truck, name of truck owner, and signatures of driver and helper. Also included should be a description of load and date/time of entrance/departure.

(b) Identification of driver and helper. This should include proof of employment by the company owning the truck or conveyance.

(c) A license check of the vehicle operator and his driver or helper.

(d) Examination of the truck or other conveyance, if feasible. The aim is detection of authorized items.

(3) Cards or badges should be issued to drivers and helpers who have been identified and registered. Such cards should permit only limited access to specific loading/unloading areas.

(4) Incoming trucks should be kept to the minimum essential for the efficient operation of the post, and escorts should be provided if vehicles are allowed access to restricted areas.

(5) Sometimes trucks carry loads that are impractical to examine. If so, door seals may be used by security personnel at the entrance gate. These seals will be opened by a security guard or designated representative at the receiving end. Likewise, the truck doors may be resealed for exit or other stops within the post.

(6) Loading and unloading operations should be strictly supervised by security personnel. This will assure that unauthorized materiel or persons do not enter or leave via trucks or other vehicles. Trash details working in restricted areas should be supervised by security personnel.

g. Railroad Car Control.

(1) The movement of railroad cars into and out of posts should be supervised, and the cars should be inspected. This will prevent the entry or removal of unauthorized personnel or materiel. Inspecting personnel should be very watchful for explosives and incendiaries.

(2) All railroad entrances in isolated areas should be controlled by locked gates when not in use. They should be under security personnel supervision when either unlocked or opened for passage of railroad cars.

(3) Railroad switching should be confined to daylight hours. Such is the case if this does not materially interfere with efficient operation of the post or facility.

(4) The numbers of the seals of all sealed railroad cars should be checked. This should occur immediately upon arrival at the post. Numbers should be checked against the list of seal numbers. This list should be requested from the shipper. Broken seals or seal numbers not in accordance with the list from the shipper warrant immediate investigation.

h. Maritime Control. Docks, piers, and quays should be separated from the main post by a fence and controlled gates. Passage to and from the area must be limited to authorized personnel. Sometimes the inspection of a vessel is necessary. This will prevent entry of unauthorized persons, cargos, or sabotage devices. Such inspections should be done by persons experienced in the intricacies of maritime construction. Aid may be sought from the Army Transportation Corps or Engineer Corps. Also, the US Coast Guard will aid in this inspection.

LESSON 1

PRACTICE EXERCISE

The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. The correct form to use for package and materiel control is which?

   A. DA Form 8181.
   B. DD Form 8181.
   C. DA Form 1818.
   D. DD Form 1818.

2. Which of the following areas is considered the most vulnerable for pilferage?

   A. Shipping and receiving.
   B. Trash channels.
   C. Empty containers.
   D. Warehouses.

3. When should you conduct spot checks?

   A. When packages are being brought into restricted areas without authorization.
   B. When 100 percent inspection is impossible for all out-going packages.
   C. At the close of the work day when personnel are leaving post.
   D. When vehicles are entering a limited access area.

4. What should be included in the guard orders at a truck entrance?

   A. Check cargo of a truck with no door seals.
   B. Check safety inspection decal on the right of the windshield.
   C. Check entries on truck register, including registration of truck.
   D. DIO contract authorization list maintained by the guard.

5. Certain procedures apply to railroad car control. Which of the following should be observed?

   A. Railroad entrances at isolated areas on post must be secured when not in use.
   B. Railroad car loading and unloading platforms should be outside restricted areas.
   C. Seals on cars must be broken only in the presence of security force personnel.
   D. Numbered seals should be available to expedite replacement of broken seals.

6. The DD Form 577 is used in the physical security environment. Why is this form used?

   A. To record inspection of all material, supplies, and equipment.
   B. To control movement of packages, materiels, and property.
   C. To verify the signature on forms such as DA Form 1818.
   D. For immediate identification of sensitive packages, materiel, and equipment.

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM		CORRECT ANSWER AND FEEDBACK
1.	C.	DA Form 1818. DA Form 1818 (Individual Property Pass) . . . (page 1-5, para a(5)).
2.	A.	Shipping and receiving. Shipping and receiving areas. (page 1-3, para 3a).
3.	B.	When 100 percent inspection is . . . When 100 percent inspection is impractical . . . (page 1-5, para a (3)).
4.	C.	Entries on truck register, including . . . Appropriate entries on a truck . . . (page 1-8, para f(2)(a)).
5.	A.	Railroad entrances at isolated areas . . . All railroad entrances in isolated . . . (page 1-9, para g(2)).
6.	C.	To verify the signature on forms . . . DD Form 577 (Signature Card) is used . . . (page 1-5, para a(4)).

LESSON 2

EVALUATE PHYSICAL SECURITY REQUIREMENTS FOR DATA PROCESSING FACILITIES AND LOGISTICAL SUPPORT ACTIVITIES

Critical Tasks: 191-386-0017
191-386-0022

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to evaluate and identify the physical security requirements for data processing facilities and logistical support activities.

TERMINAL LEARNING OBJECTIVE:

ACTION: Evaluate and provide recommendations for a physical security program.

CONDITION: You will have this subcourse, pencil, and paper.

STANDARD: You must take the final subcourse examination and earn a score of 70 percent.

REFERENCES: The material contained in this lesson was derived from the following publications: FM 19-30, AR 380-19, AR 190-13, and Physical Security Update 10-3.

INTRODUCTION

Many people associate periods in the past with major social, economical, political or technological development. Likewise, the 80's became famous for computer technology. Computers are used to store data; they are used in the development of advanced weapons systems. The DOD daily expands its dependency on microprocessing to accomplish its mission. Because of this, security for buildings that house data processing facilities is a growing concern. Not only is the data store a potential target for security threats, but corporate espionage is also a problem. This is the theft of computer technology, which has become a major international crime. You are a physical security manager or inspector. As such, you play a very large role in this complex dimension through security of Automated Information Systems (AIS) facilities.

PART A - AUTOMATED INFORMATION SYSTEMS FACILITIES

1. In planning for physical security, the security officer or inspector must know what must be protected. Generally, equipment, information, and

operational programs are housed together. With these, also are the processing main storage units and remote components. Security personnel should set up measures to survey the building housing the AIS facilities. This should be done before physical security measures are determined.

a. Building Design. New as well as existing structures must be evaluated. This is needed to determine accessibility by unauthorized persons in operations areas of a computer complex. Basement or below-ground level facilities require special design. These areas must be guarded against water damage. If possible, locate the equipment in the center of the building. This affords maximum protection and is away from other activities. Windows should be avoided to prevent forced entry problems.

b. Protective Measures. The degree of security required for computer complexes will depend on its accreditation level, location, environment, and vulnerability to security threats. Based on risk analysis done IAW AR 190-51 and DA Pam 190-51 personnel must determine the degree of protection required.

(1) Protective Barriers. A highly recommended room would be one room having four solidly built windowless walls. These would extend from the true floor to the true ceiling. Protective barriers to be considered include the following:

(a) Windows. Ground floor windows should be eliminated, if possible: Those windows deemed necessary will be protected by rod and bar grids, steel screens, or secure shutters. Mainframe rooms will not have windows.

(b) Doors. All doors to a central computer complex will be substantially constructed of solid-core wood or metal, and have a 1 and 1/2 hour fire rating. Hinges will be mounted on the inside, or if this is not possible, the hinge pins will be welded, pinned, or brazed to hinder removal. Doors, other than those used for primary access, will be secured from the inside and be devoid of external locking hardware. These doors will be equipped with appropriate hardware to permit rapid opening during fires or other emergencies.

(c) Fences. Fences may be used as a measure to provide the required dual level of protection. Fences will meet requirements of OCE Drawing 40-16-10, FE-6. Some existing fences are in good repair but do not meet this criteria. They do provide adequate security, however, with a 6-foot fabric. Such fences will not be replaced solely to comply with this requirement.

(2) Locking devices.

(a) Cylinder locks. Single doors, which are locked after duty hours, should be secured with a dead bolt having a 1-inch throw. Double doors should be secured using locking hardware devices. Also, locking hardware may be used if the facility is extremely vulnerable.

(b) Fences are often used around a complex or facility. If so, the entrance gates should be secured with an approved locking device.

(3) Protective lighting. Exterior of buildings housing computer facilities will have protective lighting. Such lighting will be installed for use during the hours of darkness.

(4) Security forces. All computer facilities should have a dedicated service provided. This service should be dependent upon the classification and sensitivity of data stored and processed. Military/security police would patrol the facility every few hours, or an on-site security force of two or three people might be provided.

(5) Personnel movement control: Recommended measures for personnel movement include the following:

(a) Use of a badge/pass system with an access control roster.

(b) Electrical release doors or cipher lock doors.

(c) A buffer zone to prevent accidental access into an area.

(d) Human control of access (such as a receptionist).

(6) Intrusion Detection System (IDS). Security personnel must keep in mind that IDSs are not delaying devices. They are detection systems. IDS should not be installed where they would hinder the operation of the facility, or cause a security hazard. Some areas are not compatible with certain types of sensors, or closed circuit television (CCTV). For instance, passive ultrasonic IDS sensors are similar to microphones and cannot be used where classified information is discussed. The use of CCTV cameras would not be advised if the guard monitoring the system could see the terminals on which classified or sensitive information is processed.

(a) Application.

(1) Use where computer facility is not manned 24 hours a day.

(2) Use where there is no dedicated guard.

(3) Use where there is no closed circuit television (CCTV).

(b) Locations.

(1) Main computer room.

(2) Mag tape/disk storage library.

(3) All other areas where sensitive information is stored.

(7) Power Source. Without electrical power a computer facility cannot operate. Protection of the power source is therefore a must. When possible, all commercial power into the facility will be conveyed by buried cables. Generators and fuel for them should be protected inside the fenced area of the computer facility. All efforts should be made in physical security planning to minimize the effects of power losses.

(8) Fire Protection. Fires are often used to sabotage strategic facilities. Computer facilities are highly vulnerable. This is due to the low temperature at which some equipment can be destroyed. Magnetic tape or disk tapes can be destroyed at 150 degrees Fahrenheit, which is quite low. All materials used in the construction of computer rooms on related facilities will have a National Fire Protection Association (NFPA), flame-spread rate of 25 or less. The following are items to consider in understanding a broad fire prevention program:

(a) Good housekeeping and operating procedures are prerequisites in maintaining a noncombustible environment.

(1) Smoking should not be allowed in a computer room.

(2) Trash containers should be made of fireproof material.

(3) Computer rooms should not be used to store paper stocks or magnetic tapes.

(b) Smoke/heat detectors minimize fire damage to ADP facilities by early detection. Systems should be capable of indicating areas of the room where a fire exists. Alarms should be tied into a local fire station or guard headquarters.

(1) Smoke sensor should be located in ceiling.

(2) Smoke and heat sensor should also be located in the subfloor area where all cables are located.

(c) Fire extinguishers must be carefully selected for computer rooms. In computer equipment rooms, a carbon dioxide or halon fire extinguisher of at least a 15-pound capacity will be on hand. This will be used for electrical fires. Chemical type extinguishers will be no further than 50 feet from equipment.

(d) Sprinkler systems should have a delay. This will permit inspection of the facility and/or evacuation before extinguishers are released. Installation should preclude unauthorized tampering; it should also preclude accidental deactivation. Protective covering can be used over equipment to reduce water damage in case of a fire.

(9) Water damage can be minimized or avoided if security personnel plan carefully. Plans should avoid locating computer rooms in basements. This area is vulnerable to flooding. Plumbing lines should not be routed

over, under, nor alongside a computer room in case lines burst. Buildings whose outer walls are glass should also be avoided.

2. Maintain Systems Integrity. Data stored in Army computer systems range from military payroll to top secret information. Because of this, it is important to maintain the system's integrity. It should be protected from threats such as espionage and sabotage. It is essential that security personnel are aware of security measures in this area.

a. Separate Primary and Backup Systems and Files. Most banking transactions are handled by computers. Have you ever wondered what would happen to your account, if your bank burned to the ground? Be assured that all would not be lost. All ADP facilities have alternate areas to run and process data. These facilities also maintain backup or alternate tape or diskette libraries. The same security should be given to the alternate systems and tape storage as a primary.

b. Supervise Maintenance Personnel. Computer maintenance on hardware is a continuing process. Knowledge and supervision of maintenance personnel is important. Technical experts can verify operations of maintenance personnel. Use of such experts will ensure that the system is not tampered with or sabotaged.

c. Protect Remote Keypunch Equipment. Keypunch equipment and locations should have physical security equal to the material being punched or prepared.

d. Strict Enforcement of All Security Measures. Secure handling of all sensitive and classified data should be stressed to everyone in the facility.

e. Direct Security Measures. Direct security protective measures toward the following:

(1) Data control areas.

(2) Access control (to data storage programs).

(3) Password control (for access into terminals).

3. Security Measures of Software. Security measures for software should be implemented. Software refers to programs and routines of computers. These security measures would include the following:

a. Security of Programs. Necessary precautions should be taken to ensure knowledge of who writes the programs. Where they are written and where they are tested and filed should also be known.

b. Data File Systems. Data file systems contain data that can be processed or produced by the computer. These files must be provided a degree of security equal to the importance of the files.

c. Documents. The document providing the historical reference record of data file systems and programs should be given the same degree of physical security as the computer terminals.

4. Procedures and Controls. Procedures and controls encompass the entire area of operation concerning the complex.

a. Separation of Duties. In most complexes personnel are divided into several functional groupings. It is not necessary or possible for these groupings to be separate and distinct in all facilities, but in large operations they should be grouped. The security classification of these personnel must be equal to the level of classification of the data or program that they are processing or developing. These functional groupings, in addition to the internal audit personnel and the security force, include the following:

(1) Programs.

(2) Operators.

(3) Librarians.

(4) Data preparers.

(5) Data controllers.

b. Rotation of Duties. This is sound personnel management and essential to control production data.

c. Production Schedules. All production work would be run according to the schedules, and all program development should be controlled separately. Production schedules should contain the following:

(1) Line authorizations.

(2) Time estimates.

(3) Data file and program library release memorandum.

(4) Data preparation and instructions.

(5) Output routing.

(6) Input/output checking guides.

5. Maintain Run Control Log. For sensitive operations, a console printer recording all data may be located remotely or in a secured part of the computer complex. Copies of these logs and all run control logs will be maintained for 90 days. This log contains detailed records of all:

a. Runs.

b. Errors.

c. Interruptions.

d. Restarts.

6. Conduct Operations Reviews. Sound management of a computer complex requires that actual performance schedules be compared to scheduled performance. Any variations should be noted, investigated, and explained. Production schedules and run control logs are essential input to this process.

7. Other Security Control Measures.

a. Input/Output Controls. Quality controls and checks on all input/output should be maintained. This should be done by a separate data control group. This is required, not just for control, but it is essential for detecting and correcting errors.

b. Program Change Control. Changes to procedure programs should occur only upon authorization. This should be verified by internal audit groups.

c. Master File Control. Master file changes should be made only by authorization, and they should be subject to an internal system of checks and balances.

d. Password Controls.

(1) A password is a protected word or string of characters. It identifies or authenticates a user, specific resource, or access type.

(2) All persons having access to the passwords used on such systems must be carefully taught about password sensitivity. They should know the meticulous care with which such critical data must be protected. They should be very aware of the individual's personal duty and obligation to help in safeguarding such passwords.

(3) Knowledge of the password must be tightly limited to a minimum number of persons. These must have a need to know. Limiting the number of people who know the password will ensure effective systems functioning.

(4) Whenever possible, initial issue of systems passwords will be made by direct personal contact. This will take place between the user and the automated data processing system security officer (ADPSSO).

(5) Single passwords will be issued only once, and they will be retired when the time limit on its use has expired. Passwords may also be retired when the user has been transferred or reassigned.

e. Auditing Support. Skilled and experienced audit personnel on the post may increase computer security. They can do so by taking part in the development and maintenance of standards and procedures.

f. File Protection Devices. Maximum use should be made of file protection devices and techniques. This will aid in preventing accidental or willful destruction of files.

g. Manual Operation Procedures. Systems design should include provisions for short-term manual operation. Such should be the case whenever possible in the event normal operations are disrupted.

h. Hardware Monitoring Prevention. Facilities should undergo a "tempest" or hardware emission test. This will determine if computer hardware is transmitting classified data which may be intercepted by hostile agents.

8. Evacuation and Contingency Plans. Every data processing facility security plan should include two types of plans. These are (1) provisions for emergency evacuation/destruction plans and (2) contingency plans. These should be provided in case something disrupts or destroys the facility.

a. Use evacuation planning to ensure effective action, if evacuation is required. Evacuation of complex may be due to fire, flood, bomb threat, or hostile action. These plans should include the following:

(1) Procedures for securing, and priority evacuation of, certain files.

(2) Procedures for destruction of hardware, software, and data files before evacuation.

b. Contingency planning is important in case everyday operation of the computer facility is disrupted or destroyed. Such planning should provide for continued operation with auxiliary power sources or alternate equipment.

PART B - LOGISTICAL SUPPORT ACTIVITIES

1. Every post has a logistical support activity. Examples are transportation warehouses, engineer yards, self-service stores, PDO, etc. Yet, these places are often neglected by our security people, because they are often "out of sight, out of mind." Also, there is not much regulatory guidance for security of these types of facilities. Planning protective measures from "the ground up" is a large, but often overlooked, aspect of an effective post physical security program. Certain elements should be planned for in advance at the "drawing board" rather than later as an afterthought. Location of storage areas on the post and the design of each facility must be considered. Planning will include the interior arrangement and installation of adequate protection measures. These would include locking devices, IDSs, fences and other barriers. Wall, floor, and ceiling construction as well as protective lighting would be included in planning. Using foresight in planning can conserve personnel by reduction of guards needed after a facility is in use. Physical security should be considered early in planning for new facilities. To ensure this, the provost marshal or security officer should serve on the planning board. Knowing what to look for at a facility and offering valuable

service makes security worthwhile. It also enhances our image. Mainly, it helps the Army save valuable resources.

a. Pilferable Items. Some items are identified with a pilferage code in the Army Master Data File (AMDF). These items signal a need for more intensive management practices. More security measures for protecting these items may also be necessary. COs and supervisors of supply and maintenance areas maintain stock record accounts of pilferage-coded items. These people will also do the following:

(1) Ensure all members of their groups handling such items are aware of their AMDF designation. Ensure they are aware of the increased risk for theft or illegal diversion. Be certain that members know any special local procedures for controlling and protecting these items.

(2) Cause pilferage-coded items to be partially inventoried at frequent intervals. The stock on-hand for each pilferage-coded line item will be inventoried once each quarter at least. Frequency of inventory should be based on prior loss experience. If no prior losses have occurred, lines should be selected for inventory at random. Substantial difference between stocks on-hand and record stocks will be investigated.

(3) Cause stock accounting records for pilferage-coded items to be periodically reviewed. Reviews should occur no less than monthly, and they should be done by an officer, NCO (E-7 or above), or civilian employee of equivalent grade. The reviewer should be thoroughly familiar with the documentation. He should be alert for inordinately high issues, receipts, or use rate compared to what might be expected. He should also be alert for bogus or modified entries, and entries that might be otherwise suspicious. Appropriate action should be taken to follow-up on suspicious entries.

(4) Take appropriate action to prevent any future unexplained losses if some have occurred. Actions might include the following:

(a) Setting up an informal log. Record in it all issues of pilferage-coded items not controlled by line item accountability.

(b) Segregating portable, pilferable items from other stock; storing them in a secure, separate container, room, or building with controlled access.

(c) Appointing a custodian to receive, account for, and issue all pilferage-coded items, particularly when these items are segregated from other stock.

2. Security In-Depth. Security of supplies and equipment is improved with the addition of certain measures. Each one that increases delay time for access to items or the likelihood of detecting a criminal improves security. Such in-depth security is provided by controlling access to and circulation on the installation such as:

a. Limit open gates to those necessary to conduct business.

b. Man open gates with MP or security police if available.

c. Issue controlled visitor passes to operators of privately owned vehicles without post decals.

d. Advise MP or security police of vehicle descriptions of suspicious operators or occupants.

e. Spot check by telephone persons, units, or offices that visitors claim they are going to visit.

f. Question persons who are obviously "out-of-place."

3. Military Police Working Dog Teams. MP working dog teams can be used effectively to improve post security and, in some cases, they can be used to save security personnel. Dogs offer dual security benefits: they are a psychological deterrence to trespassing; they enhance the ability of the security force to detect, pursue, and hold intruders. Patrol dogs are tolerant of human activity, and they can perform physical security as well as other law enforcement functions. They can also be used in mobile patrols to cover large areas. (See AR 190-12, AR 700-81, FM 19-35, and Physical Security Update 10-3 for more guidance.)

4. Recommended Security Measures. The following physical security measures are generally applicable for a logistical support facility. They are specific to no particular category of property. These measures are not required, but they are recommended if local conditions permit their use. The CO will determine those appropriate for his command.

a. Develop an end-of-day SOP for closing each office or activity.

b. Prohibit transportation of US Government property in a privately owned vehicle (POV). Sometimes this control measure is impossible. If so, require POV operators transporting such property to have appropriate papers. These should support possession of the property.

c. Limit to a single gate administrative truck traffic entering or exiting the post. Check, or spot check, nonmilitary trucks for authorization (delivery order, copy of contract) to enter the post. Check, or spot check, trucks leaving the post with military cargo. Drivers should have an authorization to transport the cargo.

d. Place seals on supply and equipment storage structures and enclosed vehicles opened once per week or less. Place seals on opening such as doors and windows.

e. Post appropriate signs at storage sites: e.g., "Off Limits to Unauthorized Personnel." (See paragraph 2-28, AR 420-70.)

f. Require the return of items issued to a person by the same individual.

g. Separate requisitioning and receiving functions. See that the same person(s) does not perform both.

h. Spot check military vehicle operators leaving the post. Spot check at various locations on the post for possession of an operator's license and valid dispatch.

i. Recrate and band items in original configuration until needed for operations. This should be done as soon as inspection of contents and receipt is complete.

j. Prohibit POV parking close to buildings and loading docks; parking should be at least 50 feet away.

k. Establish a good visitor control system; a sign-in/out register should be considered.

l. Trash removal should be monitored. Dumpster bins have been used, historically, to hide stolen items.

LESSON 2

PRACTICE EXERCISE

The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. You are making recommendations for fire protection security at a computer equipment room. Which one of the following would you correctly make?

A. Computer equipment is resistant to high temperatures; therefore, measures to protect it from water damage should be first priority.
B. Sprinkler systems should be set to activate immediately to prevent further damage.
C. Chemical type extinguishers will be no further than 50 feet from equipment.
D. Halon fire extinguishers should be used only in well ventilated areas, and only on electrical fires.

2. What should every data processing facility security plan include?

A. Criteria for evacuating hardware, software, and data files before destruction.
B. Contingency plans in case auxiliary power fails.
C. Procedures for securing, and priority evacuation of, certain files.
D. Designate persons authorized to remove sensitive files in emergencies.

3. What is the purpose of password controls?

A. Limit access to terminals.
B. Limit entry into main computer room.
C. Limit access to data processing equipment power source.
D. Verification of data processing system security officer.

4. Security personnel must maintain the Army computer system's integrity from espionage and sabotage. What should be done to maintain integrity?

A. Only personnel handling sensitive and classified data should know all security measures.
B. Separate primary and backup systems and files.
C. Maintain one area to run, process data, and store material and equipment.
D. Ensure that all personnel working in the data processing area have SECRET clearance.

5. Fences built to protect data processing facilities will be in accordance with which of the following?

   A. OCE Drawing 40-16-10, FE-6.
   B. AR 700-81.
   C. FM 19-130.
   D. AR Drawing 40-16-10, FE-6.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM		CORRECT ANSWER AND FEEDBACK
1.	C.	Chemical type extinguishers will be no further than . . . Chemical type extinguishers will be . . . (page 2-4, para 1 (8)(c)).
2.	C.	Procedures for securing, and priority evacuation . . . Procedures for securing, and . . . (page 2-8, para 8a (1)).
3.	A.	Limit access to terminals. A password is a protected word . . . (page 2-7, para d (1)).
4.	B.	Separate primary and backup systems from files. Separate primary and backup . . . (page 2-5, para 2a).
5.	A.	OCE Drawing 40-16-10, FE-6. Fences will meet requirements of . . . (page 2-2, para b (1)(c)).

LESSON 3

EVALUATE PHYSICAL SECURITY REQUIREMENTS FOR ARMS, AMMUNITION, AND EXPLOSIVES STORAGE/ARMS ROOMS

Critical Tasks: 191-386-0011

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to evaluate and identify the physical security requirements for arms, ammunition, and explosives storage/arms rooms.

TERMINAL LEARNING OBJECTIVE:

ACTION: Apply current physical security standards to arms, ammunition, and explosives storage areas.

CONDITION: You will have this subcourse, pencil, and paper.

STANDARD: You must take the final subcourse examination and earn a score of 70 percent.

REFERENCES: The material contained in this lesson was derived from the following publications: AR-190-11, AR 190-13, AR 710-2, DA Pam 710-2-1, AR 740-26, DOD 5100.76-M, and Physical Security Update 10-3.

INTRODUCTION

"The military must be able to respond immediately to national security threats. This ability depends largely upon the availability and functioning of arms, ammunition, and explosives (AA&E). These items are therefore of prime interest to the enemy. Sabotage or theft of such items would seriously cripple operational readiness. AA&E are items required and normally in short supply by terrorist and armed revolutionary groups. They will get AA&E by any means possible. This includes theft or illegal purchases. Policies, procedures, and standards must provide minimum security measures for such sensitive items. As the threat will vary depending on numerous factors, local commanders must supplement Department of the Army standards to meet local needs. Appendix A, at the end of this subcourse, lists terms useful in understanding applicable security measures in this area."

PART A - CATEGORIES OF ARMS, AMMUNITION, AND EXPLOSIVES

1. A uniform approach must be taken to the security and identification of sensitive AA&E. To ensure this, four categories have been established to identify the required degree of protection. Appendix B, at the end of this subcourse, identifies these categories. You should become familiar with them.

2. Deviations from the priorities shall be allowed only when local threats dictate.

3. Standards in AR 190-11 and DOD 5100.76-M are presented in this lesson. Waivers and exceptions of structural standards below these requirements may be approved, but only 10 percent deviation is allowed. COs of MACOMs have the authority of approval. Also, heads of Army staff agencies who command field agencies and activities have this authority.

4. Waivers and exceptions will be granted under the following provisions.

a. Blanket waivers and exceptions are unauthorized. Each case must be individually considered.

b. Compensatory measures in effect or recommended must be contained in each waiver request and must be in effect at the time of submission.

c. Waivers will be valid for up to 1 year.

d. Exceptions will be regarded as generally permanent; but, they must be reviewed at least every two years by the approving authority or the commander to whom the exception was granted.

PART B - SECURITY OF ARMS

1. Weapons.

a. Weapons shall be stored in an arms room or an arms storage building, unless operations dictate arms are to be stored or installed on vehicles or aircraft.

b. Once issued, weapons become the responsibility of the person issued to or in possession of the arms.

c. Structural standards for rooms and buildings used for arms storage must comply with those outlined in Appendix C, at the end of this subcourse.

d. Existing facilities shall be up-graded to meet the standards or provide equal protection as indicated in Appendix C, at the end of this subcourse.

2. Class 5 Containers.

a. Small storage racks in arms rooms or buildings are used to store weapons and ammunition. However, certain filing cabinets and class 5 containers may be used in place of these racks.

(1) Map and plan size, with combination lock, class 5, NSN 7110-00-931-0770, LIN H42724.

(2) Map and plan size, steel gray, with combination lock, without base, NSN 7110-00-068-7736, LIN H42737.

(3) Cap size, two drawer, with combination lock, gray, NSN 7110-00-082-6112, LIN H41655.

(4) Cap size, four drawer, with combination lock, gray, NSN 7110-00-082-6111, LIN H41659.

b. When storing category III arms, structural standards are considered met when the class 5 container is used. However, other factors, such as the requirement for guards or IDS, must be considered if overall security is to be reached. Consideration must be given to the vulnerability. Contents are sometimes left unattended for long periods. The location where the cabinet is to be placed is also important. The building and room in which the cabinet is to be placed must be carefully evaluated. Keep in mind the accessibility and ease of removal of the cabinet. Selection of a position for the cabinet should result in its being least vulnerable to unauthorized movement by heavy lifting equipment. The position should make it very hard for unauthorized persons to remove the cabinet.

3. Arms Racks and Containers.

a. All arms shall be stored in banded crates or containers or they shall be stored in standard issue, or locally made arms racks constructed to meet the standards listed in the Technical Data Package (TDP) and certified by the local facilities engineer.

b. Secondary padlocks shall be used to lock all arms racks or containers (See figure 3-1). These padlocks shall meet or exceed Military Specification P-17802.

c. Racks must be built so a weapon cannot be removed by partly disassembling either it or the rack.

d. Weapons racks and containers which weigh less than 500 pounds (empty weight) shall be fastened to the structure with bolts or chains equipped with secondary padlocks, or fastened together in groups totalling more than 500 pounds in weight. Chains used to secure racks will be of heavy duty, hardened, galvanized steel. Chains should be straight link and at least 5/16 inch diameter or of equal strength.

e. Racks having hinged locking bars will have the hinge pins welded. This will prevent easy removal.

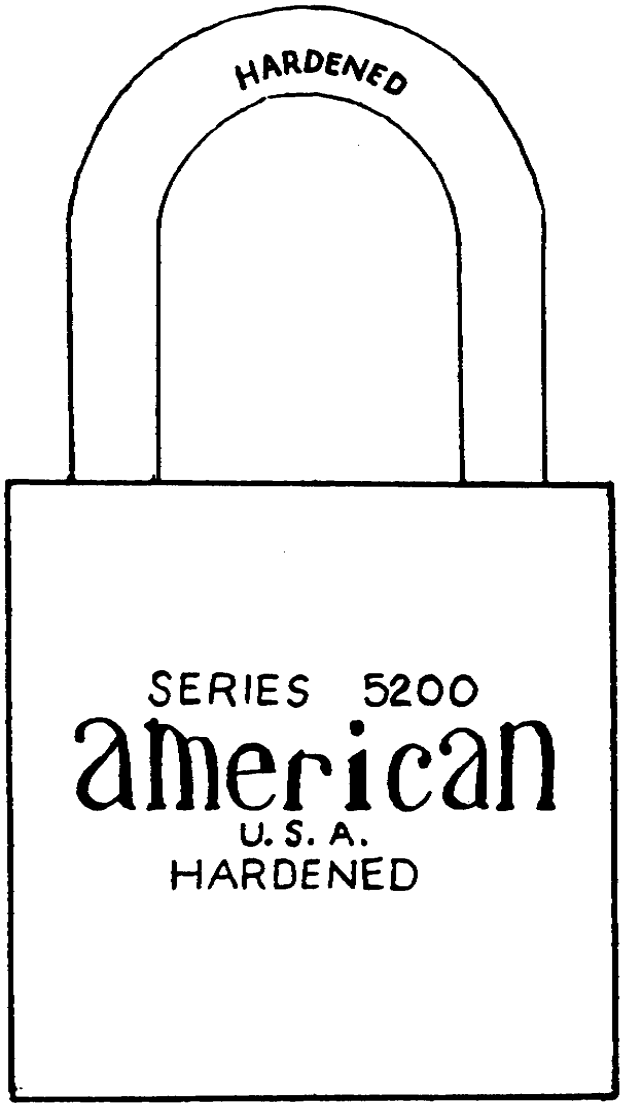


Figure 3-1. Approved secondary padlock.

NOTE: The Series 5200 (shown) and 200 (similar, not shown) are approved secondary padlocks utilized in AA&E storage facilities.

f. Some crew-served weapons and other weapons will not fit into issue racks or containers. These weapons will be secured in locally built containers. Locally fabricated containers/racks will be constructed in accordance with the technical data package (TDP). Commercially manufactured storage containers may be used.

4. Administrative Control Procedures.

a. Accountability.

(1) A physical count inventory of all weapons received will be conducted. This should take place immediately upon receipt of weapons at unit/activity level. At the same time, the serial numbers will be entered in unit and/or station property records. These records must be kept current at all times.

(2) All weapons not in bulk storage will be inventoried by physical count. A 100% serial number inventory will be conducted at least once each quarter. They will be inventoried by physical count each time responsibility for the custody of arms storage room keys is transferred. ARNG and USAR units will do a physical inventory monthly and a serial number inventory quarterly.

(3) Weapons in bulk or in depot storage will be inventoried at least once each fiscal year. They will be inventoried by quantity and type, based on a count of sealed containers.

(4) Written inventory records will be maintained in unit files for two years and then be destroyed. If there is a discrepancy in the records, these inventory records will be maintained for four years.

b. Unit issue and return procedures.

(1) Each person who is issued a weapon must be issued a DA Form 3749 (Weapons Receipt). This must be turned in to the arms room when the person draws his assigned weapon. At the time of issuance, he will enter the serial number of the weapon drawn and his signature on an issue sheet or log. The sheet or log will bear the date of the transaction. At the time of turn-in an entry will be made on the issue sheet or log indicating that the weapon was returned, the armorer (issuer) will sign or initial the entry, and the person's Weapons Receipt will be returned.

(2) Unit COs must establish written alternate procedures for the issue of weapons during emergencies or field exercises. Procedures should also include those times when operational necessity dictates a need for rapid issue of equipment.

5. Security Measures for Arms Rooms.

a. Lighting. Interior and exterior security lighting will be provided for all arms storage buildings. Such lighting will be provided in buildings having arms storage rooms. Motor pools, hangars, and outdoor parking areas for vehicle or aircraft with weapons stored on board must have such lighting.

(1) The lighting must be of enough intensity to afford guards excellent observation during the night. They should be able to immediately recognize illegal acts. Examples are breaking and entering or unauthorized removal of arms.

(2) Switches for exterior lighting will be installed so that they are not accessible to unauthorized persons.

b. Locks and Keys.

(1) All doors used for access to arms storage rooms will meet the requirements of AR 190-11 or DOD Manual 5100.76-M. If there are two doors on the arms storage room (on the same entrance or doorway), at least one of these will meet the requirements. The Security Construction Statement (DA Form 4604-R) will state which of these doors is the most secure. The most secure door will have a high-security hasp and high-security padlock installed on it. The other door will be secured with a secondary padlock or equivalent mortise cylinder lock. A Class V steel door may be used in lieu of other doors. Vehicles and facilities in which items are stored will be secured with locking devices specified in modification work orders (MWOs). Devices will not be designed and produced locally without special approval. The product manager, physical security equipment (PM-PSE), gives such approval.

(2) Keys to arms storage buildings, rooms, racks, and containers will be maintained separately from other keys. These will be accessible only to those persons whose official duties require access to them. A current roster of these persons will be kept within the unit, agency, or organization. The number of keys will be held to the minimum number essential. Custody of keys will be transferred between authorized persons after both parties have done a visual inventory of weapons. This should include total count of weapons on hand. The change of custody and visual inventory will be recorded. After duty hours, keys will be locked in a secure receptacle. This should be located away from the storage area. Keys may be left in the custody of the responsible duty officer/NCO or CQ. If the duty officer/NCO or CQ is not on the unaccompanied access roster for the arms storage area, they will sign for a sealed box of keys (sealed with a secondary padlock). This box of keys, if weighing less than 500 pounds, cannot be left unguarded unless it is fastened to the structure by using a chain and padlock meeting the same requirements as for weapons racks. At no time will keys be left unattended or unsecured. Keys to arms storage buildings, rooms, racks, and/or containers will not be removed from the post. The use of a master key system is prohibited. In the event of lost, misplaced, or stolen keys, affected locks or cores to locks will be replaced immediately. Replacement or reserve locks, cores, and keys will be well secured. This will preclude them from being readily accessible to unauthorized persons.

(3) Key control registers will contain the printed name and signature of the person receiving the key and the date/time of issuance. These registers will also contain the key number(s), printed name and signature of the person issuing the keys, and date/time key was returned. Also, the printed name and signature of the person receiving the returned key will be entered in the register.

(4) Padlocks will be locked to the staple or hasp when the area or container is open. This measure will preclude theft, loss, or substitution of the lock.

(5) Inventories of keys and locks will be conducted semiannually. This inventory will include the backup or second set of keys. Inventory records will be kept in unit files for one year, then destroyed.

c. Intrusion Detection Systems (IDS).

(1) IDS alarms are essential parts of the physical security system. These devices, however, are not a substitute for barrier protection and administrative control. The IDS shall be an approved DOD standardized system. One example is the Joint-Service Interior Intrusion Detection System (J-SIIDS). COs are responsible for ensuring that certain personnel have proper clearance. These are those persons who must install, maintain, or repair the system.

(2) All structures or containers storing category II and above AA&E will be protected by an IDS. This will hold true unless such structures or containers are continuously manned or under constant surveillance.

(3) Plans and specifications for installation of commercial IDSs must be forwarded through command channels.

(4) IDSs are sometimes used at arms storage rooms in civil communities. If so, arrangements will be made, if possible, to connect alarms to civil/campus police headquarters. From there immediate response can be directed in case of unauthorized entry.

(5) A daily log will be kept of all alarms received. This will include the nature of the alarm. Examples are intrusion, system failure, or false alarm. When appropriate, a copy of the log should be forwarded to the supporting engineer office. There the log will receive evaluation, and necessary maintenance will be ordered.

(6) Transmission lines for the alarm circuits must be electronically supervised. This will preclude tampering. Lines must also be inspected often by guard personnel. A protected backup power supply should be approved.

d. Security of tools and high value items.

(1) Tools located in the vicinity of arms storage areas will be secured in a locked container, and they will be removed from the vicinity of that building or room. Sometimes an arms storage facility is the only secure location available. If so, such tools will be stored there within a locked container. Other times the access door to an arms room is located within the unit supply room. If so, tools will not be stored in the supply room. Examples of such tools are hammers, bolt cutters, chisels, crowbars, and similar items. These would aid in gaining forced entry.

(2) Other secure storage facilities are often reasonably available. If so, high value items other than weapons and limited amounts of ammunition will not be stored in the arms room. Examples of such items are field glasses, compasses, watches, and other high value things subject to pilferage.

It sometimes happens that there is an absence of secure facilities mentioned above. If so, unit commanders may grant special authority. They may authorize sensitive items, other than weapons and ammunition, to be stored in arms storage facilities.

e. Restricted Area Posting.

(1) All areas in which AA&E are stored will be designated and posted as a restricted area. This will be done in accordance with AR 190-13. Posting will include fire control measures and symbols. In overseas commands, the areas must be posted in English and the language of the host country.

(2) Signs will be displayed on all arms storage facilities using IDSs. These signs will prominently announce the presence of such systems. Signs will be metal, as described at Appendix D, and they will be affixed at eye level, wherever possible. They will be placed on the exterior of each wall which contains an entrance to the arms storage room, vault, building, or magazine.

f. Fences and Associated Barriers. Certain areas will be enclosed with fences which meet the requirements listed below. These areas are arms storage buildings and outside areas where aircraft or vehicles are parked with weapons aboard.

(1) Fabric. Fence fabric shall be of chain link (galvanized, aluminized, or plastic-coated woven steel) 2 inch square mesh, 9-gauge diameter wire. Fencing used in Europe may conform to NATO Standard Designed Fencing. Specifications for NATO fencing shall be 2.5-3mm gauge, 76mm grid opening, 2 meter height, and 3.176 meter post separation.

(2) Mounting. Post, bracings and other structure members will be located on the inside of the fence fabric. Fence Fabric shall be secured to posts and other structural members. Galvanized steel or aluminum tie-wires equal in gauge will be used to secure the fencing.

(3) Height. The minimum height of the fence shall be 6 feet.

(4) Anchoring. The bottom of the fence fabric will extend to within 2 inches of firm ground. This will prevent intruders from lifting the fabric to gain access. Sometimes surface stabilization is not possible. This may be due to loose sand or shifting soils. If so, concrete curbs, sills, or other anchoring devices, extending below ground level, shall be provided.

(5) Modification to Existing Fencing. Existing Fencing may provide an equivalent or greater penetration resistance. If so, changes to existing chain link fencing shall not be made to conform to the above requirements.

(6) Barrier Openings.

(a) A minimum number of vehicular and pedestrian gates shall be established for barriers. The number should be based on operational

requirements. Gates shall be structurally comparable to the adjacent fence. They shall be designed to allow traffic to pass through under positive control of the security force. A lock approved by the DOD Component shall be used on gates not continuously manned. Hinge pins and hardware shall be welded or otherwise secured to prevent removal.

(b) Drainage structures and water passages penetrating the barrier will be barred. This will cause obstacles for unauthorized entry. Such obstacles will be equal to the fence itself. Some openings to drainage structures measure more than 96 square inches: they may have a smaller dimension greater than 6 inches. Multiple pipes each having a diameter of 10 inches or less may be joined together. These may then be joined to the drainage culvert and used as an alternative. Multiple pipes of this diameter may also be placed and secured in the "in-flow" end of the drainage culvert. This will also prevent intrusion into the area.

(c) Building walls may be incorporated into the barrier system. However, they must offer protection against intrusion equal to that of the perimeter barrier, and they must be subject to observation. The walls must have a minimum height of 7 ft, with a barbed wire top guard sloped outward at a 45 degree angle.

g. Clear Zone. Clear zones shall extend 12 feet on the outside and 30 feet on the inside of the perimeter fence. Clear zones shall be free of all obstacles. They shall be free of anything that could provide cover for an intruder, or anything that could reduce the effectiveness of the physical barrier. Examples are topographical features, such as hills, and vegetation more than 8 inches in height.

h. Access Control.

(1) Routine/unaccompanied access to arms storage facilities will be limited to the least number of persons designated by the unit CO. Personnel may be military or civilian. Names and duty positions of these persons will be posted inside the arms room. They will be authorized unaccompanied access to arms only after they have passed a command-developed background check or local files check. These checks will be done by the area provost marshal, local civilian police, and other agencies which might have pertinent data on file. Pertinent data is that which would reflect on the honesty or stability of the person. Supplemental checks will be done every 3 years after assignment of new personnel. COs will prohibit any persons on whom derogatory information is revealed from unaccompanied access to the arms storage facility. Also, COs will relieve such personnel of those duties for which unaccompanied access is required.

(2) A two-person rule security system may be used to control access to all arms rooms and arms storage buildings. Two authorized persons will be present during any operation which affords access to these facilities. These two persons will be considered present when they are in a physical position to positively detect incorrect or unauthorized procedures. Such procedures are those related to the task and/or operation being performed. Persons

designated unaccompanied access are exempt from the two person requirement, and they are not required to be present when a facility is entered. COs must establish internal lock and key control procedures. This will preclude defeat of the two-man rule.

PART C - INDIVIDUAL WEAPON SECURITY

1. Individual weapons used for training, operations, or any other reason, will be carried at all times on the person of the individual to whom issued. Except during emergencies, e.g., field evacuation, weapons will not be given to the charge of any other person.

2. During field exercises and training, pistols and revolvers are often issued to individuals. Such arms should be secured to the person by means of a locally made lanyard. Military issue field lanyards will be used when they are available.

a. Pistols or revolvers sometimes lack a device to affix the lanyard. If so, these arms will be secured by running the lanyard through the pistol trigger guard. This can be done during field and training exercises, where drawing the pistol is not contemplated. If drawing the pistol is contemplated, such pistols are exempt from the lanyard requirement.

b. Pistols and revolvers issued for operational purposes need not be secured by a lanyard.

c. Local COs will prescribe specific security measures to preclude the loss of other assigned weapons.

PART D - SECURITY OF AMMUNITION AND EXPLOSIVES

1. Magazines, igloos, or facilities used to store ammunition or explosives will meet the same requirements as established for small arms storage rooms. See Appendix C and Standards in AR 385-64, para. 3-1a, b, c, e, f, and g.

2. Active Army unit Commanders (CO) and Reserve Component (RC) and ROTC unit COs may approve storage of small amounts of ammunition in unit arms rooms. Storage of such items must be limited to meet operational requirements. Items will be stored in separate, locked containers.

3. Ammunition stored in the unit arms room will be inventoried at the same time as the serial number inventory of weapons. Ammunition will be inventoried by physical count, type (i.e., 7.62mm linked, etc.), Lot number, and DODIC number. The DODIC number can be found in DA Pam 710-2-1, and identifies the ammunition by how it is configured. 7.62mm (M-60/M-14 ammo) comes in several different types, such as ball, tracer, or armor piercing, or a combination of these types. If the container it was shipped in has been opened, the cartridge headstamp number must be used instead of the lot number. Ammunition assigned in the property records of a unit will be inventoried monthly. During inventory, all loose ammunition and/or that not in banded containers will be physically counted. Banded containers or ammunition will

be counted by container, and they will be inspected to assure that bands and seals are intact. All inventories will be recorded.

4. Ammunition is sometimes authorized for retention in unit arms storage rooms. Such ammunition will be stored in a locked, locally built container. It will be built of at least 22 gauge steel, or the container may be commercially manufactured. These containers shall be made of at least 22 gauge steel. A locked, class 5 container may also be used.

5. Containers will be locked with secondary padlocks or equivalent when not in use. They will be fastened securely to the walls or floor of the arms room. This measure will prevent unauthorized removal.

6. Chains of the same type used to secure arms racks will be used to secure ammunition containers.

PART E - ACTION IN THE EVENT OF MISSING OR RECOVERED FIREARMS, AMMUNITION, AND EXPLOSIVES

AA&E are sometimes lost stolen, illegally disposed of or recovered. When this occurs, those directly responsible for the property will act immediately. These persons may be the COs or their representatives. They will notify the supporting provost marshal or security officer. All known facts should be presented, so that an investigation may begin.

LESSON 3

PRACTICE EXERCISE

The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. You have a small activity complex which your security force is responsible for. It is 65 miles from your depot, so it is not feasible for the security guards at the complex to turn their weapons into the arms room at the main depot. To solve this problem, what would you do?

   A. Let the guard sign for them and take them home after duty hours.
   B. Turn them in for safekeeping to the local police station after each shift.
   C. Requisition the appropriate class 5 container in which to keep the weapons.
   D. Have a patrol pick up the weapons at the complex at the beginning and end of each shift.

2. Restricted area posting will be in accordance with what regulation?

   A. AR 190-13.
   B. AR 320-10.
   C. AR 600-200.
   D. AR 380-5.

3. Routine unaccompanied access by military or civilian personnel to arms storage facilities will be:

   A. Applied to everybody that is assigned to the unit.
   B. Applied to only those personnel with a need to know.
   C. Limited to the least number of responsible personnel designated by the unit CO.
   D. Limited to only the unit CO and battalion S4 officer.

4. All arms racks must be locked with what?

   A. A high security padlock.
   B. Both a high security padlock and a high security hasp.
   C. Any padlock with a case hardened shackle.
   D. Approved secondary padlocks.

5. While inspecting your arms storage room, you notice that the M16 racks are not secured to the wall or floor. From your previous study, you know that chains can be used for this purpose, and that the chains must also what?

A. Be secured with a high security padlock.
B. Be of heavy duty hardened steel chain, welded, straight link, galvanized, at least 5/16-inch thick.
C. Same as b above, except the chain must be 5/8-inch thick.
D. Be of the heavy duty hardened steel chain, tested at least .62 on the RC scale, and locked with a high security padlock.

6. You are considering interior and exterior lighting for your arms room. You know that regulations require which of the following?

A. Lighting should be of such intensity that guards can detect illegal acts of penetration during hours of darkness.
B. Floodlights are located on all sides of the building.
C. All arms room light bulbs (interior and exterior) should be covered with a globe.
D. Protective lighting wire should be protected with steel conduit.

LESSON 3

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM		CORRECT ANSWER AND FEEDBACK
1.	C.	Requisition the appropriate class 5 container in . . . However, certain filing cabinets and . . . (page 3-3, para 2a).
2.	A.	AR 190-13. This will be done in accordance with . . . (page 3-8, para e(1)).
3.	C.	Limited to the least number of responsible personnel . . . Routine/unaccompanied access to arms storage . . . (page 3-9, para h(1).
4.	D.	Approved secondary padlocks. Secondary padlocks shall be used to lock . . . (page 3-3, para 3b).
5.	B.	Be of heavy duty hardened steel chain . . . Chains used to secure racks will be of . . . (page 3-3, para 3d).
6.	A.	Lighting should be of such intensity that guards can . . . The lighting must be of enough intensity . . . (page, 3-5, para 5a(1)).

LESSON 4

DETERMINE PHYSICAL SECURITY STANDARDS FOR MEDICAL STORAGE AREAS AND FUND HANDLING ACTIVITIES

Critical Tasks: 191-386-0014

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to determine physical security standards for medical storage areas and fund handling activities.

TERMINAL LEARNING OBJECTIVE:

ACTION: Develop a physical security program for a medical storage area and for fund handling activities.

CONDITION: You will have this subcourse, pencil, and paper.

STANDARD: You must take the final subcourse examination and earn a score of 70 percent.

REFERENCES: The material contained in this lesson was derived from the following publications: FM 19-30, AR 40-2, AR 40-61, AR 30-1, AR 37-103, AR 60-10, AR 190-51, and DA Pam 190-5-1.

INTRODUCTION

1. The Health Services Command (HSC) is a major command of the DA. The HSC provides health care services to authorized persons and medical training for personnel. The command also provides security protection measures for mission accomplishment. Area security provided includes post hospitals, medical centers (MEDCENs) and medical department activities (MEDDAC). Clinics, dispensaries and special mission activities on post are also included.

2. Security measures for medical facilities prevents pilferage. Such measures also provide security for sensitive items, equipment, and supplies. Activities that must be considered under each MEDCEN or MEDDAC include the following:

(1) Dental activities.

(2) Veterinary activities.

(3) Community mental health activities.

(4) Health and environment activities.

(5) Medical center hospital.

(6) Medical warehouse storage facilities.

PART A - ESTABLISHING SECURITY MEASURES FOR MEDICAL FACILITIES

1. Physical Measures.

a. Circulation Control. Some movement control within medical facilities requires security planning. Employees, visitors, and patients must be covered. Each group requires special control techniques.

b. Security Lighting.

(1) Security lighting can be routinely used:

(a) Within medical treatment facilities.

(b) Adjacent to medical treatment facilities.

(c) Along all well-traveled foot paths, where possible.

(2) Special use of security lighting:

(a) Prevents/reduces crime.

(b) Prevents/reduces vehicular and pedestrian accidents.

(c) Assists in emergency activities.

(d) Accommodates nighttime circulation pattern or vice versa.

(e) Illuminates entrances to critical or sensitive areas, and other access points.

c. Lock and Key Control. A lock and key control system identifies locks and their locations. The system also identifies personnel in possession of keys and/or combinations.

(1) All keys and combinations to controlled, medical sensitive items and precious metals will be issued to only certain persons. These are those persons authorized access to those items. Personnel having access should be kept to a minimum. Containers will only be unlocked when items are removed or inert. Containers may be unlocked only when under enough control or observation of designated personnel to prevent unauthorized entry/use.

(2) Special Form 700 relates to Classified Container Information. This form will be used and posted near all combination locks. Names of individuals authorized access to the container will be identified thereon.

(3) Locks or combinations will be changed when loss or compromise is suspected, every 12 months, or when personnel with access leave, whichever is sooner.

(4) DA Form 702 is the Safe or Cabinet Security Record. This will be used to record the times that devices are opened, locked, and checked.

(5) Combination and key control records will be protected as "FOR OFFICIAL USE ONLY" information.

(6) Unissued keys to storage areas for controlled substances and sensitive items will be stored in an approved safe. This safe will be secured to the structure and away from storage areas.

(7) All keys will be signed in and out on a key register. After duty hours, keys, including IDS keys, will be locked in a container. This will be made of at least 20 gauge steel or material of equivalent strength, and it will be stored away from the storage area or in the custody of the responsible duty officer, NCO, or CQ. At no time will keys be left unattended or unsecured.

(8) The use of a master key system is prohibited.

d. Intrusion Detection System (IDS). IDSs must provide at least two types of sensors as a means of alarm annunciation at the MP station or guard force agency. From either place an armed response can be immediately dispatched.

e. Personnel Screening. Army policy forbids the assignment of personnel with any history of drug abuse to MOS 91Q, Pharmacy Specialist. Personnel holding this MOS are involved in the receipt, storage, and processing of controlled substances. They are also involved with the manufacture, transportation, preparation, and dispensing of controlled substances. Civilians must have, at a minimum, a local military and civilian records check and an NCIC check. Such checks must be done before assignment to a medical facility.

f. Materiel Control.

(1) Some medical materials require special security and accountability. They are as follows:

(a) Controlled substances.

(b) Stored hospital linens.

(c) Expensive medical equipment.

(d) Money and valuables.

(e) Medical sensitive items.

(2) Sensitive and accountable items should be stored away from the mainstream of heavy foot traffic to aid in detecting removal.

(3) A controlled medical substance is a drug or other substance, or its immediate precursor, listed in current schedules of 21 USC 812 in medical facilities. Such substances are used for treatment, therapy, or research. Categories listed in this section are as follows:

(a) Narcotics.

(b) Amphetamines.

(c) Barbiturates.

(d) Hallucinogens.

(4) Medically sensitive items are standard or nonstandard medical items. They are considered by medical COs to be sensitive enough to warrant some physical security in storage. Needles and syringes are examples.

(5) Controlled medical items are assigned letter designation in the Federal Supply Catalog, Nonstandard Drug Enforcement Administration Schedule III, IV, and V. Controlled substances denote specific categories which are as follows:

(a) Note R Controlled Medical Items. These are drugs having a high abuse potential with severe psychic or physical dependence liability; they are identified as Schedule II controlled substances.

(b) Note Q Controlled Medical Items. These are drugs having an abuse potential less than Note R substances; they are identified as Schedule III, IV, and V controlled substances.

(c) Note C Controlled Medical Items. Sets, kits, and outfits containing one or more components of Note R or Q items.

(6) Structural Standards.

(a) Provide controlled access protection to Note R items. These should be stored in an approved safe or vault, and they should be secured with a Class V vault door, as follows:

(1) Store small quantities of controlled medical substances in an approved safe.

(2) Ensure minimum structural standards for a vault in a new facility.

(a) Walls, floor, and ceiling will have at least 8 inches of concrete. This will be reinforced vertically and horizontally on each face with 1/2 inch diameter bars placed 9 inches on center.

(b) The vault may be required to remain open for frequent access. If so, it must have a self-closing and self-locking "day gate" or its equivalent. A day gate is not needed if the vault is not opened often, and it is relocked immediately after use.

(b) At an existing facility where it is not possible to construct the type vault described above, select a storage site as follows.

(1) The room or building should have walls made of masonry. They should extend from floor to ceiling with reinforced concrete ceiling and floor. If this is not possible, the structure should be built of wood and made as sound as possible. The inside will have the walls, floors, and ceiling lined with 1 inch thick lumber or 1/2 inch plywood. Steel mesh will be affixed, and smooth-headed bolts or rivets will be peened on the inside. This will prevent removal from the outside.

(2) Limit the number of windows to as few as possible. Block up all other windows if you can. Protect the remaining windows with steel mesh or bars. These must be welded to a steel channel frame and fastened to the building by smooth-headed bolts imbedded in the structure.

(3) Limit doors. If a vault-type door is not used, the entrance will be a two-door back-to-back system. Build the outer door of solid wood at least 1 3/4 inch thick. This door will be covered with a sheet of steel, not less than 1/16 inch thick (16 gauge USS). Build the inner door of steel bars welded to a grid, with openings that do not exceed 32 square inches; or you may use a solid wood door with the same particulars as the outer door. Install door hinges so that it will not be possible to remove the closed doors without greatly damaging the door frame. Spot weld hinge pins to prevent removal. Secure the outer door with a high security lock and hasp. Secure the inner door with an approved secondary padlock, a combination lock, and hasp.

(c) Store Note Q items under the same criteria as Note R items. The dual back-to-back door protection may be ignored provided the entrance door is solid wood. Also, it must be a minimum of 1 3/4 inches thick and covered with a sheet of steel not less than 1/16 inch thick. Secure the door with a high security padlock and hasp and hang on security-type hinges.

(d) Store Note C chests, kits, outfits under guidance outlined above for Note R and Q items.

2. Special Handling Procedures.

a. Drugs. As noted before, drugs and controlled medical items are assigned letter designators, and the degree of physical security depends on the category. AR 190-51, Chapter #4, provides minimum guidance for handling controlled substances. Some general measures applicable to handling such items include the following:

(1) Pharmacies will be designated as limited access areas. Note R and Q items will be positioned out of sight of the public during operating hours.

(2) Storage containers for controlled items will be unlocked only when property is removed.

(3) Unit dose carts containing medication will be kept in limited access areas when not in use.

(4) Unit dose carts will be kept under physical control or in clear view by authorized personnel while medications are being given.

b. Radioactive Material. Radioactive material is hazardous, and unauthorized tampering and theft may endanger a community. To avoid unauthorized access, the guidelines listed below should be followed.

(1) Storage areas for radioactive material must have a controlled access.

(2) Establish an ID system for authorized personnel.

(3) All first floor windows and exterior openings must be sealed, or they must have bars or steel mesh affixed. Doors must be reinforced or eliminated.

(4) A strictly controlled lock and key system will be implemented, and the number of persons authorized to use keys will be limited.

(5) Interior and exterior security lighting should be used.

(6) Security personnel working in health care facilities should be trained in the hazards and potential hazards of radioactive materials. They should also be trained in the safety and emergency actions involved.

3. Special Consideration.

a. Security of Designated Persons (VIPs).

(1) AR 40-3 outlines DA policies and procedures for the medical care of foreign dignitaries. The regulation also covers such care for important US government personnel.

(2) CID has primary responsibility for VIP security, and MP assets are used mostly in a support capacity.

(3) VIP security must be of the low profile-type. Generally, it should be carried out in a separate location where possible.

(4) The MEDCEN/MEDDAC security officer advises project officers in VIP operations on vulnerabilities of the hospital.

b. Patients are often admitted to a medical care facility for inpatient care. They should have a tamperproof, nontransferable band placed on either wrist for ID purposes. Patient movement control is restricted in order to provide necessary medical care. Their movement is also controlled to preclude access to unauthorized areas. Policies should define areas of free access to unescorted inpatients. Such areas may be reading rooms or visitors' lounges. Inpatients must be offered a place where valuables can be safely stored.

c. Outpatients may be required to disrobe for examinations or testing. They should be given a place for securing their valuables. X-ray departments, for example, usually have a large number of people to leave valuables during X-ray sessions. It may not be possible to provide security lockers. If this is the case, staff must be alert and provide security of valuables.

d. Visitors are normally restricted by time and location. Many areas in the MEDCEN/MEDDAC must have restricted access. These would preclude visitor access. When possible administrators should consider routing visitor traffic to patient rooms. This will avoid visitors entering secured areas. Directional signs should be posted. This will help prevent visitors being lost and crossing unauthorized areas. For greatest effectiveness, visiting hours must be properly enforced. Visitor's passes are also desirable security measures for identifying those persons authorized in a certain area.

e. Employees at medical facilities may be extended similar restrictions as visitors when entering areas with controlled access. The pharmacy is one area. Here drugs or controlled substances are handled. All employees should not have access to these. Medical personnel may be required to wear ID cards, tags, or badges. Lockers or like means of security should be provided for the staff.

f. Staff and visitor parking should be well lit. These areas should be given police protection for shift changes during the hours of darkness.

g. Hospitalized Prisoners. Medical care and treatment of the hospitalized prisoners is common. COs of medical facilities must designate an area within the hospital for this treatment. Parolees, minimum and medium custody prisoners do not require armed guards, but they must be closely supervised by specific hospital staff. Maximum custody prisoners in hospitals require guards at all times. Whenever possible, these guards should be provided by the prisoner's parent unit rather than the post PM. Unarmed guards may be used on other than maximum custody prisoners, if the confinement facility CO decides the circumstances warrant.

4. Security Awareness Considering Medical Records.

a. Medical records are documents with information about findings, diagnosis, or therapy recorded by or for the physician or dentist. Outpatient treatment records, health records, and x-rays are medical records, also. The data contained in these records are classified as "private," since it is of concern only to the patient and his physician.

b. Medical records must be secured to prevent access by unauthorized persons. Security of medical records must include the following:

(1) Area must be designated as a controlled access area.

(2) Key and lock controls must be implemented.

(3) Interior and exterior lighting must be used.

(4) If record storage area is on the first floor, windows must be covered with bars, steel mesh, and doors must be reinforced.

5. Security of Emergency Treatment Facilities.

a. Emergency rooms are areas plagued with a lot of pedestrian traffic. This presents special security problems. Supplies and equipment must be readily available, but at the same time, they must provide minimum access to unauthorized persons. Crash carts and emergency trays having controlled substances will be kept to a minimum; they will be secured to the greatest extent possible so as not to interfere with necessary operating procedures. Emergency rooms are often the first place victims of crimes will come when they need medical attention. MP may be posted at or near the emergency room. There are several advantages in providing law enforcement personnel in this area. Disruption is minimized and controlled; assistance to victim and family is available; police investigations and initial paperwork and reports are expedited; and visitors and the news media, who may disrupt procedures, can be controlled.

b. The Emergency Operations Center (EOC) must be considered in physical security planning. This is because it is the center of any health care efforts during a disaster or emergency. As such, the EOC must be protected.

c. Emergency treatment facilities depend upon utility services. Therefore, water, natural gas, fuel, oil and electricity must be integrated into plans for emergency protection. Heating, air conditioning, and telephone services must also be included.

PART B - FUND-HANDLING ACTIVITIES

Fund handling activities will always remain likely targets for criminals. This is due to the ease with which certain supplies can be black marketed and money circulated. Private industries have one primary interest--profit. Management realizes that petty theft causes the loss of billions of dollars each year. Industry must find a means of compensating for such losses. To do so, they build into the cost of goods and services an added percentage to cover losses. The government is not a profit making business. Taxpayers assume the loss for funds and merchandise. Every effort possible should be extended to minimize these losses. This is possible by establishing physical security requirements for fund-handling activities.

1. Identification of Fund-Handling Activities. A security program should emphasize prevention of losses. This should be the goal in planning for the protection of assets of fund-handling activities. These activities include the following:

a. Bank.

b. Finance and accounting office.

c. Post exchange.

(1) Main exchange.

(2) Annexes.

(3) Concessions.

(4) Snack bars.

(5) Movie theaters.

(6) Bowling alleys.

d. Commissary.

e. Credit union.

f. Clubs.

g. Dining facilities.

h. Post office.

i. Class VI sales stores.

j. Recreation services.

(1) Ceramic shop.

(2) Auto craft shop.

(3) Golf course.

(4) Recreational equipment rental.

(5) Fish and game skeet range.

k. Clothing sales.

l. Property disposal activities.

2. Banking Facilities.

a. Banking facilities located on military posts are encouraged to use intrusion detection and duress alarm systems. These systems should be monitored at security police headquarters.

b. During nonoperational periods, the MP or DOD civilian security police force will check the banking facility at least every two hours. Care must be taken to avoid the same routine or time interval for checking the facility.

3. Finance and Accounting. Security measures for finance and accounting offices should ensure adequate provisions for the following:

a. Vaults and Safes. Unauthorized personnel should not have access to these areas at any time. Whenever vaults or safes are opened, care must be taken. Combinations must be protected from observation.

b. Cash Control. Cash in excess of operation needs should be promptly deposited.

c. Windows and Doors. Points of entry such as windows and doors should be secured by locks or bars at all times after business hours.

d. Keys. Keys for the locking devices of the meter and protective unit of check-signing machines are kept in the custody of the finance and accounting officer at all times. Keys may also be kept in the custody of an authorized deputy.

e. Internal Office Procedures. Procedures must be set up to adequately control all undelivered and returned checks. Such control must also be provided a central point for receipt, holding, and final disposition of checks. Responsibility for these checks must be charged to a specific person.

4. Credit Union.

a. Internal physical security devices, such as an IDS, are provided by credit union management.

b. Post COs may make suggestions as to safeguarding funds.

c. Inadequate protective measures should be reported by the CO to the National Credit Union Administration.

5. Post Exchange.

a. Management determines the security measures to be used in Army and Air Force Exchange Service (AAFES).

b. AAFES alarm systems will be tested at least once weekly.

6. Commissary.

a. Controlled access is one means of providing security for commissaries. Areas to which access should be controlled are as follows:

(1) Parking areas for incoming shipments of food items. Shipments may be by rail, motor transportation, air, etc.

(2) On/off loading areas. This includes areas in the direction of travel to specific points within a warehouse or to sales outlets.

(3) Entrances. Entrances to areas should be located so supervisory personnel can watch entry and exit.

(4) Guard rails. Guard rails could be established. These would serve to channel personnel entering through one designated central point.

b. Identification system. An ID system must be established. It should provide positive identification of patrons prior to shopping.

c. Cash limits. The amount of cash in the change fund for each cash register should not exceed $150. (This amount has been established by Troop Support Agency).

d. Opening and closing procedures. SOPs should provide detailed operating procedures for opening and closing the activity.

7. Escorting Public Funds. Escort service protects both funds and the person being escorted. These duties performed by the MP should be of the highest standards.

8. Security Measures.

a. Avoid escorting at the same time.

b. Refrain from using the same route.

c. Vary direction of approach to pickup and delivery points.

d. Avoid using the same entrance/exit to the building for pickup and delivery.

9. Coordination of Escort Action. Activities transporting funds will stay in contact with the security police desk sergeant. They should advise him of departure time, route, and approximate arrival time. Contact should also be made when the escort is completed.

a. Coordinating the pickup and delivery time of courier personnel will reduce complacency.

b. Coordination should be maintained with the fund facility manager. He should furnish the name, information, and pictures of courier personnel. This will aid in identification and will expedite escort procedures at pickup points.

c. Request employees working at pickup and delivery points to observe escort arrivals and departures. Employees should do this while maintaining telephonic contact with the MP station.

10. Escorts.

a. Consolidate fund escort schedules. This should be done to the fullest extent possible.

b. Fund activities requiring security police escort will ascertain the name(s) of the patrolman (men) sent. Before initiating the escort, the patrolman (men) will be identified by the custodian.

c. Appropriated and nonappropriated funds in excess of $1,000 will be escorted by armed military guards, MP, or DOD guards. Escort will be furnished to and from banks on or off post. This service may include credit unions.

d. Funds in the amount of $500 or less may be transported by the fund activity without an escort.

e. Funds in amounts of $501 to $1,000 will be transported by the fund activity; however, an unarmed escort will accompany the person carrying the funds.

f. Funds in amounts of $1,001 to $10,000 will require one security police escort.

g. Funds in excess of $10,000 will require two security police escorts.

LESSON 4

PRACTICE EXERCISE

The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. During after duty hours, keys to the IDS in medical facilities--

   A. will be kept by the duty officer.
   B. must be secured by responsible security forces.
   C. becomes the responsibility of the building custodian.
   D. will be locked in a container made of at least 20 gauge steel.

2. Handling of controlled substances is covered in which regulation?

   A. AR 19-5.
   B. AR 190-5.
   C. AR 190-51, Chapter 4.
   D. AR 119-50.

3. VIP protection in Army medical facilities is covered in which regulation?

   A. AR 4-3.
   B. AR 40-30.
   C. AR 40-3.
   D. AR 400-3.

4. Civilians employed in a medical facility must have which of the following?

   A. A security clearance.
   B. A top secret clearance.
   C. An NCIC check.
   D. Clearance for handling sensitive items.

5. Locks or combinations to controlled medical sensitive items will be changed how often?

   A. Every 4 months.
   B. Every 6 months.
   C. Every 12 months.
   D. Every 24 months.

LESSON 4

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM		CORRECT ANSWER AND FEEDBACK
1.	D.	Will be locked in a container made of at least 20 gauge steel. After duty hours, keys, including IDS keys . . . (page 4-3, para c(7)).
2.	C.	AR 190-51. Chapter 4 AR 190-51, Chapter 4, provides minimum . . . (page 4-5, para 2a).
3.	C.	AR 40-3. AR 40-3 outlines DA policies and procedures . . . (page 4-6, para 3a(1)).
4.	C.	An NCIC check. Civilians must have, at a minimum, a . . . (page 4-3, para 1e)
5.	C.	Every 12 months. Locks or combinations will be changed . . . (page 4-3, para c(3)).

LESSON 5

PHYSICAL SECURITY PLANS FOR AIRCRAFT, MOTOR POOLS AND POL PRODUCTS

Critical Tasks: 191-386-0019
191-386-0020
191-286-0021

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to determine requirements for a physical security plan for aircraft, motor pools, and POL products.

TERMINAL LEARNING OBJECTIVES:

ACTION: Provide recommendations for a physical security plan for aircraft, motor pools, and POL products.

CONDITION: You will have this subcourse, pencil, and paper.

STANDARD: You must take the final subcourse examination and earn a score of 70 percent.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-11, AR 190-51, DA Pam 190-51, FM 19-30, and Physical Security Update 10-3.

INTRODUCTION

Identification of critical and vulnerable posts or areas is the first concern of physical security personnel. The threat or perceived threat must be assessed in light of the mission. Aircraft, motor pools, and POL storage areas require maximum protection. Each CO must ensure that security personnel are trained to give the best protection.

PART A - LEVELS OF PHYSICAL SECURITY

1. Some security procedures and physical protection measures are a must. These are Level I measures and they are basic and essential in safeguarding property. There are minimum requirements Armywide in accordance with AR 190-51.

2. Level II measures may also be implemented in accordance with AR 190-51 based on a risk analysis using DA Pam 190-51.

3. Level III measures are the highest and may be implemented in accordance with AR 190-51 based on a risk analysis using DA Pam 190-51. This level necessarily includes Level I and Level II measures.

PART B - ESTABLISH PHYSICAL SECURITY MEASURES FOR AIRCRAFT AND COMPONENTS

1. Responsibility.

a. The CO is responsible for a written physical security plan. Army posts with a permanent aviation facility located there or nearby will annex the post security plan with one for each airfield.

b. Some aviation facilities are not on Army property. If this is the case, the CO will coordinate with the host authority to provide a security plan.

c. A physical security officer will be appointed to develop physical security plans. He will also coordinate, implement, and update these plans. This officer may be a commissioned officer, a warrant officer, a noncommissioned officer, or a civilian.

2. Security Requirements.

a. Whenever practical, an aircraft will be parked at any Army airfield or civilian airport having an active security program.

b. Some locations do not have an active security program. If not, a crew member should remain with the aircraft, if possible. Otherwise, the CO is responsible for advising aviation authorities and the local law enforcement agency of the following:

(1) Aircraft location.

(2) Aircraft identification.

(3) Estimated length of stay.

(4) How crew members may be contacted.

c. The aircraft will be checked by a crewmember at least once a day.

3. Minimum Guard Standards.

a. Aircraft will be parked in hangars or available structures if at all possible.

b. Aircraft parked upon the flight line of Active Army, USAR, and ARNG aviation facilities will be checked by roving guards no less than once every three hours.

4. Security Measures.

a. AR 190-11 will be applied when an aircraft has weapons and/or ammunition aboard. Aircrafts with weapons and/or ammunition aboard must be provided constant surveillance.

b. A manufacturer approved security device will be used to secure an idle Army aircraft. A modified work order approved ignition security and door security device will be used. Emergency aircraft and aircraft undergoing maintenance with duty personnel present are exceptions. Aircraft used in a tactical exercise are also exceptions.

c. Lock and key control procedures must be included in the physical security plan, and they must be strictly followed. A master key or common key is prohibited on aircraft and hangars. Such a key is also prohibited on structures sheltering aircraft or their components.

d. The aviation physical security plan should include ID and movement control. Access to an aircraft can thereby be determined.

e. Privately owned vehicles are prohibited from flight line area and aircraft parking area. The only exception occurs when authorized by the airfield CO.

f. Unauthorized usage of some items would circumvent security measures. Such items will be secured during nonduty hours. These items include the following:

(1) Auxiliary power units (APUs).

(2) Vehicle tugs.

(3) Forklifts.

(4) Aircraft boarding ladders.

(5) Toolboxes.

5. Security Education. A formal security education program for employees is greatly beneficial. It will aid in minimizing threats to aircraft and aircraft components. A security briefing should be given all new employees, and a reinforcement of security awareness for all employees should be done periodically each year. Several methods could be used to emphasize support of security plans. Handouts, policy letters, and formal briefings are examples.

6. Physical Security Measures. Level II.

a. Construct a perimeter barrier and a patrol road or path. Build these around the flight line, parking ramps, pads and areas; build them around hangars, and other critical facilities. Erect protective lighting at outside aircraft parking sites.

b. Designate the aviation facility a "mission essential/vulnerable area," according to AR 190-13.

c. Secure aircraft tiedowns with locking devices.

d. Post warning sign around boundaries. These should read, "Off Limits to Unauthorized Personnel."

e. Require clearance before starting an aircraft engine.

f. Increase guard posts.

g. Install an IDS in hangars and structures and/or along perimeter fence; install CCTV at approved entrances and exits.

h. Implement security identification systems.

i. Park aircraft in permanently assigned spaces. These may be in hangars and outside parking areas. Rapid identification of missing aircraft is then aided.

j. Restrict parking of privately owned vehicles to designated lots. These should be at least 100 feet (30.48 meters) from protected areas of the airfield.

k. Implement a package control system.

l. Erect guard tower(s) in the vicinity of aircraft parking area(s). This tower(s) will provide vantage point(s) for guard surveillance.

PART C - ESTABLISH PHYSICAL SECURITY FOR MOTOR POOL

1. Introduction. Post motor pool and park is the nerve center for mobility. Vehicles, maintenance tools and equipment make the area vulnerable to theft and sabotage. The value of material found at motor pools and parks necessitates maximum security protection. Again, Level I physical security measures are mandatory, while Level II is at the discretion of the CO.

2. Level I Physical Security Measures for Motor Pools and Parks.

a. Motor pools and motor parks will be guarded during non-duty hours. Roving guard personnel may be used to conduct periodic security checks.

(1) Motor pools or parks are bound by a perimeter fence or barriers. These must meet the standards outlined in Appendix E, at the end of this subcourse. Grates and openings are closed and locked. Fences/barriers must be 7-8 feet high with a single top guard.

(2) Vehicle parking areas are lighted during the hours of darkness. Exceptions are those areas having empty trailers.

(3) Each vehicle in the motor pool or motor park is secured with a locking device. (Locking devices are covered by paragraph 3-5e(1)(a) through (d), AR 190-51.)

(4) Valuable items are vulnerable to theft if left exposed, assessable, and easily removable. Examples are radios, optical, and fire control equipment, etc. Utility items include hand tools, basic issue items, etc. All of these should be removed and secured separately, or they should be given added protection by some other means.

(5) No ammunition-bearing ("uploaded") vehicles or carriage-mounted/towed weapons system are parked therein in a complete, ready-to-fire configuration.

(6) Roving guards check the motor pool or motor park on an irregular basis. Security checks should occur not less than once every 2 hours.

(7) Dedicated guard personnel will be used at sites where criteria (1) through (6) above are not met.

b. Buildings are considered secure storage structures if they meet the following standards:

(1) Doors should provide the same degree of security to that of the walls of the structure.

(2) Door hinge mounting screws are not exposed to the building's exterior.

(3) Door hinge pins exposed to the exterior are designed or changed to prevent easy removal.

(4) Windows have individual locking devices. If within 12 feet of ground level they are barred or grilled. They may be covered with chain link material in a way to preclude easy removal.

(5) Walls, floors, and ceilings are built of at least 1/2 inch plywood, 1 inch tongue and groove wallboards, or equivalent.

c. There are certain standard procedures used at all motor pools or parks. They include the following:

(1) Privately owned vehicles will not be allowed in the motor pools or parks.

(2) Items that can be used to defeat security measures will not be left lying around the motor pool/park areas. Examples are bolt cutters, hacksaws, axes, steel rods or bars. When not in use, tools of this nature will be secured in the respective tool kits, or they will be secured in other locations.

(3) Entry to and exit from motor pools and parks will be controlled. Leave open only the minimum number of gates or openings. These should be necessary for efficient operations.

(4) Use of a common or master key to secure Army vehicles, motor pools, or parks will be forbidden. Keys and locks will be stringently controlled (See Appendix F at the end of this subcourse). Vehicles with ammunition aboard will be safeguarded according to standards and provisions of AR 190-11.

3. Establish Physical Security for Repair Parts and Their Storage Area.

a. Stocks of repair parts will be stored in a single area. The area will be readily accessible to maintenance and supply personnel. The following measures must be done to the greatest extent possible.

(1) Portable repair parts will be secured by one of the following means:

(a) In a locked, separate building or room. The area should meet security standards outlined in Appendix G at the end of this subcourse.

(b) In a locked, steel cage.

(c) In a locked, built-in container (bin, drawer, cabinet); or in a free-standing container large and heavy enough to be non-portable with stored parts.

(d) To the building in which located, or other permanent structure.

b. Non-portable repair parts will be secured by storing them in a building with doors and windows locked during non-operational hours. Bulky or heavy items are sometimes stored outside. These will be protected by a perimeter barrier and security lighting. Such security measures will meet the standards outlined in Appendix E at the end of this subcourse.

c. Access to repair parts storage areas and padlock keys will be strictly controlled.

d. Some items are identified with a pilferage code in the Army Master Data File (AMDF). These items signal a need for more intensive management practices. Added security measures may also be necessary. Some COs and supervisors have supply and maintenance activities which keep stock record accounts of pilferage items. These COs and supervisors will do the following:

(1) Ensure all their personnel handling such items know their AMDF designation. Ensure that they know the increased risk for pilferage or illegal diversion. Also, ensure that personnel are aware of any special procedures for control and protection of these items.

(2) Have pilferage-coded items partly inventoried at frequent intervals. As a minimum, the stock on-hand for each pilferage-coded line item will be inventoried once each quarter. Frequency of inventory for a particular line should be based on prior loss experience. If no prior losses have occurred, line should be selected for inventory at random. Large differences between stocks on-hand and record stocks will be investigated. This will first be done in-house; if not found, then a 15-6 investigation will be performed.

(3) Have stock accounting records for pilferage-coded items periodically reviewed. This should occur no less than monthly. It should be done by an officer, NCO (E-7 or above), or civilian employee of equal grade. Reviewer should be thoroughly familiar with the documentation, and he should be alert for unusually high issues, receipts, or use rates. Reviewer should be alert for bogus, modified, or other entries that might be suspicious. Appropriate action should be taken to follow up on suspicious entries.

(4) Take appropriate action to prevent any further unexplained losses, if some have occurred. Actions might include the following:

(a) Set up an informal log. Record in it all issues of pilferage-coded items not controlled by line-item accountability.

(b) Segregate portable, pilferable items from other stock; store them in a secure, separate container, room, or building with controlled access.

(c) Appoint a custodian to receive, account for, and issue all pilferage-coded items. These items, segregated from other stock need particular attention.

4. The following measures listed may also be implemented. This is up to the discretion of the local CO. The CO, in coordination with the PM or security officer, should analyze the security environment of his command.

a. Erect perimeter fences, associated barriers, and protective lighting.

b. Post motor pool or park perimeter with warning signs.

c. Designate motor pool/park a "mission essential/vulnerable area" according to AR 190-13.

d. Require written authorization signed by unit COs, or their representatives, before dispatch of vehicles.

e. Maintain vehicle dispatch control records or logs. Keep these at central location with a dispatcher. Park vehicles in designated parking spaces. Correlate control records or log placement and vehicle parking (by "line" or "block") and mark each accordingly. A system can then be devised to check quickly the validity of dispatch of a missing vehicle.

f. Check drivers for possession of a valid dispatch. Check drivers for valid operators' permits (OF 364). Do so before they depart from the motor park/pool.

g. Establish a policy requiring periodic checks of Army vehicles. Include those that operate on, enter, and leave the post. This measure will ensure vehicles are properly dispatched. It will ensure, also, that the vehicles are used for official business.

h. Segregate types of vehicles particularly vulnerable ones. These would be vehicles vulnerable to theft, misappropriation, or damage in the motor park/pool. Place these vehicles where guards can keep them most easily under surveillance.

PART D - ESTABLISH PHYSICAL SECURITY FOR POL STORAGE AREA

1. Introduction. For over a decade OPEC has virtually dominated and dictated the state of the world economy. OPEC does this through control of oil production and prices. OPEC leaders were keenly aware that the economy of industrialized nations could be crippled, if their oil supply was cut off. Not desirous of self-defeat, oil producing nations joined forces to limit production. They forced the price of oil per barrel to triple. The world is so dependent upon petroleum products that it is as precious as gold. Fuel is a major consideration in military capabilities. Aircraft will not fly, tanks will not move, and supplies and troops cannot be transported. POL storage areas, therefore, are critical and vulnerable areas for theft. High cost and sabotage are the reasons for this vulnerability.

2. POL Handling Facilities. Level I Security.

a. There are several types and methods of protection connected with the handling and dispersing of petroleum. Bulk POL handling facilities include the following:

(1) Buried or semi-buried construction.

(2) Floating roof (roof rises and lowers depending on the amount of fuel in the tank).

(3) Splinter proofing.

(4) Blast walls.

b. POL Storage areas will have fences and barriers. These will be built in accordance with OCE drawing 40-16-08, FE-6 type. The fences will be 7 feet high, including top guard. This should be single. Metal or reinforced concrete posts must be used. These must be set apart in multiples of 10 feet. 9 gauge chain link is authorized for use for POL storage areas.

c. POL pumps will be locked, and electrical power will be turned off when not under the surveillance of personnel. These must be only those persons

authorized to dispense the products. Hoses to pumps will be secured. This will prevent loss of POL through gravity feed.

d. POL tank trucks often contain fuel, and they are not always under surveillance of the operator. Such trucks will be secured with a lock hatch cover or lock manifold access doors. Each manifold valve may be secured with a transportation seal, if a manifold access door cannot be locked.

e. Fuel pods on vehicles and M561 (GOER) fuel vehicle tanks will be secured with padlocks. This measure will be taken when the vehicles or tanks are carrying fuel. The measure will also be taken when vehicles/tanks are not under the surveillance of the operator. Fuel-carrying vehicles will be parked in lighted areas of airfields or motor pools. These areas will be protected by locked perimeter barriers, or guards, when possible.

f. Tanker rail cars are sometimes spotted on post for unloading, and not under surveillance by POL handlers. If these tankers carry POL products, special treatment is called for: dome covers and manifold system shutoff valves will be locked. Railcars with packaged POL products aboard will be secured by locking all doors.

g. Packaged POL products not on board a vehicle or rail car will also be safeguarded. One of the following means will be used:

(1) In a structure meeting the standards in Appendix G at the end of this subcourse.

(a) Walls, floors, and ceiling will be built of at least 1/2-inch plywood, 1-inch tongue and groove wallboards, or equivalent.

(b) Doors will afford comparable security as walls.

(c) All openings of 96 square inches or more will be protected by bars and grills. They may be covered with chain link material instead.

(2) In an area protected by lighting and perimeter barriers in accordance with Appendix E at the end of this subcourse.

(3) In an area protected by guards during hours the storage facility is nonoperational.

h. Written instructions must be sent to POL dispensing personnel at filling station operations and Class III supply points. These instructions will include specific procedures for the following:

(1) Deciding if a customer is authorized.

(2) Deciding if drivers of military vehicles are licensed and the vehicles are properly dispatched.

(3) Seeing that pumps at dispensing points are locked, power is cut off, and hoses are secured when facility is not operational.

i. POL credit cards and ID plates will be centrally controlled by a custodian. This will be done preferably at Director of Industrial Operations (DIO) level. (If used weekly, or more often, a card or identaplate may be left with the vehicle or aircraft log book. Credit cards and identaplates will be kept in a locked container, with restricted access. This is the case regardless of location.) These cards and plates will be controlled through the use of a log book with the following information:

(1) Signature of person to whom issued.

(2) Rank of person to whom issued.

(3) Credit and identaplate serial number.

(4) Aircraft or vehicle number or USA registration number.

(5) Date and time signed out.

(6) Date and time returned.

3. Level II Security Measures for POL. The following are added security measures that may be implemented. Use is up to the discretion of the local CO. He should coordinate with the PM or security officer; together they should analyze the security environment of their command.

a. Designate POL storage and dispensing points as mission-essential or vulnerable areas. Do so in accordance with AR 190-13.

b. Ensure containers that can be used to carry fuel are secured. Ensure that hoses that can be used for siphoning are also secured. None of these items should be left lying around.

c. Ensure POL point attendants properly and legibly complete entries on the correct issues forms. Attendants (not recipients) should complete forms. Verify quantity issued by personally reading meter; spot check recipient's signature against the signature of the Armed Forces ID card.

d. Place seals on all points that might allow fuel theft by any means. Examples are bulk fuel tanks, tank trucks and fuel pads. Storage buildings and containers might also need such seals. This practice is very important on points where a padlock cannot be used. The measure is also useful for bulk shipments off the post. Broken seals indicate tampering (See Appendix H at the end of this subcourse).

e. Monitor unit or activity POL usage. Do so to determine if it is excessive. Periodically validate unit or activity requirements against POL point issues. This is done to discover indications of criminal activity. Spot check frequency and quantities of issues to specific vehicles at POL

points. Cross-check this against vehicle mileage for indications of theft or illegal diversion. Do so using DA Form 3643, figure 5-1.

f. Spot check the contents of containers storing used POL products, and ensure they are used (not fresh products) and marked properly. Ensure used POL products are stored separately.

g. Supervise loading of used products. This will ensure that fresh stocks are not included with material being disposed of.

h. Ensure all issues of fuel are made under adequate supervision or at least spot checked. Ensure that measuring devices are adequately calibrated and secured when not in use. See that large POL packages, e.g., 55-gallon drums, are handled in such a way as to preclude their use as hiding places for pilfered items.

i. Control the circulation of commercial POL tankers on the post. Have MPs check commercial tanker operators for a delivery order or copy of the procurement contract. Either authorizes them to enter the post. Bar entry of privately owned vehicles into POL dispensing points.

j. Review delivery and issue documents for indications of falsification. These may be changes or fictitious aircraft or vehicle ID numbers. Other indications may take the form of fictitious or dual-delivery receipts, or forged documents.

Follow up on bulk POL issues to ensure the same quantity issued actually arrives at the destination. Seals and locks on tanks may also be used.

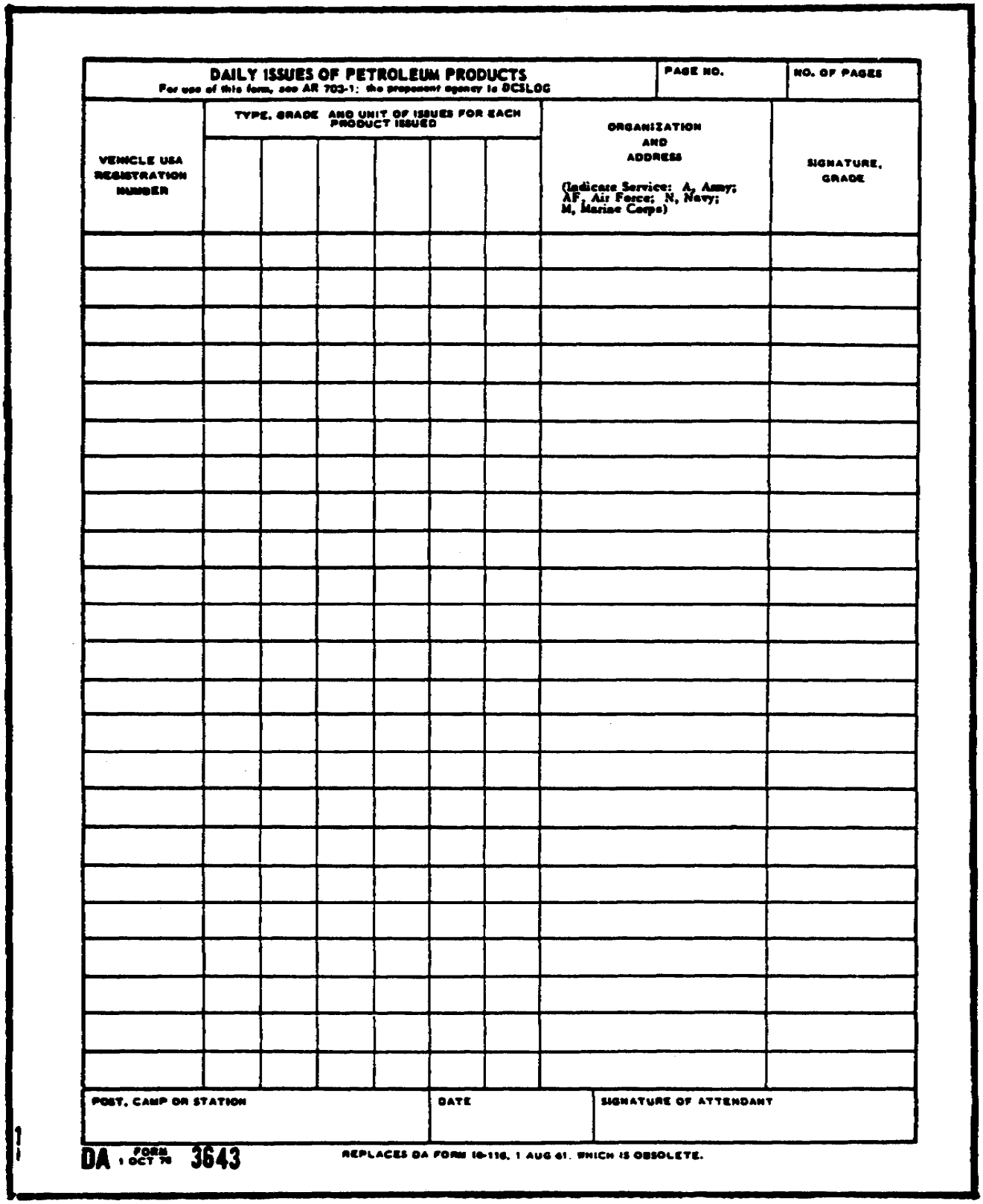
k. Make arrangements to have POL delivery tank trucks transport no more than that amount ordered. Delivery vehicles can then be checked before leaving the post. This will ensure the tanks are empty.

l. Conduct periodic unannounced audits of POL facilities.

m. See that inventories are done daily on all used pumps and monthly on bulk storage tanks.

n. Ensure placement of locking gas cap devices and antisiphon units in the vehicles.

o. Install IDSs in buildings used to secure POL products, (See Appendix I at the end of this subcourse).



DAILY ISSUES OF PETROLEUM PRODUCTS
For use of this form, see AR 703-1; the proponent agency is DCSLOG

PAGE NO. | NO. OF PAGES

VEHICLE USA REGISTRATION NUMBER	TYPE, GRADE AND UNIT OF ISSUES FOR EACH PRODUCT ISSUED						ORGANIZATION AND ADDRESS (Indicate Service: A, Army; AF, Air Force; N, Navy; M, Marine Corps)	SIGNATURE, GRADE

POST, CAMP OR STATION	DATE	SIGNATURE OF ATTENDANT

DA FORM 1 OCT 76 3643 REPLACES DA FORM 10-116, 1 AUG 61, WHICH IS OBSOLETE.

Figure 5-1. Daily Issues of Petroleum Products, DA Form 3643, (Front)

VEHICLE USA REGISTRATION NUMBER	TYPE, GRADE AND UNIT OF ISSUES FOR EACH PRODUCT ISSUED						ORGANIZATION AND ADDRESS (Indicate Service: A, Army; AF, Air Force; N, Navy; M, Marine Corps)	SIGNATURE, GRADE
POST, CAMP OR STATION				DATE			SIGNATURE OF ATTENDANT	

Figure 5-1. Daily Issues of Petroleum Products, DA Form 3643 (Reverse)

THIS PAGE INTENTIONALLY LEFT BLANK.

LESSON 5

PRACTICE EXERCISE

The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. The use of a common key to lock an aircraft is:

   A. authorized in emergencies.
   B. prohibited.
   C. unauthorized except upon approval by the CO.
   D. authorized.

2. Securing vehicles in the motor pool with a locking device is considered as what level of security measure?

   A. I.
   B. II.
   C. III.
   D. I and II.

3. Parts used for repair which are pilferage-coded items will be inventoried how often as a minimum?

   A. Monthly.
   B. Weekly.
   C. Quarterly.
   D. Semiannually.

4. When must dedicated guard personnel be used to protect aircraft located on an Army post?

   A. During the night when six or more aircraft are parked within a fence.
   B. When any aircraft is parked in the open.
   C. Only when the local environment possesses a hostile threat.
   D. At the aircraft CO's discretion.

5. It is recommended that POL credit cards will be centrally controlled by whom?

   A. POL storage supervisor.
   B. Vehicle dispatch operator.
   C. Physical security officer.
   D. DIO level custodian.

LESSON 5

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM		CORRECT ANSWER AND FEEDBACK
1.	B.	Prohibited. A master key or common key is prohibited . . . (page 5-3, para 4c).
2.	A.	I. Each vehicle in the motor pool . . . (page 5-5, para 2a(3)).
3.	C.	Quarterly. As a minimum, the stock on-hand . . . (page 5-7, para d(2)).
4.	B.	When any aircraft is parked in the open. Aircraft parked upon the fight line of . . . (page 5-2, para 3b).
5.	D.	DIO level custodian. POL credit cards and ID plates will . . . (page 5-10, para 2i).

APPENDIX A

DEFINITIONS

1. AMMUNITION. A device charged with explosives; propellants; pyrotechnics; initiating composition; riot control agents; chemical herbicides; smoke; and flame.

2. ARMS. Weapons that will expel a projectile or flame by the action of an explosive; the frame or receiver of any such weapon.

3. ARMS, AMMUNITION, AND EXPLOSIVES (AA&E). This includes the following:

a. Small arms.
b. Light crew-served weapons.
c. Ammunition.
d. Explosives.
e. Demolitions.
f. Privately owned weapons.
g. Special purpose weapons and ammunition.

4. ARMS STORAGE FACILITIES. Buildings used solely for arms storage; arms rooms or containers located in buildings used for other purposes.

5. EXPLOSIVES. Any chemical compound, mixture, or device whose main purpose is to explode. The term includes, but is not limited to, the following:

a. Individual land mines.
b. Demolition charges.
c. Blocks of explosives (dynamite, TNT, C-4, and other high explosives).
d. Other explosives consisting of 10 pounds or more (for example, gunpowder, nitroguanidine, etc.).

6. PROTECTION IN DEPTH. A system of providing several supplementary security barriers; e.g., perimeter fences; secure buildings, vaults, and locked containers that provide four depths (layers) of protection.

7. SENSITIVE ARMS AND AMMUNITION. Arms and ammunition requiring a high degree of protection and control due to vulnerability of theft and potential for use in civil disturbances. Sensitive arms and ammunition usually have an unpacked unit weight of 100 pounds or less.

8. WEAPONS CABINET. As a minimum, commercially built or locally made racks or containers for use within an arms storage room. It becomes part of the double barrier protection system for that room.

9. WIRE MESH CAGES. Prefabricated cages constructed according to OCE standards drawing 40-21-01. These cages are used to reinforce arms rooms as an inner liner.

APPENDIX B

CATEGORIES OF ARMS, AMMUNITION, AND EXPLOSIVES

1. MISSILES AND ROCKETS. Category I. These are nonnuclear manportable missiles and rockets in a ready to fire configuration. Examples are Hamlet, Redeye, Stinger, Dragon, light antitank weapon (LAW), Viper, AT-4, and javelin. This category also applies in cases where the launcher tube and the explosive rounds are jointly stored or transported.

2. ARMS.

a. Category II. Light automatic weapons up to and including .50-caliber, M16A2 rifle, SAW and 40-mm MK19 grenade machine gun.

b. Category III.

(1) Launch tube and gripstock for Stinger missile.

(2) Launch tube, sight assembly, and gripstock for Hamlet and Redeye missile.

(3) Tracker for Dragon missiles.

(4) Mortar tubes up to and including 81-mm.

(5) Grenade launchers.

(6) Rocket and missile launchers, unpacked weight of 100 pounds or less.

(7) Flame throwers.

(8) The launcher or missile guidance set or the optical sight for the TOW.

(9) Launch control unit for javelin.

c. Category IV.

(1) Shoulder-fired weapons, other than grenade launchers, not fully automatic.

(2) Handguns.

(3) Recoilless rifles up to and including 90-mm.

3. AMMUNITION AND EXPLOSIVES.

a. Category I. Explosive complete rounds for Category I missiles and rockets (Section B, above).

b. Category II.

(1) Hand or rifle grenades, high explosive, and white phosphorus.

(2) Mines, antitank, or antipersonnel (unpacked weight of 50 pounds or less each).

(3) Explosives used in demolition operations; for example, C-4, military dynamite, and TNT.

(4) Critical binary munitions components containing "DF" and "QL" when stored separately from each other and from the binary chemical munition bodies in which they are intended to be employed (see AR 190-59).

c. Category III.

(1) Ammunition, .50 caliber and larger, with explosive filled projectile (unpacked weight of 100 pounds or less each).

(2) Grenades, incendiary, and fuses for high explosive grenades.

(3) Blasting caps.

(4) Supplementary charges.

(5) Bulk explosives.

(6) Detonating cord.

d. Category IV.

(1) Ammunition with nonexplosive projectile (unpacked weight of 100 pounds or less each).

(2) Fuses, except for paragraph 3c, (2) above.

(3) Grenades, illumination, smoke, and CS/CN (tear producing).

(4) Incendiary destroyers.

(5) Riot control agents, 100 pound package or less.

(6) Ammunition for weapons above, not otherwise categorized.

APPENDIX C

STRUCTURAL REQUIREMENTS FOR
ARMS, AMMUNITION, AND EXPLOSIVES
STORAGE BUILDINGS

(New Constructions or Modifications to Existing Structures)

1. WALLS. These may be of three different types.

a. Eight inches of concrete, reinforced with No. 4 bars at 9 inches on center in each direction. Bars are staggered on each face to form a grid about 4 1/2 inches square.

b. Eight inch concrete block with No. 4 bars threaded through cavities. Cavities are filled with mortar or concrete, and they have a horizontal joint reinforcement at every course.

c. Eight inch brick interlocked between inner and outer courses.

2. FLOORS. These shall be built of concrete a minimum of 6 inches thick. They will be reinforced with 6 x 6 inch W4 x W4 mesh or equivalent bars.

3. CEILING AND ROOFS: Reinforcing bar spacing will form a grid; the area of any opening will not exceed 96 square inches. No. 4 bars or larger will be used. The ceiling or roof may be of concrete pan-joist construction. If so, the thinnest part may not be less that 6 inches, and the clear space between joists may not be less than 20 inches. The reinforcing grid requirements for flat slab construction also apply. Roof structures and ceilings of existing buildings shall provide a degree of security comparable to that required for windows and doors.

4. DOORS.

a. Doors shall be built of 1 3/4 inch thick solid or laminated wood. A 12 gauge steel plate will be mounted on the outside face. Doors may be built of 1 3/4 inch thick, hollow metal with a minimum 14 gauge skin plate thickness. These doors will be internally reinforced by vertical, continuous steel stiffeners spaced 6 inches maximum on center.

(1) Door bucks, frames, and keepers shall be rigidly anchored. They will be provided with antispread space filler reinforcement. This will prevent disengagement of the lock bolt by prying or jacking of the door frame. The frames and locks for both interior and exterior doors shall be especially designed and installed. This is to prevent removal of the frame facing or the built-in locking mechanism. Otherwise, disengagement of the lock bolt from outside a secured room could occur when the door is closed and locked.

(2) Construction requirements for door frames and thresholds shall be as exacting as those for the doors. For example, where metal doors are used, the frame and thresholds shall be metal. A class 5 steel vault door may be

used instead. This door must have a built-in, three-position, dial-type, changeable combination lock.

b. Various types of hinges are commercially available. When choosing the proper type of hinge for secure area doors, hinges shall be of the fixed pin security hinge-type or equivalent; exposed hinge pins shall be peened, spot welded, or otherwise secured to prevent removal; and hinge mounting screws may not be exposed to the outside of the arms room.

5. WINDOWS AND OTHER OPENINGS.

a. Windows and other openings shall be sealed with material comparable to that forming the adjacent walls, and they must be otherwise limited to the minimum number essential. Windows, ducts, vents, or like openings of 96 square inches or more with the least dimension greater than 6 inches shall be equipped with any of the following:

(1) Three eighths inch or larger hardened steel bars, provided the vertical bars are not more than 4 inches apart. Horizontal bars must be welded to the vertical bars so that the openings do not exceed 32 square inches.

(2) Number 8 gauge high carbon manganese steel mesh with 2 inch diamond grid.

(3) Number 6 gauge steel mesh with 2 inch diamond grid when number 8, in subparagraph (2) above, is not available.

b. Bars or steel mesh shall be securely embedded in the structure of the building, or they shall be welded to a steel frame securely attached to the wall. Fasteners shall be inaccessible from the exterior of the arms storage facility.

APPENDIX D

SPECIFICATIONS FOR INTRUSION
DETECTION SYSTEM SIGNS

1. SAMPLE. A sample IDS sign that may be used is shown in figure D-1. The sign is flat with shape, size, and legend as shown. The sign face should consist of reflectorized sheeting bonded to an aluminum backing as specified in paragraph 2.

2. SPECIFICATIONS. Sign backing is flat, degreased, etched, and unpainted aluminum alloy. It is type 6061T6, not less that 1/16 inch thick. For interior posting, plastic or wood could be used.

3. LANGUAGE. In non-English speaking overseas areas, a sign in the language of the host country should be mounted alongside the English language sign. In the US and its possessions, where a major minority language is spoken, similar signs may be posted as a safety precaution.

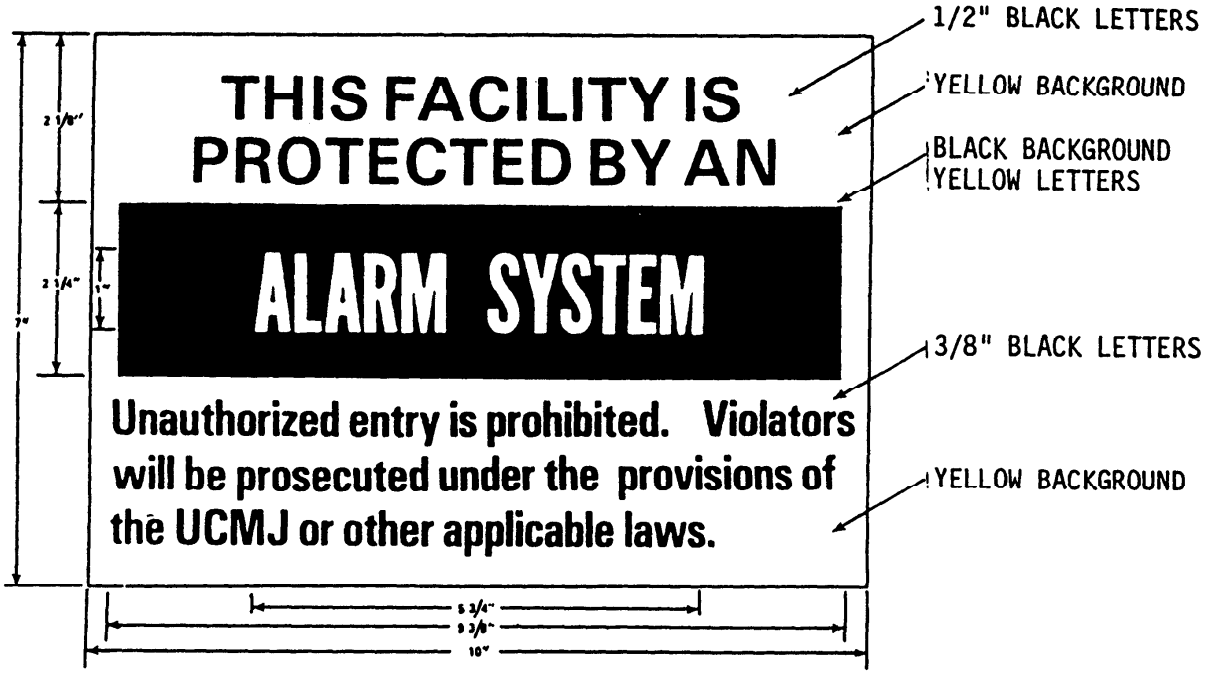


FIGURE D-1, SAMPLE INTRUSION DETECTION SYSTEM SIGN

APPENDIX E

PERIMETER FENCES, ASSOCIATED BARRIERS, AND PROTECTIVE LIGHTING

1. FENCES AND ASSOCIATED BARRIERS.

a. Fences for the security of unclassified, nonsensitive items should be FE-6 type. They should be built in accordance with COE Standard Drawing 40-16-08, and specification CEGS-02711.

b. Changes to existing chain link fences should not be made just to conform to the requirements of this appendix. If the existing fencing provides a like deterrent to penetration, it will suffice.

c. Drainage structures and water passages penetrating the fence should be barred. This measure will form obstacles to unauthorized entry. Some openings to drainage structures have a cross-sectioned area greater than 96 square inches (619.4 square centimeters). These openings should be provided with a welded bar or grillwork barrier on the upstream side. Parallel bars used to prevent access should be spaced horizontally. Not more than 6 inches (15.2 centimeters) of space should occur between bars. Where grillwork is used, the largest opening should be 6 inches (15.2 centimeters) in any direction. As an alternative, drainage structures may be built of multiple pipes. Each pipe should have a diameter of 10 inches (25.4 centimeters) or less. Multiple pipes of this diameter also may be secured in the part of the culvert facing the outside of the secured area. This measure will prevent intrusion into the area. All drainage plans must consider these items in deciding the proper size of the traverse drain to be used.

d. Openings in perimeter fences should be kept to a minimum. Use only that number necessary for efficient operations.

e. At some sites wet weather largely hinders ground traffic. This prevents guard personnel from having ready access to any point in the fence line. In this case, an all-weather patrol road or path should be constructed. As a minimum, roads should be surfaced with aggregate rock, and paths should be raised.

2. PROTECTIVE LIGHTING.

a. Protective lighting should be used in accordance with the principles outlined in FM 19-30.

b. Changes to existing protective lighting should not be made just to conform to the provisions of FM 19-30. If the lighting approximates these standards, it will suffice.

3. ADDITIONAL GUIDANCE. See FM 19-30.

APPENDIX F

KEYS, LOCKS, AND CHAINS

1. KEY CUSTODIAN. A key custodian will be named to issue and receive keys. He will also account for office, unit, or activity keys. The key custodian will also ensure that persons are assigned to issue, receive, and account for keys in his absence. The key custodian will see that these persons clearly understand local key control procedures.

2. KEY CONTROL REGISTER. Key control registers shall contain the printed name and signature of the individual receiving the key(s), date, and hour of issuance, serial number of key(s), printed name, signature of person issuing key, date and hour key(s) was returned and the signature of the individual receiving the returned key(s).

3. KEY DEPOSITORY.

a. A lockable container will be used to secure keys. This container may be a safe or filing cabinet. It could be a key depository made of at least 26 gauge steel. The depository must be equipped with a tumbler-type locking device, and it must be permanently affixed to a wall.

b. Only necessary primary keys will be kept in the depository. This way keys are more easily accounted for. Duplicate keys will be stored in a separate, locked container.

c. The key depository will be kept locked. Exceptions occur when issuing/returning a key and conducting inventories.

d. The key depository will be in a room where it is kept under surveillance around-the-clock, or it will be kept in a room that can be locked during nonduty hours.

4. LOCKS.

a. If a lock is required, US Government, key-operated, tumbler-type padlocks will be used to safeguard certain items. Examples are unclassified, nonsensitive Army supplies and equipment. The following padlocks are recommended; selection should be based on value of items protected and mission; choice should also be based on how essential the items are and how vulnerable to criminal attack:

(1) Padlock, low security, key (without chain), NSN 5340-00-158-3805; (with chain), NSN 5340-00-158-3807.

(2) Padlock, medium security, key, NSN 5340-00-799-8016.

b. Master key (common key) padlock sets will not be used.

c. Padlocks in use should not be changed just to conform with the recommendations of this appendix. Such is the case only if the existing padlocks afford an equal level of security.

d. Padlocks not in use will be secured in a locked container along with their keys. Access to the container will be controlled.

5. KEY AND LOCK ACCOUNTABILITY.

a. Keys to locks used to protect property will be checked at the end of each duty day. Differences between on-hand keys and the key control register will be reconciled. Keys may be issued for personal retention. Such is the case only if daily turn-in clearly endangers mission readiness, or if this procedure seriously impedes operational efficiencies. Personally retained keys will be inventoried on a "show basis" no less than monthly.

b. Padlocks and their keys will be inventoried by serial number. Such inventory will take place no less that semiannually. Inventory will be done on a "show basis" only.

c. Padlocks will be rotated at least once annually. Rotation of existing locks and keys should be centralized, and it should be controlled by the key custodian.

d. When a key to a padlock is found missing, the padlock will be replaced immediately.

6. CHAINS. A chain may be required for security of unclassified, nonsensitive equipment and supplies. If so, it can be obtained under the following NSN:

a. NSN 4010-00-129-6049 (1/4 in/.64 cm).

b. NSN 4010-00-702-4003 (1/4 in/.64 cm).

c. NSN 4010-00-988-3181 (1/4 in/.64 cm).

d. NSN 4010-00-149-5583 (5/16 in/.79 cm).

e. NSN 4010-00-286-5527 (5/16 in/.79 cm).

f. NSN 4010-00-161-9299 (3/8 in/.95 cm).

g. NSN 4010-00-186-5645 (3/8 in/.95 cm).

h. NSN 4010-00-720-4591 (3/8 in/.95 cm).

i. NSN 4010-00-824-1404 (3/8 in/.95 cm).

7. ADDITIONAL GUIDANCE. Key control procedures for arms, ammunition, and explosives are in AR 190-11. AR 190-51 contains procedures for storage of controlled medical substances and other medically sensitive items. Additional guidance on general procedures in Chapter 4, FM 19-30.

APPENDIX G

STORAGE STRUCTURE SECURITY

Buildings and rooms are considered secure storage structures if they meet the following standards:

1. Doors provide a degree of security equal to that of the walls.

2. Door hinge mounting screws are not exposed to the exterior of the building. Exposed screws will be spot welded, covered, or filled with material in a way to prevent easy removal. Nails will not be used to mount hinges.

3. Door hinge pins exposed to the exterior of the building are of a design or changed to prevent easy removal.

4. Doors to the exterior, locked from the inside, are secured with a dead bolt locking device or crossbar. Such doors may be secured by a similar locking device resistant to jimmying and manipulation from the outside. A latch style door lock is not desirable.

5. Windows have individual locking devices.

6. Certain first floor openings, except doors, are in excess of 96 square inches (619.4 square centimeters). When these openings are located less than 12 feet (3.7 meters) from the ground level, they are barred or grilled. They may be covered, instead, with chain link material in a way to preclude easy removal.

7. Doors secured from the outside must have special locking devices. These must conform with CE specifications for that type of structure. Locking devices may be US Government tumbler-type, key-operated padlocks (See Appendix E).

8. Walls, floors, and ceilings are constructed of at least 1/2 inch plywood, 1 inch tongue-in-groove wall boards, or equivalent.

APPENDIX H

USE AND CONTROL OR PROTECTIVE SEALS

1. PURPOSE OF SEAL. The purpose of a seal is to show whether integrity has been compromised. Storage buildings, vehicle or rail shipments, or containers may be sealed. A plain seal is not a lock, although combination items referred to as "seal-locks" are available. The whole purpose of a seal, no matter how well made, may be defeated. Strict accountability and disciplined application must be maintained for success.

2. ORDERING AND STORING SEALS.

a. Seals should be strong enough to prevent accident breakage during normal use.

(1) Design. Seals should be complex enough to make unauthorized manufacture of a replacement difficult.

(2) Tamper proof. Seals should readily provide visible evidence of tampering, and they should be built in a way that makes simulated locking difficult once the seal has been broken.

(3) Individually identifiable. Seals should have embossed serial numbers and owner identification.

b. A single office on post should be responsible for ordering and issuing seals to users. The source for the seals should ship the seals to the attention of a seal custodian in that office.

c. Seals not issued for actual use should always be secured. They should be kept in a locked metal container with controlled access. Only seal custodians and alternates, and perhaps a supervisor or CO, should have access.

3. ACCOUNTING FOR SEALS.

a. Seal custodians should maintain seal logbooks. These should be hard cover, not looseleaf books.

b. Issue of seals to a using custodian should reflect date of issue, name of recipient, and seal serial numbers.

c. Issue of a seal for actual use by a custodian should reflect seal number and date and time applied. Identification of item to which the seal was applied and location on item if other than main door(s) should also be included. In addition, the name of the person applying the seal should be recorded. Outbound loaded trailers, railcars, and container shipments must be covered; the appropriate trailer, railcar, or container number and load destination should be noted.

4. APPLICATION OF SEALS.

a. Seal all doors and openings, not merely the main one.

b. Run seal strap through hasp only once. Seals wrapped around several times become illegible.

c. Listen for "click" when inserting point of seal into sheath.

d. To ensure positive closure, tug down on strap; twist the point section inserted into the locking mechanism.

5. CHECKING SEALS AND BROKEN SEALS. The command using the seals should develop detailed procedures for checking seals. This command should determine the actions to be taken for breaking a seal. Lastly, this command must decide on procedures to follow upon finding a broken or suspect seal.

6. DISPOSITION OF USED SEALS.

a. All shipping documents will reflect seal number(s). All seals will be verified with seal log, shipping documents, or other appropriate documents. This will be done before removal and disposal of shipment.

b. Seals should be deformed enough upon removal so that they cannot be used to simulate a good seal. They may be disposed of in normal trash.

c. The user seal log may be located on the same post. If so, the custodian should be advised of the seal's destruction, or the seal should be returned to the custodian. The custodian should annotate the date and time removed, and he should enter the name of the person removing the seal across from the original entry on the seal in the log book.

7. CHANGING SEALS. Colors of seals procured should be changed periodically as an added physical security measure.

APPENDIX I

INTRUSION DETECTION SYSTEMS

1. PURPOSE OF INTRUSION DETECTION SYSTEMS. Intrusion detection systems (IDS) consist of sensors and detection of various types. The purpose of an IDS is to protect property. It does so by signaling the presence of an intruder upon penetration, or movement in, the protected area. A system should be properly designed, installed and maintained; it should be monitored and integrated with other measures. In this way a physical security program can greatly improve the level of protection. Such protection must be given to government property. Many times, the system can also reduce personnel devoted to guard duties. On the other hand, the system is not effective when poor internal control procedures and worker theft are the causes of losses. COs and supervisors considering an IDS should first consult with the local PM or security officer.

2. DETERMINING THE AVAILABILITY OF IDS EQUIPMENT. Government furnished IDS equipment will be used to secure Army property. Availability of equipment may be determined through coordination with HQ, US Army Aviation Troop Command, Physical Security Equipment Management Office (PSEMO), ATTN: AMSAT-D-WCP, 5900 Putman Rd, Suite 1, Ft Belvior, VA 22060-5420.

3. PROCUREMENT AND INSTALLATION OF IDS EQUIPMENT. Commercially available IDS equipment may be procured and installed provided:

a. A statement of nonavailability of Government furnished equipment is obtained. This statement must come from the Intrusion Detection System project officer at ATSCOM. Requirements should be sent to the address indicated in paragraph 2 above.

b. A life cycle cost analysis is performed to determine if IDS equipment should be leased or purchased.