SUBCOURSE
MP1001

EDITION
C

INSTALLATION SECURITY

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM

A
I
P
D

READINESS / PROFESSIONALISM THRU GROWTH

INSTALLATION PHYSICAL SECURITY

Subcourse Number MP1001

Edition C

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

5 Credit Hours

Edition Date: November 1995

SUBCOURSE OVERVIEW

We designed this subcourse to teach you the procedures you will need to perform as a physical security specialist/supervisor. This subcourse covers all aspects of physical security from basic measures to the development of a complete installation physical security plan.

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 identify the procedures for establishing and maintaining physical security.

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

STANDARD: You must achieve a score of 70 percent on the final subcourse examination to demonstrate competency on the subcourse material.

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LESSON 1

IDENTIFY PHYSICAL SECURITY THREATS

Critical Task: 191-386-0001

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to identify threats to physical security and implement methods for controlling these threats.

TERMINAL LEARNING OBJECTIVE:

ACTION: Identify threats to physical security and implement methods for controlling these threats.

CONDITION: You have this subcourse, pencil and paper.

STANDARD: You must complete all exercises for each lesson. You must take the final subcourse examination and earn a score of at least 70 percent correct to demonstrate competency.

REFERENCES: The material contained in this lesson was derived from the following publications: FM 3-19.30, AR 190-13, and Current Army Threat Statement.

INTRODUCTION

Political instability is world-wide. This condition threatens the ideology of democratic countries. Individuals, as well as organized groups seek to change government structures. They do so by means of sabotage, terrorism, and stealing. They may also use espionage, subversive acts, and civil wars. Such threats form a web of insurgency; US military operations are prime targets.

1. General.

a. The Department of the Army (DA) represents a vital force in US defense. Therefore, safeguards for personnel and the post/facilities that are mission essential or vulnerable to attack are vital. Attacks and kidnapping of US diplomats and military leaders over the world are examples. These are the kinds of problems facing the MP Corps in the realm of physical security.

b. Today, strategy for the professional MP focuses resources and efforts toward preventing criminal acts. These pose a real threat to security.

Reaching this goal means work. We must identify, analyze, and plan solutions for the threat. With this knowledge they can recognize and plan effective measures to counter and halt threats.

2. Priorities for Physical Security Requirements.

a. Physical security is a large part of the overall defense of a post and its Crime Prevention Program.

b. All DA installations are valuable to the national defense structure. An analysis of the mission of a post is important. This will aid in deciding the extent of physical security needs.

c. Cost effectiveness is the silent force behind defense spending now. In simple words, it means eliminating waste; it means receiving the most for each dollar spent. Those activities requiring less protection must be identified. This must be done in the interest of the economy. Establishing criteria to assess security priorities is a must. Priority is based upon an analysis of two factors -criticality and vulnerability. A post may be both highly critical and highly vulnerable. If so, a broad physical security program is vital. Less important and susceptible areas receive less protection.

d. Criticality relates to the effects of partial or complete loss of a post/facility. What effect would such loss have on the ability of the post/facility to perform its mission? Would this affect the mission for a considerable period of time? The relative criticality may have no direct relationship to size. It may not be related to whether an end product is produced. This must be determined on the basis of its importance to the post/facility as a whole. A good example would be the sabotage of a petroleum, oils, and lubricants (POL) storage area supporting units in a theater of operation. This would have serious impact upon the unit. It would harm the unit's ability to perform its mission for a long time. Areas such as this would be highly critical. They would require extensive physical security measures. To deter threats would call for broad protection. One or more internal areas may require maximum protection. The overall mission, however, may not warrant such for the entire post. Each requires expertise. Each post also needs physical security personnel such as yourself to analyze the need.

e. Vulnerability pertains to the likelihood that a threat could cause sufficient loss, damage, or destruction to affect accomplishment of the mission. Often, one or more threats exist which could easily achieve this result. If so, then threats are likely to interfere with the mission. Aviation facilities and motor pools are highly vulnerable areas. So are ammunition and explosives storage areas. The degree of risk from each threat varies. Variation might be due to the type of facility involved or to the mission performed. Physical layout, construction, and the protective program being used would vary. Vulnerability should be related to specific threats. Examples are terrorism, criminality, etc.

3. Security Threats. Security threats are acts or conditions which might disrupt the post. Examples are damage, loss, or destruction of property; personal injury or loss of life. Compromise of defense information is another example. There are two major classes of security threats; natural and human.

a. Natural threats. Natural security threats are the consequence of natural phenomena. Some, however, can be caused by human action. Physical security measures cannot prevent loss, damage, or destruction of property. They cannot prevent injury and loss of like due to these types of threats. After natural disaster, basic security measures may be rendered ineffective for a while. Emergency plans should be coordinated with physical plans. The aim should be to control the situation and reinstate security measures.

(1) Floods, tornadoes, fires, and earthquakes are natural threats. So are fog, snow and ice, and wind. Any of these can destroy installations. Any can destroy lives. The actual effect of these on the physical protection of the post is of prime importance. Alarm systems may be inoperative; communication will likely be disrupted; perimeter fences may be down; property may be scattered, inviting looting. Advance planning allows security personnel to manage a crisis situation. It allows them to implement protective measures to the greatest extent possible.

(2) Earthquakes frequently break gas lines. This increases the possibility that fires may begin. Security personnel must be on the alert to notify firefighters immediately. Intruders may capitalize on the situation. They may enter the post while security personnel are busy.

(3) Limited visibility creates vast problems. The cause can be darkness, fog, heavy rain, or sand storms. Response time to alarms may be restricted. Thus, saboteurs, thieves, and espionage agents could cause grave harm before they are apprehended. Criminals can use these conditions to hide their acts. Careful planning should be done to provide protective barriers and lighting. These are necessary for secured areas. Such measures would offset the advantages criminals otherwise would have.

b. Human threats. Human threats are varied. They result from a state-of-mind, attitude, weakness, or character trait. These may occur in one or more persons. These threats include acts of commission or omission; they may be overt or covert. Any one of these threats could disrupt or destroy the post operation or mission. Human threats are physical acts. Human behavior cannot be accurately predicted; therefore, security planning must be based on the assumption that a risk does exist. Espionage and theft are human threats. So are sabotage and terrorism. All of these call for grave attention in security planning.

4. Espionage.

a. Espionage is the act of spying on a country. It occurs when the agent secretly or under false pretenses, searches out information or makes observations; the goal is the intention of passing this data to another country. Every member of the Army is a target for espionage activities. This is due to the knowledge they possess of military operations. The problem does not stop here. We are in an age of advanced technology and scientific development. Much of it is geared toward national defense. Therefore, industrial facilities and defense depots rank high as targets for espionage.

b. Gathering intelligence data is much like working a puzzle. Shrewd, expertly trained agents collect fragments of data from varied sources. Once assembled, these pieces present a broad enough picture for the enemy. They can then make fairly accurate assumptions about operations. They can piece together technical development or military readiness. The goal of espionage is to have a military edge in case of war. Espionage is a valuable tool in reaching this goal.

5. Methods of Espionage. Trench coat and dark glasses are not typical of today's espionage agents. They may disguise themselves as legitimate businessmen. They may assume disguises of tradesmen such as electricians or plumbers. They may pretend to be college students or professors. They may be coworkers, neighbors, or social acquaintances. Be assured that some agents obtain considerable rank. This may occur in military as well as civilian government and industrial positions. To avoid espionage, security personnel must have a sharp knowledge of how information is gathered. It is vital that you learn how the enemy thinks, since great ingenuity is used by agents in getting information. Some of the methods employed are as follows:

a. Stealing or buying information from employees. Persons with financial crisis are victimized by agents. They offer financial aid for favors.

b. Stealing information from records. Agents may actually be employees at a post. They may seize chances to steal valuable records.

c. Using threats of danger to relatives or friends of an employee to gain information.

d. Using blackmail techniques by threatening to expose intimate and personal information about a person.

e. Securing information from waste and carbon paper and other discarded records.

f. Obtaining information from loose talk at social gatherings.

g. Using "fronts," such as commercial concerns or import-export businesses. Travel agencies and scientific organizations are other examples. Agents use these fronts to obtain information.

6. Espionage Targets. Security personnel should be knowledgeable of specific subjects which may interest espionage agents. This would include any specific data which adds to an evaluation of the nation's war potential. Specific areas of interest include the following:

a. Strengths, location and disposition of US and Allied troops. Also, their movement and combat efficiency.

b. Capacity, production rate, and industrial mobilization schedules.

c. Specifications of products or special equipment; methods of operation.

d. Test records of newly developed items or equipment.

e. Critical and vulnerable points; possible methods of effective sabotage.

f. Inventory of completed products; destination and transportation means and routes.

7. Espionage Countermeasures. The FBI and USAMI each bear a primary responsibility. That is investigation of subversive acts and counterespionage operations. The role of physical security personnel IS NOT to investigate; they re to make espionage more difficult. They do so by applying protective measures. Investigating subversive activities may take months or years. This is done by trained counterintelligence people. One thoughtless act by security personnel may foil the effort. Counterintelligence efforts must be closely coordinated. This reduces the degree of risk from espionage. Some of the duties within control of security personnel are as follows:

a. Thorough loyalty checks of personnel, particularly before employment.

b. Prevention of unauthorized entry to the premises of the post.

c. Special guarding, careful handling, and safekeeping of classified material.

d. Controlled burning of waste paper, carbons, and typing tape used in preparing classified data.

e. Restriction of movement of all personnel within the post.

f. Periodic evaluations of personnel with access to classified data.

g. Security education and training programs for employees.

NOTE: Some of the above will be done in conjunction with Military Intelligence.

8. Sabotage. Sabotage is any act that may injure, interfere with, or obstruct the US or any ally in preparing for or in carrying on war. Sabotage can also be defined as any willful act of making war material in a defective manner. Security personnel should expand this definition. It should include any act which maliciously destroys property or disrupts a post operation or mission for any reason. Military operations could be jeopardized badly due to sabotage.

a. Motives for sabotage. Do not allow yourself to think that sabotage is always motivated by defense interests. This is high on the list of motives. Consideration for the persons or groups involved must also be given. A saboteur may work for pay, hatred or revenge. He may work from sincere belief, to settle a real or imagined wrong, or because of blackmail. Enemy agents are trained to identify easy targets for recruitment. Likewise, you must also be aware of such persons. Suspicious behavior should be reported to the proper investigating agency.

b. Characteristics of saboteurs. Who is the saboteur? He may be anyone. He could be a foreign agent, well trained, or a rank amateur from any nation. Saboteurs may be motivated by any of the reasons mentioned above. The use of legitimate business as a front allows them to infiltrate installations and industries. Saboteurs may work alone or in groups with possible aid from sympathizers. How they work depends on how broad the mission. Behavior patterns give clues to the characteristics of a saboteur. Persons may frequently act on impulse. They may act discontented with their job. They may be easily swayed by subversive propaganda; they could be mentally ill.

c. Sabotage targets. Targets selected for sabotage will result in disruption of national defense capabilities. The disruption may be direct or indirect, complete or partial. Agents lie dormant for long periods of time. They analyze weaknesses in security programs; they identify vulnerable activities. Then they make plans for the assault. As security personnel, your planning must reach past the obvious; it must include assumptions of other possibilities. There is not however, a foolproof security system. Knowing which targets are critical and vulnerable aids in defense planning. Military installations of all branches of the service are targets. So are public utilities -power, water, gas, lights, and sewage lines. Transportation -highways, airports, waterways, and facilities supporting these functions are targets. Logistics -warehouses, supply depots, weapons and ammunition storage areas are also. Each of these areas demand a threat analysis. This is a must when determining criticality and vulnerability. Appropriate security planning will be based on this analysis. It will also be based on available resources.

d. Sabotage methods. Ingenious methods used by saboteurs are endless. However, the methods may be generally classified as follows: fire, explosive/mechanical devices, chemical, and psychological. Recognition of an act of sabotage is often difficult. This is because the act itself often destroys evidence of sabotage. To use effective countermeasures, you must understand some of the methods used.

e. Countersabotage. The enemy adopts new methods and devices to use in sabotage. Likewise, you should be motivated toward better security measures to counter these acts. Using physical security measures would help stop sabotage. Following is a list of countermeasures:

(1) Use of effective planning.

(2) Risk analysis and evaluation.

(3) Physical security education programs.

(4) Use of protective barriers.

(5) Identification and movement control system.

(6) Search of incoming vehicles.

(7) Designation of restricted areas.

(8) Safeguarding classified information.

(9) Physical security surveys and inspections.

(10) Emphasis on building/maintaining employee morale and awareness.

9. Terrorism.

a. Terrorism is the use of violence, force, or threat. The aim is to reach political goals through fear, intimidation, and coercion. The media is used by terrorists to bring worldwide attention to their political objectives. At the same time, their attention creates a sense of government incompetency. Physical security has a great impact on terrorism. It makes the terrorist work harder, and complicates his plan. It requires him to increase the risk of compromise. Threat analysis is the first stage of controlling terrorism. In the process, the collection of intelligence and criminal information is used. This is necessary in evaluating vulnerability of a post against terrorism. Effective security programs emit excellent results; however, it is impossible to completely safeguard a post against terrorists.

b. Terrorism is a strategy; it is a tool of the weak. Though few in number, terrorists are well-organized groups. Normally they plan all operations with care.

c. Target selection. Victims of terrorism are a part of the strategy. The goal of terrorism is to attract worldwide attention to their cause. This may take the form of violence or the taking of political prisoners. Targets are selected to maximize that goal. What better method to gain attention than by hijacking a commercial aircraft filled with innocent people? What is better than keeping the world watching, while terrorists dramatically stage refuel stops from country to country. Random violence as in public gatherings occurs not because of mass violence. They select these locales because of the maximum shock effect of the act.

d. Methods used by terrorists:

(1) Bombing displays their capability of direct assault. This may occur on any targets as a means of retaliation. In the early morning, October 23, 1983, the U.S. Marine barracks in Beirut, Lebanon was bombed by terrorists. A truck carrying explosives was driven through a security checkpoint, through other barriers and into the center of the Marines'

Operations Building and exploded. At least 241 Marines and Sailors were killed; others died later as a result of their injuries. The Marines were part of the peacekeeping forces, along with France, Italy, and Great Britain. This terrorist activity was in defiance of U.S. presence and policies in the Mideast.

(2) Robbery is the method used to get supplies. They need these to maintain terrorist activities. Ammunition, weapons, communications equipment, and money are examples. These rank high on the list of priorities of terrorists.

(3) Kidnapping of officials and family members is a method embraced by terrorists. Yet, victims are seldom the actual targets. In December 1981, in Verona, Italy, a US Army General was kidnapped from his quarters. The General did work at HQ, NATO command in Southern Europe. However, his position consisted merely of bureaucratic functions. The likely target was NATO itself. Terrorists unhappy with NATO operations and the US used the incident to demonstrate vulnerability. They also used the event to gain attention and to shock the world. Perhaps they hoped to gain a few sympathizers.

(4) Arson of government property may be a gesture of their ability to destroy critical facilities. Arson could be a diversionary tactic prior to assault on actual targets.

(5) Ambushes. Terrorist training, weapons, and method of operation make an ambush a highly attractive terrorist tactic. This tactic underscores the four characteristics of terrorist operations; they are dynamic and constantly changing, simple, though well planned, executed quickly to conserve personnel and equipment, and designed for maximum publicity for their impact.

(6) Hijacking tactics offer the chance to use hostages in bargaining for various demands. Security personnel must admit that terrorists are well disciplined for violence and destroying human life. Even their own life means little if it stands in the way of reaching their goals.

e. Terrorism Counteraction. The broad scope of terrorist operations warrants a course of study in itself.

10. Pilferage.

a. Physical security personnel have a working definition of pilferage. It includes the meanings of "steal," "theft," "larceny," and similar terms. Included is both petty theft and theft of any amount or monetary value. Theft of government property should not be viewed solely in terms of monetary value. Rather it should be viewed in terms of criticality. The loss of supplies critical to the post mission could endanger it.

b. Types of pilferers.

(1) The casual thief steals because he cannot resist the temptation. This type normally acts alone; he takes small quantities of supplies for family use in the home. Pens, pencils, notebook pads, and small handtools are typical examples. Poor security measures invite the opportunity for theft.

(2) The systematic thief is one who steals according to preconceived plans. He steals any and all types of supplies to sell for cash or trade. Weapons and ammunition are popular targets, since terrorists provide a rich market for such items. Systematic stealing may be a one-time occurrence; or it may be extended over a period of months or years. It may consist of one person or an organized group; and he may or may not be an employee of the post.

c. Methods of pilfering. Removal of property by the casual thief would normally be by concealment on the person or in his car. This makes the act hard to detect and even harder to prove. Systematic thieves use more complex plans. They may falsify shipping and receiving documents. They may dispose of property in a trash can and salvage it later. They have been known to classify new or serviceable material as salvage.

d. Countermeasures for casual pilferage. Using a psychological deterrent is the best way to control casual theft. This may be done in a number of ways. Some are discussed in the following paragraphs.

(1) Search persons and vehicles leaving the post at unannounced times and places.

(2) Set up aggressive security education programs. Disseminate information on cases where employees were fired or prosecuted for stealing. Take caution to avoid identifying those persons; possible civil suits for defamation of character could result.

(3) Establish enough inventory and control measures to account for all material, supplies, and equipment. One person should not have control of all shipping and receiving.

(4) Identify government tools and equipment by some mark or code. Do so when possible.

e. Control measures for systematic pilferage. Physical security measures are the best deterrents to systematic theft. Security people such as yourself must weigh each case, since security needs will vary. Based on your assumptions, measures such as the ones listed must be used. However, you are not limited to only these.

(1) Set up security surveillance of all post exits.

(2) Begin a good package and material control system.

(3) Locate parking areas for private vehicles outside the bounds of the post.

(4) Use careful preemployment screening.

(5) Investigate all losses quickly and well.

(6) Set up good key control system.

(7) Use adequate security patrols to check buildings, grounds, and perimeter.

(8) Install mechanical and electrical intrusion detection devices. Do so where needed and practical.

(9) Establish appropriate perimeter fencing, lighting, and parking facilities. Also include necessary vehicle gate security controls.

THIS PAGE LEFT BLANK INTENTIONALLY

LESSON 1

PRACTICE EXERCISE

REQUIREMENT: 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 been studying methods of operations which may be used by thieves. Systematic pilferers are most apt to try to remove property by what method?

    A. Using normal shipping operations: railroad cars and trucks.
    B. Randomly selecting vehicles leaving the area.
    C. Concealing it in privately owned vehicles.
    D. Concealing it on their person.

2. What is the primary concern of a systematic pilferer in selecting a target?

    A. There is no great demand for the item among the local people.
    B. It is readily available to any employee on the post.
    C. It would require aid from an accomplice to remove it from the post.
    D. It has monetary value.

3. Which one of the following is a human threat?

    A. Earthquakes.
    B. Espionage.
    C. Tornadoes.
    D. Tidal waves.

4. Which one of the following would be an investigative agency function rather than a physical security function?

    A. Investigation of sabotage attempts.
    B. Protection of equipment.
    C. Preventing damage to equipment.
    D. Writing security plans.

5. What is the most practical and effective method for controlling a casual pilferer?

    A. Frequent inventories.
    B. Psychological deterrents.
    C. Stringent disciplinary actions.
    D. Effective use of trained investigators.

6. You are asked to analyze the need for additional physical security requirements on your post. What should priority be based on?

A. Installation commander's directives.
B. Criticality and vulnerability.
C. Installation location.
D. Area crime report.

7. The use of violence, force or threat to obtain a goal best describes which of the following?

A. Sabotage.
B. Espionage.
C. Subversive activities.
D. Terrorism.

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item Correct Answer and Feedback

1. A. Using normal shipping operations
They may falsify shipping...(page 1-9, para 10c).

2. D. It has monetary value.
He steals any and all... (page 1-9, para 10b(2)).

3. B. Espionage.
Espionage and theft... (page 1-3, para 3b).

4. A. Investigation of sabotage attempts.
Suspicious behavior should... (page 1-6, para 8a).

5. B. Psychological deterrents.
Using a psychological deterrent... (page 1-9, para 10d).

6. B. Critically and vulnerability.
Priority is based upon... (page 1-2, para 2c).

7. D. Terrorism.
Terrorism is the use of... (page 1-7, para 9a).

LESSON 2

PROTECTIVE BARRIERS AND LIGHTING

Critical Tasks: 191-386-0003
191-386-0004

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to identify the need for and use of protective measures in a physical security plan.

TERMINAL LEARNING OBJECTIVE:

ACTION: Identify the need for and use of protective measures.

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

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

REFERENCES: The material contained in this lesson was derived from the following publications: FM 3-19.30, AR 190-11, AR 190-13, and TM 5-820-4.

INTRODUCTION

One or more persons unknown gained access to the post medical storage area. An undetermined amount of controlled drugs were removed. First investigation showed that electrical power had been interrupted for about two hours. It happened during a thunderstorm the previous night. As physical security officer, you are not simply concerned with capturing the thief, but the flaw in your security plan must be examined. Were available detection aids in use? These might have included perimeter barriers, protective lighting, and/or intrusion detection systems. Was there an alternate power source available for use during emergencies? Security aids are not complete solutions for security. However, when used as a part of a security system, they enhance the total physical security posture. Perimeter barriers and protective lighting are designed to delay penetration.

PART A - PROTECTIVE BARRIERS.

1. General.

a. Protective barriers are obstacles used to define the physical limits of a post, activity, or area. They are used to restrict, channel, or impede access. Barriers alone will not stop a determined intruder.

b. Barriers function to:

(1) Define the aforementioned physical limits.

(2) Create a physical and psychological deterrent to unlawful entry.

(3) Help the security force to capture an intruder.

(4) Use as few security persons as possible to get the job done.

(5) Direct the flow of persons and vehicles through certain gates and facilities for identification and control.

2. Categories of Protective Barriers. There are two major categories of protective barriers -structural and natural.

a. Structural barriers are devices installed to deter penetration of an area. Examples are fences, gates, and walls. Floors, towers, and perimeter roads and clear zones are further examples.

b. Natural barriers include terrain features. Examples are mountains, cliffs, and canyons. Rivers, and other bodies of water, marshes, and deserts are examples. These are barriers broad enough to deter unlawful entry. They are supplemented with structural barriers, where required.

3. Consideration.

a. Protective physical barriers should be used to safeguard the entire post or facility. These should also be used in setting up restricted areas.

b. Certainly the size of the area may be a factor; however, this decision must be based on what is being protected.

4. Types of Fences. There are four types of fencing normally used to protect security areas. These are chain link, barbed wire, concertina, and barbed tape. Choice depends upon the degree of permanence of the area involved. Also considered are the materials and time available for construction. Outside perimeter fencing should be straight. This permits unhampered observation.

a. Chain Link. Chain link fence is the most common type of barrier at permanent posts. There are three types of chain link fences. Type FE-5 fence is constructed with a six-foot fabric and no top guard. This type fence should be used as a minimum for installation perimeter security and for conventional arms and ammunition security at bulk storage facilities. NOTE: It is not intended that because of construction design, the fence cannot have a top guard placed on it. This is purely the commander's option, if he so desires, to have one added. The FE-6 fence provides a commander with more security in that it is constructed with a seven-foot fabric and a one-foot top guard facing upward and outward at a 45-degree angle toward the threat (facing away from the protected area). Finally, the FE-7 fence provides even more security. The fence is also constructed of a seven-foot fabric. However, the top guard is constructed with a "Y" top guard. Both outriggers are facing upward and outward at a 45-degree angle. One facing the threat and the other facing the protected facility. Nine-gauge or heavier wire, galvanized, is used with mesh openings not larger than 2 inches. The wire is twisted and barbed selvage at the top and bottom prevents the fence from unraveling. Posts may be metal or concrete, and they are to be set apart in 10 foot increments. The fence is to be securely fastened. If painted, a nonreflective color will be used. On soft ground, the fence must reach below the surface deeply enough to compensate for shifting soil or sand.

(1) Chain link fencing is durable, strong, and low in maintenance cost.

(2) It is used for protection of permanent security areas.

(3) Openings in this type of fencing are small enough to deter the passing through of some stolen articles.

b. Barbed Wire. Standard barbed wire is twisted, double-strand #12-gauge wire. It has 4-point barbs placed an equal distance apart. When the purpose of a fence is to deter human trespass, it should not be less than 7 feet high, excluding the top guard. It must be tightly stretched and firmly affixed to posts not more than 6 feet apart. Distance between strands of wire should not exceed 6 inches. At least one wire will be interlaced vertically and midway between posts. Fences of shorter heights are allowed when the purpose is to separate the boundary of government property.

(1) Barbed wire fences are mainly used at semi-permanent installations.

(2) It is also used for perimeter fences at vast isolated posts.

(3) Handling barbed wire is difficult.

c. Concertina. Standard concertina is a wire coil of high-strength, steel, barbed wire. It is clipped together at intervals to form a cylinder. Opened, it is 50 feet long and 3 feet in diameter. Concertina should be laid with one roll on top of another, in a pyramid arrangement. A minimum of three rolls should be used.

(1) Concertina can be quickly laid and picked up due to its elasticity.

(2) It is more difficult to cut than standard barbed wire.

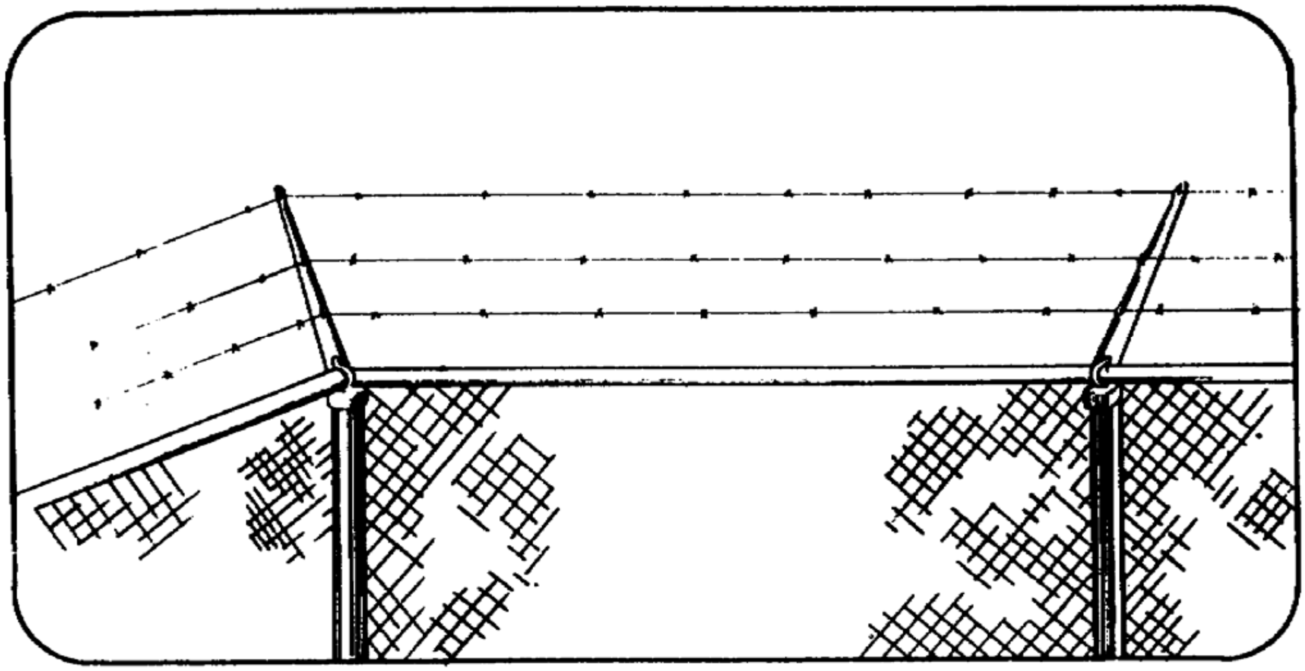


Figure 2-1. Supporting arms on top guard point outward

d. Barbed tape or razor ribbon. Barbed tape or razor ribbon may be used as top guard; it may be used at combat fortifications.

(1) Temporary barriers may be built of this type fencing.

(2) Ground maintenance is hampered.

e. Top Guard.

(1) Top guards may be added on interior enclosures, also, when added protection is desired. A top guard is overhang of barbed wire along the top of a fence. It faces outward and upward at an angle of 45 degrees (toward the threat).

(2) Three strands of barbed wire, spaced 6 inches apart, are used on the supporting arms. The length of these arms and the number of strands of wire can be increased when required. The supporting arms are affixed to the top of the fence posts. They will be of a height to increase the overall height of the fence at least 1 foot. (See Figure 2-1.)

f. Gates and entrances. The number of gates and perimeter entrances must be the minimum required for safe and efficient operation. When gates and entrances are closed, they must give the same degree of protection as the barriers.

g. Type field perimeter fence. A combination of concertina fencing may be used. This is a double-barbed wire fence with five rolls of concertina between the fences (cattle fence). (See Figure 2-2.)

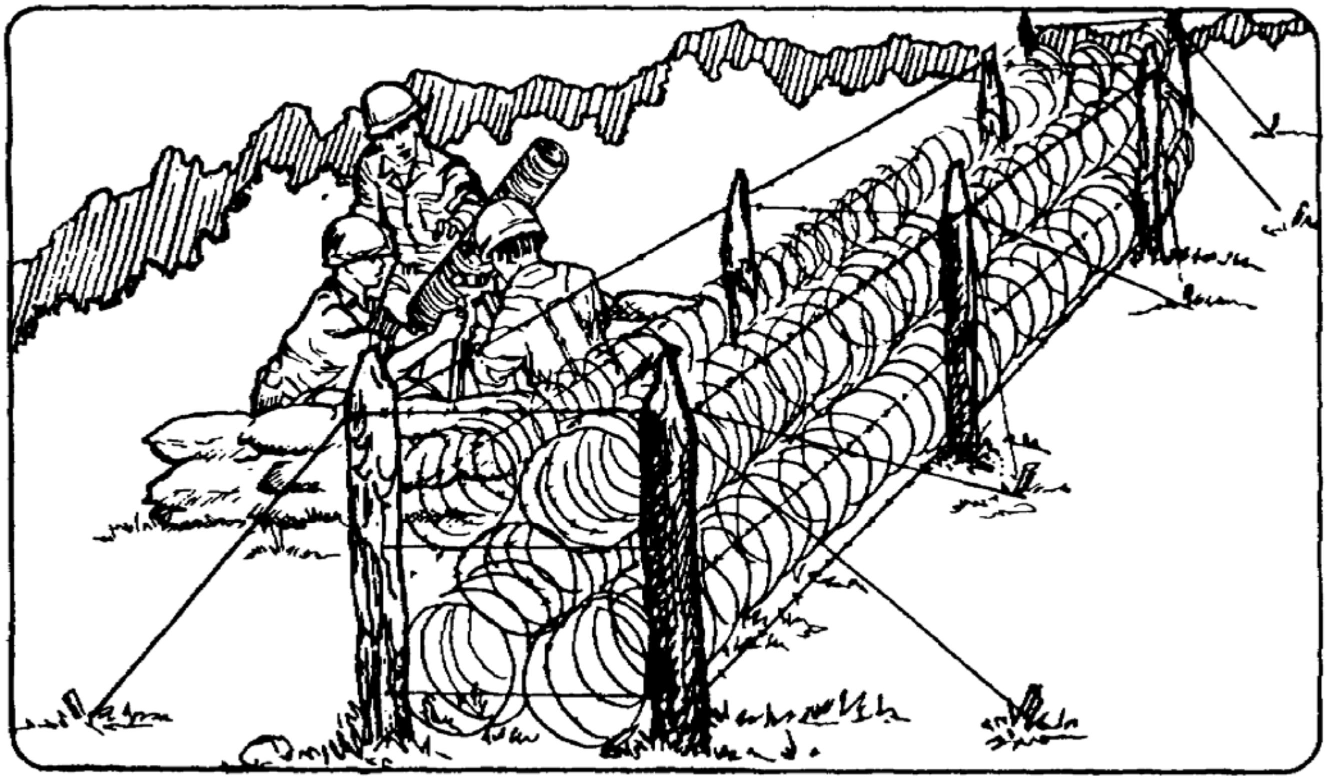


Figure 2-2. Cattle fence of double-barbed and concertina wire

h. Tanglefoot wire.

(1) Barbed wire or tape may be used differently in appropriate cases. One example is to construct a tanglefoot obstruction either outside a single perimeter fence or in an area between double fences. This is done to provide an additional deterrent to intruders.

(2) Hampers ground maintenance.

5. Security Requirement for Utility Openings.

a. Utility openings include sewers, manholes, and drainage ditches. Also included are culverts, vents, and ducts. These provide access to criminals for sabotage, espionage, and theft. (See Figure 2-3.)

b. Sewers, air and water intakes, and exhausts with openings of 10 inches or more in diameter must be protected with rods and bar grills.

c. Any drainage ditches of greater than 96 square inches must also be protected.

6. Other Perimeter Barriers.

a. Sometimes building walls and roofs serve as perimeter barriers. If so, they must be built to provide equal protection.

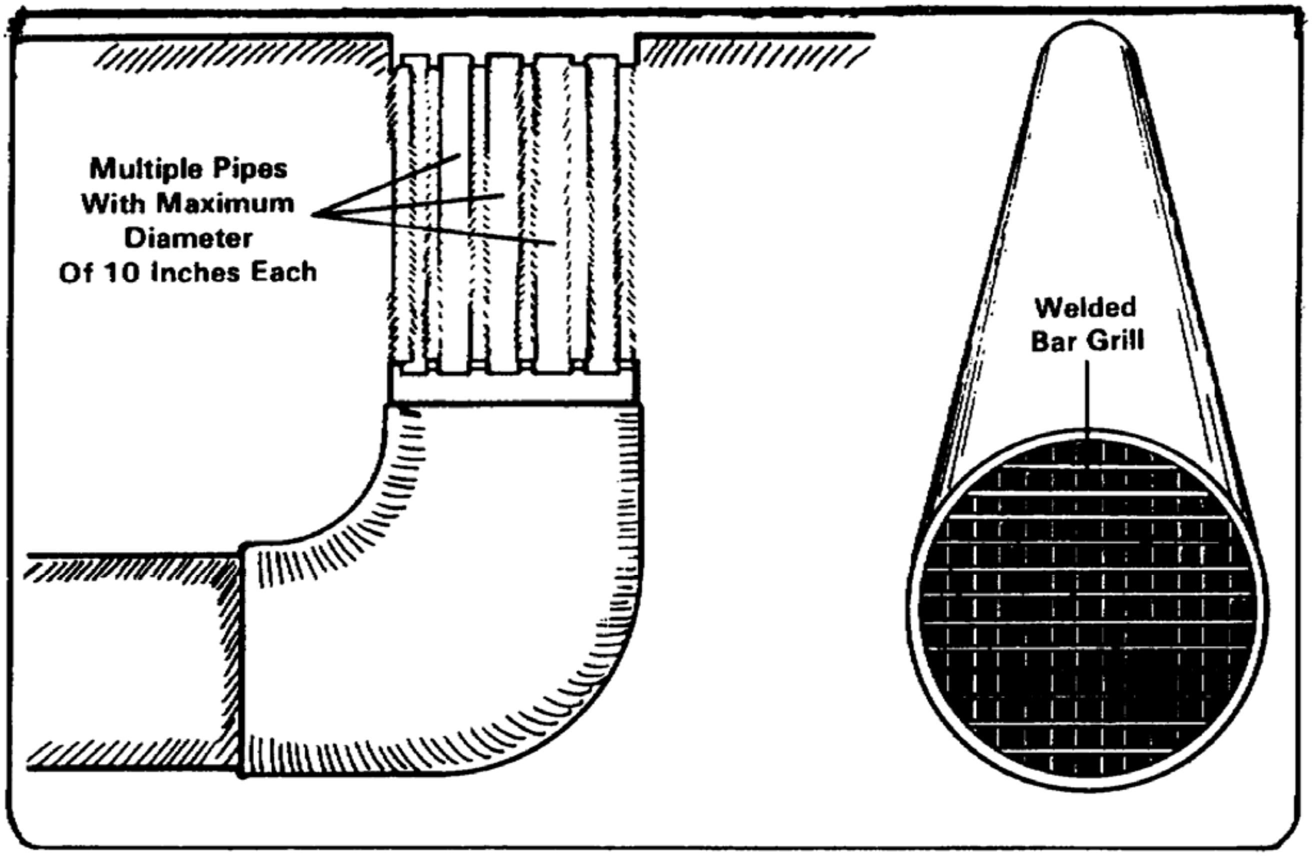


Figure 2-3. Examples of secured utility openings

b. If these buildings are less than two stories high, they must have a top guard on outside cropping.

7. Signs and Notices.

a. Put up control signs on all approaches to the perimeter. These should be readable from a reasonable distance. These signs are to aid in controlling entry onto the post. They also serve to deter unauthorized entry and to prevent accidental entry. These signs will contain the designation "United States Army." They may contain other control and ownership information if necessary. This is the case in areas where English is but one of two or more languages commonly spoken. The signs will be placed at eye level.

b. Put up provision of entry signs on all principal entrances. These should be legible at a distance of not less than 50 feet from the point of entry. These signs tell persons desiring entry of the provision concerning search of persons, vehicles, etc. They may tell of prohibitions against cameras. They could concern entry for other than official business. Any of these signs may be prescribed by the post CO.

c. Put up restricted area signs at all entrances to affected areas. Place them also at conspicuous and appropriate points along the perimeters of these areas. These signs designate the restricted area. They are also used at all otherwise concealed areas. Each sign or notice will be marked with the words "RESTRICTED AREA." This is the case regardless of the type of restricted area. In addition, the signs will include the following notice:

WARNING

> This (fort, range, plant, laboratory, etc.) has been declared a restricted area by authority of (TITLE) Commanding General, Commander, etc., in accordance with the provisions of the directive issued by the Secretary of Defense on 20 Aug 54, Act of 1950. Unauthorized entry is prohibited. All persons and vehicles entering hereon are liable to search. Photographing, making notes, drawings, maps, or graphic representations of this area or activities, is prohibited unless specifically authorized by the commander. Any such material found in the possession of unauthorized persons will be confiscated.

d. Put up danger warning signs when necessary. Do so especially where children approach perimeter barriers. These signs will warn them away from such barriers as barbed wire or tape.

8. Restricted Areas.

a. Restricted areas are defined (AR 190-13) as, "Any area, entry to which is subject to special restrictions or controls for reasons of security or safeguarding of property or material."

b. The post CO is responsible for designating restricted areas. His authority comes from DOD Directive No. 5200.8, dated 20 August 1954. Authority also comes from AR 190-13.

c. Security protection of a restricted area pertains particularly to subversive activities control. This includes protection against espionage, and sabotage. Also included are any such restrictions adversely affecting U.S. national defense. Restricted areas are not for the purpose of protection of unclassified property or material nonessential to defense. Examples are areas devoted to storage or use of classified documents; also equipment or materials should be classified to safeguard against espionage. A post communications center should also be so classified, as well as a cashier's cage or mechanic's toolroom. The responsibility for designation is the CO's. However, the one advising him, the provost marshal or security officer, should consider carefully the foregoing guidance. He should evaluate the purpose of any proposed designation of a restricted area. He should coordinate with the intelligence officer and SJA. He should then plan his recommendation accordingly.

d. A restricted area must be designated in writing by the CO. It must be posted with warning signs or notices. These should be of the type described in AR 190-13.

e. The establishment of restricted areas improves security. It does so by providing defense in-depth. It increases efficiency by providing degrees of security compatible with operational requirements. These areas may also provide for economy of operation. It reduces the need for stringent control measures for the entire post.

9. Type of Restricted Areas.

a. The degree of security and controls required will be dependent upon several things. The nature, sensitivity, or importance of the security interest affect the degree. Restricted areas may be established to provide the following:

(1) Effective use of necessary security measures; exclusion of unauthorized personnel.

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

(3) Conditions for segregating special areas; also conditions for providing increased security of classified data with little impact on total operations.

b. Areas have different degrees of security interest. The degree depends upon the area's purpose and the nature of the work. It also depends on the information and/or materials concerned. For similar reasons, different areas on a post may have varying degrees of security importance. Sometimes, the entire area of a post may have a uniform degree. It may require only one level of restriction and control. In others, differences will require more segregation of certain activities.

c. To meet these different levels of security further designations may be needed. Examples are "exclusion," "limited," "controlled" areas. (It must be understood that the term "restricted area is, in effect, a legal designation; whereas, the terms "exclusion," "limited," and "controlled" are administrative only.)

d. The main criterion for an administrative designation is the degree of restriction or controls required. The goal is to prevent compromise of security interest or other matter therein. Characteristics of these are as follows:

(1) Exclusion area. This is a restricted area containing the following:

(a) a security interest of such nature that entry to the area is the same as having access to such security interests, or (b) a security interest of such importance that just being in the area is treated as equivalent to (a) above.

(2) Limited area. This is a restricted area having a security interest. In this area uncontrolled movement will permit access. Within this area, use escorts and other internal controls. Persons who have a legitimate reason for entering a limited area may, but they can do so only if provided adequate restrictions and controls. These measures usually consist of escorts and other physical safeguards.

(3) Controlled area. This is an area usually across from or surrounding limited or exclusion areas. Entry to the controlled area is restricted to those with a need for access. Here movement of authorized personnel is not necessarily controlled. Also, entry here does not give access to the security interest or other matter within the exclusion or limited areas. The controlled area is provided for administrative control and safety. It is a buffer zone for depth in security for the exclusion or limited areas. The degree of control movement within this area will be prescribed by the appropriate CO.

e. A post may have varying degrees of security designation. Or it may have none at all. It may be entirely a restricted area; it may have no further degree of restrictions or controls. It may further be administratively classified, in whole or in portions. Further classifications were covered in the preceding material. These were an exclusion area, a limited area, or a controlled area.

10. Clear Zone. The effectiveness of security observation, installation perimeter barriers and lighting depends largely on one thing: that is the quality of the clear zones around the post. Clear zones are maintained on both sides of the perimeter barrier. This provides an unobstructed view of the perimeter. Clear zones should be kept clear of weeds, rubbish, and other material. Any of this is capable of hiding a potential intruder. The texture and color of the clear zone surface should provide as much contrast as possible to intruders crossing it. Clearing and maintaining the zone can be very difficult; it may require bulldozing, burning, and cutting. It is a must to control vegetation in this zone. A clear zone of 20 feet or more should be maintained in some areas. Examples are between the installation perimeter barriers and exterior structures. This zone should also be kept between the barriers and parking areas and natural features. When possible, another clear zone of 50 feet or more should be maintained, between the perimeter barriers and structures within the protected areas. Exceptions occur when a building wall is part of the barrier. Sometimes the threat of intruders slipping through the perimeter barrier is great, as for instance, in a theater of operations. Clear zones there may be very wide. This provides maximum observation and field of fire. In this case, several lines of perimeter

barriers may be installed, and a clear zone is set up between each. Intrusion detection and antipersonnel devices may be installed in the zones. They increase detection and repelling capabilities. Sometimes it is impossible to have adequate clear zones because of property lines or natural or man-made features. Then it may be necessary to increase the height or complexity of the perimeter barrier. You may need to increase security patrol coverage. You may also need to install more protective lighting and intrusion detection devices. These need to be placed along that portion of the perimeter.

PART B - PROTECTIVE LIGHTING

1. General.

a. Protective lighting provides the same protection in the dark like that maintained during the day. This safeguard serves as a deterrent to thieves and vandals, and it makes the job of the saboteur more difficult.

b. Protective lighting is only one element in a physical security design. Therefore, an analysis of each case will reveal which security protection or combination provides the security needed.

c. Security duties are carried out better with the aid of protective lighting. Such duties include the identification of badges and people at gates. Other duties are the inspection of vehicles and detection of intruders. Also, the inspection of suspicious circumstances is aided by such lighting.

2. Areas Requiring Protective Lighting.

a. All limited and exclusion areas must have protective lighting, and they must have it on a permanent basis. Such lighting should be placed at perimeter and access control points.

b. Arms storage facilities and rooms, motor pool bays, and hangers that have weapons stored on board must have security lighting. Outdoor parking areas for vehicles or aircraft having stored weapons also need this lighting.

c. Other places which may need such lighting include pier and dock areas, vital buildings, and warehouses. Banks, finance and accounting offices, helipads and hangers, and medical facilities may also need it.

3. Characteristics.

a. Lighting is inexpensive to maintain.

b. Protective lighting may reduce the need for security forces.

c. Such lighting provides personal protection for forces. It does so by reducing the advantages of concealment and surprise for an intruder.

d. Protective lighting usually requires less intensity than working light.

4. Commander's Responsibility.

a. COs must determine lighting requirements, since physical layout, terrain, climatic conditions, etc., will vary with each post facility.

b. Lighting requirements depend on:

(1) Threat.

(2) Perimeter extremities.

(3) Surveillance capabilities.

(4) Available guard force.

c. Contingency planning is required. This will ensure proper functioning during hours of reduced visibility. Emergencies and mobilization alerts will also need to be covered.

5. Planning Consideration. Physical security personnel plan the most effective use of protective lighting. Therefore, numerous factors must be considered that have a direct bearing on each case. The aid of the Corps of Engineers should be sought. Also, information from manufacturers of lighting equipment should be sought. Compliance with FM 3-19.30, Physical Security, and other applicable regulations, is a must.

a. Plan for the cleaning and replacement of lamps. Include cost and maintenance required and available.

b. Consider the use of photoelectric and mercury control or automatic controls. These are desirable in peacetime situations, but they are undesirable when blackout is a possibility.

c. Local weather conditions could affect various types of lamps and luminaries.

d. Fluctuating and erratic voltages in the primary power source could cause problems.

e. Establish a burning-time record. The ledger should be kept based on 80 percent life expectancy. It should also include the following data:

(1) Type and wattage of lamp.

(2) Area, facility, or utility pole used.

(3) Date of insertion.

(4) Programmed date of extraction.

(5) Where used (administrative area).

f. Limited and exclusion areas must have protective lighting on a permanent basis. The light must be positioned to prevent glare. This may temporarily blind the guards. At entrance points, light should be intense enough to enable guards to identify bearers and badges. Control of the lighting must be with the security forces.

g. Interior and exterior arms storage lighting must be provided. Included are buildings where arms storage rooms are located, motor pools, and hangers. Also, outdoor parking areas for vehicles or aircraft that have weapons stored aboard are included. Unauthorized persons must not have access to switches for exterior lights. Wire mesh screen must be placed over these lights. This will prevent their being broken by thrown objects.

6. Principles of Protective Lighting.

a. Security forces should be able to watch activities around or inside a post. They should be able to do so without disclosing their presence. Protective lighting should be used in conjunction with other measures. Examples are fixed security posts or patrols, fences, and alarms. Do not use protective lighting alone. Guards must see long distances; they must be able to see low contrast. This vision is improved by higher levels of brightness.

b. In planning protective lighting, high brightness contrast between intruder and background should be considered first. Dark, dirty surfaces or camouflage-type painted surfaces require more light.

c. To be effective, protective lighting should:

(1) Discourage or deter attempts at entry by intruders.

(2) Make detection likely if entry is attempted.

7. Types of Protective Lighting Systems. The type of lighting system to be used will depend upon the overall security requirements of the post/area (See Table 2-4). There are four general systems of protective lighting; these are continuous, standby, movable, and emergency.

a. Continuous light (stationary). This system is the most common. It consists of a series of fixed light fixtures arranged to flood the area. Flooding is in overlapping cones of light during hours of darkness. Continuous lighting is used in two primary methods: glare projection and controlled lighting.

(1) Glare projection lighting directs the glare outward toward a perimeter approach. At the same time it restricts the downward beam of light. This method makes it hard for the intruder to see inside the area. It also allows the guard to watch intruders at great distances beyond the perimeter.

Lastly, this method protects the guard by keeping him in comparative darkness. Glare projection is not appropriate where security troop emplacement may be silhouetted or illuminated for the enemy (See Figure 2-5).

(2) Controlled lighting adjusts and controls the width of the lighted strip to fit the particular need. A wide strip inside the fence and a narrow strip outside may be needed because of adjoining highways, air ports, etc. (See Figure 2-6.) The floodlighting of a storage tank or roof is another example. This method has the disadvantage of illuminating security posts and patrols.

b. Standby lighting (stationary). This is similar to continuous lighting. However, the lights are turned on, either automatically or manually. They are turned on when suspicious activity is detected by security or alarm system. Or they may be used when there is a need for added security.

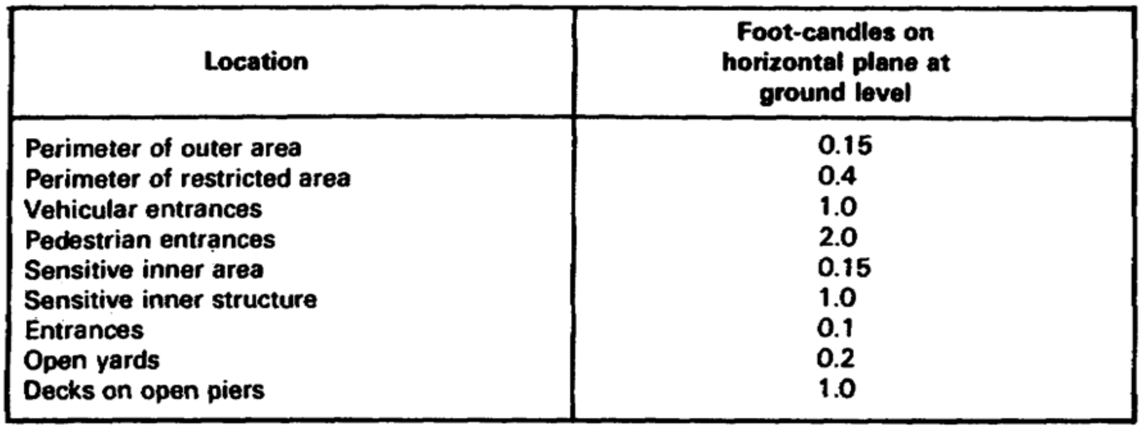
c. Movable lighting (stationary). This consists of manually operated, movable searchlights. Such lighting is normally used to supplement all the other systems, such as standby. These units may be installed on patrol and reaction vehicles. They may also be placed in towers and at strategic points on the perimeter.

d. Emergency lighting. Such lighting duplicates any or all the above systems. It is used when power failure or other emergencies shut down the primary systems. Emergency lighting requires an alternate power source. Portable generators and batteries are examples.

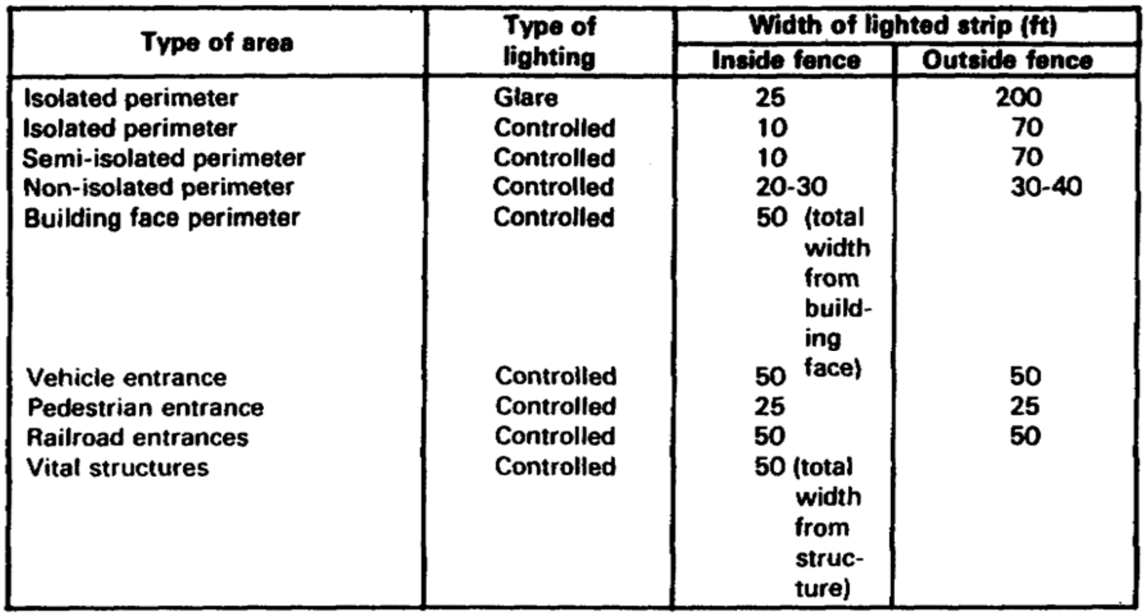
e. Dual lighting. Active entrances should have two or more lighting units. There should be enough illumination for recognition of persons and examination of credentials. Semiactive and inactive entrances should have the same continuous lighting as the rest of the perimeter. Also, there should be sufficient standby lighting to be used when entrance becomes active.

f. Pier/dock lighting. Piers and docks should have both water approaches and the pier illuminated. Small wattage floodlights may be used under piers and around pilings. The US Coast Guard should be consulted for approval of proposed lighting near navigational waters.

g. Other lighting. Vital structures and areas should be considered first in planning protective fencing and lighting. Power, heat, water and communications need attention. So do explosive and critical materials. Delicate machinery and areas where highly classified material is stored or produced need special attention. So do valuable finished products. Vital structures of areas which are classified vulnerable from a distance should be kept dark. Standby lighting should be available. Those areas which can be damaged close at hand should be well lighted. The surroundings would be well lighted. This forces an intruder to cross a lighted area. Walls (if a building) should be lighted to a height of 8 feet. This eases silhouette vision.



Location	Foot-candles on horizontal plane at ground level
Perimeter of outer area	0.15
Perimeter of restricted area	0.4
Vehicular entrances	1.0
Pedestrian entrances	2.0
Sensitive inner area	0.15
Sensitive inner structure	1.0
Entrances	0.1
Open yards	0.2
Decks on open piers	1.0



Type of area	Type of lighting	Width of lighted strip (ft)	
		Inside fence	Outside fence
Isolated perimeter	Glare	25	200
Isolated perimeter	Controlled	10	70
Semi-isolated perimeter	Controlled	10	70
Non-isolated perimeter	Controlled	20-30	30-40
Building face perimeter	Controlled	50 (total width from building face)	
Vehicle entrance	Controlled	50	50
Pedestrian entrance	Controlled	25	25
Railroad entrances	Controlled	50	50
Vital structures	Controlled	50 (total width from structure)	

Table 2-4. Lighting specifications

8. <u>Wiring Systems</u>. Both multiple and series circuits may be used to advantage in protective lighting systems. Their use depends upon the type of lighting used; use also depends on other design features of the system. The circuit should be so arranged that failure of any one lamp will not leave part of the perimeter line in darkness. Neither should a critical or vulnerable position be left in darkness. Connections should be such that normal interruptions will not hamper the system. These interruptions can be caused by overloads, industrial accidents, and building or brush fires. Also, lines should be placed underground or sufficiently inside the perimeter as with overhead wiring. This will lessen the chance of sabotage or vandalism from outside the perimeter. The design should require system maintenance that is simple and economical. It should require minimum shutdowns. Cases where this occurs are in the course of routine repairs, cleaning, and lamp replacement.

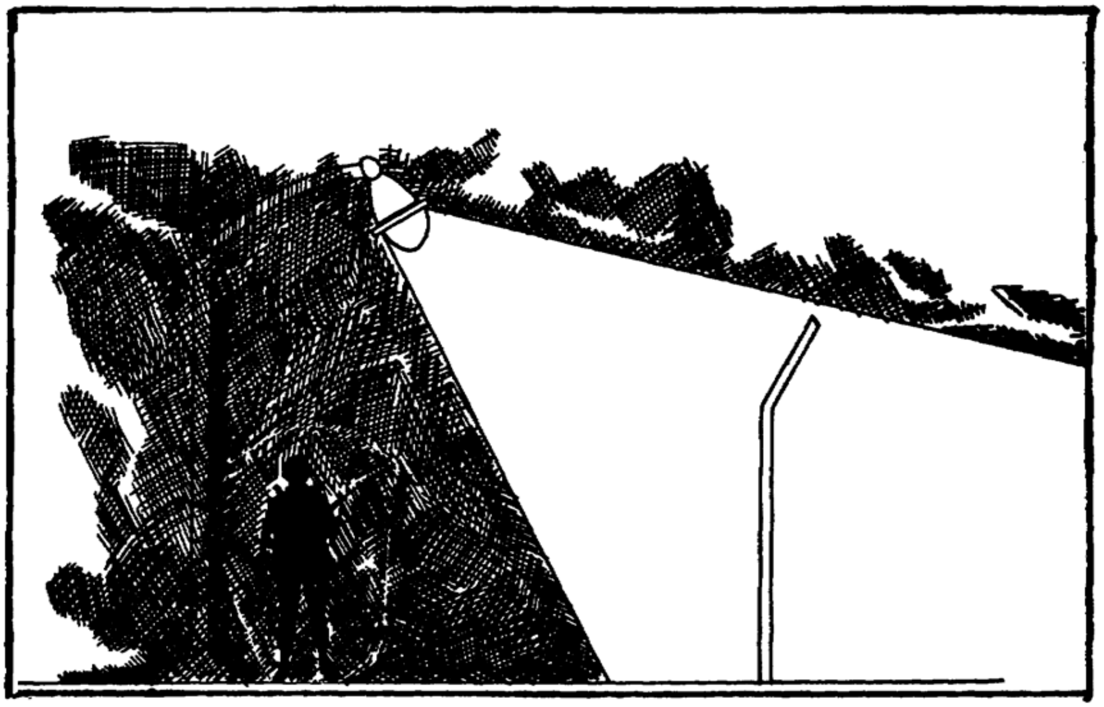


Figure 2-5. Boundary lighting (glare projection method)

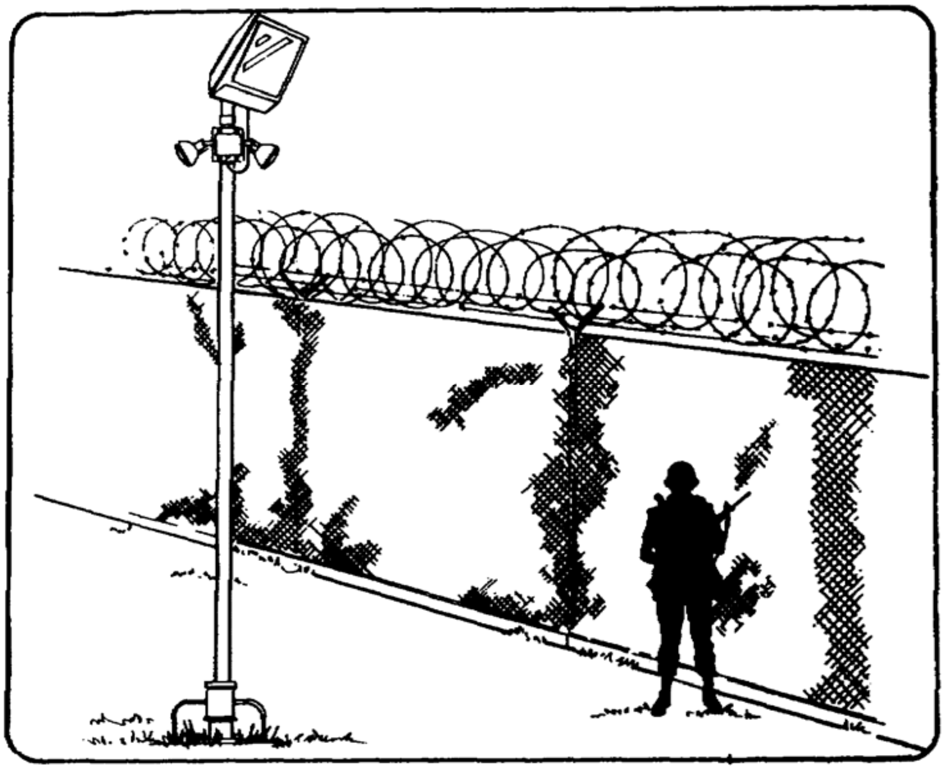


Figure 2-6. Boundary Lighting near adjoining property (controlled lighting).

9. Power Sources. Usually, the main power source at a post is a local public utility. The interest of the guard force begins at the points at which feeder power lines enter the post. An alternate source of power should be provided where the primary one is subject to interruptions or failures. Standby gasoline-driven generators with automatic starters will ensure continuous light. These generators begin to run upon the failure of outside power. However, they may be inadequate for sustained operations of the post. Generator or battery-powered portable and/or stationary lights should be available at key control points. They can be used in case of a complete failure. This is one in which even the secondary power supply of the post is rendered ineffective.

THIS PAGE LEFT BLANK INTENTIONALLY

LESSON 2

PRACTICE EXERCISE

REQUIREMENT. 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. Restricted areas may be administratively designated as which of the following?

   A. Limited, exclusion, controlled.
   B. Off-limit, exclusion, authorized personnel only.
   C. Controlled, authorized personnel only, exclusion.
   D. Sensitive, controlled, exclusion.

2. Which of the following statements is true concerning protective barriers?

   A. Protective barriers are designed to deter penetration by intruders.
   B. Areas not designated as restricted are not required to have protective barriers.
   C. Determination of the types of protective barriers must be based on what is being processed.
   D. Natural barriers always provide adequate protection.

3. Which of the following statements best describes an exclusion area?

   A. A building in an area having classified material which is of such a nature that access to the building would not be the same as access to material itself.
   B. A building on a military post storing classified material which is of such a nature that access to the building would be the same as access to the material itself.
   C. An area where the degree of control movement will be prescribed by the appropriate CO.
   D. An area in which special security measures are used to stop unauthorized access to classified data.

4. You have been asked by the provost marshal to advise the engineer crew on clear zone requirements along perimeter barriers. What should you advise them regarding clear zones?

- A. They are needed if perimeter lighting is inadequate.
- B. At least 30 feet is desirable between the barrier and inside structures.
- C. These zones must be plowed so that footprints can be spotted easily.
- D. At least 20 feet is mandatory between the barrier and outside structures.

5. You are discussing protective lighting with the lighting engineer. He should recommend a schedule for replacing lamps at what stage of their rated life?

- A. 60 percent of their rated life.
- B. 70 percent of their rated life.
- C. 80 percent of their rated life.

6. You are discussing wiring circuits for protective lighting with the illumination engineer. He would be CORRECT if he states which of the following?

- A. Series circuits cannot be used effectively.
- B. Multiple circuits cannot be used effectively.
- C. Both multiple and series circuits can be used effectively.
- D. A combination of both circuits must be used to be effective.

7. To obtain approval to designate a facility as a restricted area, whom would you contact?

- A. The installation provost marshal.
- B. A general officer.
- C. The post G2.
- D. The installation commander.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item   Correct Answer and Feedback

1.   A.   Limited, exclusion, controlled.
Examples are "exclusion,"... (page 2-8, para 9c).

2.   A.   Protective barriers are designed to deter penetration
They are used to... (page 2-2, para 1).

3.   B.   A building on a military post storing classified
A security interest of... (page 2-9, Part A, para 9d(l)(a)).

4.   D.   At least 20 feet are desirable between the barrier
When possible a clear zone of... (page 2-9, para 10).

5.   C.   80 percent of their rated life.
The ledger should be kept... (page 2-11, para 5e).

6.   C.   Both multiple and series circuits can be
Both multiple and series... (page 2-14, para 8).

7.   D.   The installation commander.
A restricted area must be... (page 2-8, para 8d).

LESSON 3

LOCKS AND KEY CONTROL

Critical Task: 191-386-0008

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to establish lock and key control procedures and inspect locking devices.

TERMINAL LEARNING OBJECTIVE:

ACTION: Establish lock and key control procedures and inspect locking devices.

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

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

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-50 and AR 380-5.

INTRODUCTION

Lock and key system of security is the most widely used means of protection. However, like the other security aids, alone it does not stop penetration. This system should be considered as a delay device; it requires one or more combinations of security steps and should be used as a back up to other security devices.

1. General:

It does not matter how good the quality or cost of locks is acclaimed to be; keep in mind that equally ingenious means have been found to open them. All locks can be opened with force and the right tools.

2. Survey the Security Area to Determine Requirements.

a. Physical security personnel must use the systems approach to provide a good security program. An analysis should be done to determine vulnerability and need for protection of security areas.

b. A survey will identify areas where protective countermeasures may be used. Examples are locking devices and keys. These areas will include:

(1) Warehouses.

(2) Shops.

(3) Storage areas.

(4) Safes.

(5) Filing cabinets.

(6) Door and gates.

3. The Physical Security Plan. It has been stated that a systems approach should be followed. The physical security plan will include lock security as a part of para 4, aids to security. This should occur once requirements have been identified. Items to be considered are discussed below.

a. Key custodian/alternate. A primary/alternate key custodian is the person who will:

(1) Be appointed in writing to issue and receive keys and maintain accountability for office, unit, or activity keys.

(2) Ensure that individuals are designated to issue, receive, and account for keys in his or her absence and that they clearly understand local key control procedures.

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

(4) Be listed on an access roster.

b. Key control register. The key control register must contain the following entries:

(1) Key number.

(2) Date and time of issuance.

(3) Printed name and signature of issuer.

(4) Printed name and signature of receiver.

(5) Date and time of return.

(6) Printed name and signature of receiver.

c. Number of keys and locks. The number of keys and locks in the system, including replacement or reserve locks must be recorded. Also, control must record the following items:

(1) Total number of keys.

(2) Number of keys issued.

(3) Number of keys on hand.

d. Location of keys and locks.

e. Location and contents of depositories, keys to be turned into each depository by building, area, or cabinet number.

f. Action required if keys are lost or stolen.

g. Frequency and method of lock rotation.

h. Inventory procedures. Keys and locks will be inventoried by serial number no less than semi-annually. Keys to locks in use which protect the property of an office, unit, or activity will be checked at the end of each duty day. A written record of the inventory will be retained until the next inventory is conducted.

i. Under no circumstances will any keys, locks, or alternate keys or locks be placed in a security container that contains or stores classified material.

4. Key and Lock Control of Classified Security Containers. The authorized locking device is dependent upon the level of classification of the material being secured.

a. Only those personnel with a bonafide need will be issued combinations or keys.

b. AR 380-5 dictates the changing of combinations to safe locks and padlocks securing classified material. Change should take place:

(1) When placed in use.

(2) Whenever an individual knowing the combination no longer requires access.

(3) When the combination has been subject to possible compromise.

(4) At least annually.

(5) When taken out of service.

c. There should always be sufficient numbers of spare locks on hand.

d. Spare keys and combination numbers should be treated as classified in some cases. This would occur if their locks are used for classified storage.

e. Maintain a key access list in the key storage container.

f. At the end of each shift, check key containers and contents. A key depository must be used to secure keys during nonoperational hours.

5. Locking Devices.

a. Key locks. A key lock can be picked by an expert in a few minutes. Loss and compromise of a key and the case in which an impression may be made should be considered. Determine the security value of such a key-type lock.

b. Conventional Combination Locks. This type lock may be opened by a skillful person. He may be able to determine the settings of the tumblers of a common three-position, dial-type combination lock. He does so through his sense of touch and hearing. Some combination locks may require several hours to open. An expert can open an average conventional combination lock in a few minutes.

c. Manipulation-Resistant Combination Locks. A manipulation-resistant lock is specially designed. The opening lever does not come in contact with the tumblers until the combination has been set.

d. Other Combination Locks. Combination locks with four or more tumblers may be desirable. These can be used for containers of highly important items.

e. Relocking Devices. A relocking device on a safe or vault door gives an added degree of security. Such a device increases the difficulty of opening a combination lock container. Forced entry is often accomplished by punching, drilling, or blocking the lock or its parts. A relocking device is recommended for heavy safes and vaults.

f. Interchangeable Cores. The interchangeable core system uses a type of lock with a removable core that can be replaced by another, using a different key. A control key is used for core removal and maintenance and is square shaped at the end. The operator key is used for opening and locking only and is rounded at the end. Its main features include the following:

(1) Cores may be quickly replaced. This instantly changes matching locks and keys when their security is compromised.

(2) Interchangeable cores are economical. This is due to reduction in maintenance costs and new lock expense.

(3) Such a system is flexible and can be engineered to the needs of the post.

(4) This system makes record keeping simple.

g. Cypher Locks. These are digital combination door locking devices.

6. Identifying Locking Devices Inspection Procedures. A periodic inspection should be instituted regarding all locks. This will determine the mechanism's effectiveness. It will also detect tampering and facilitate making replacements. A test key may be inserted no more than 1/4 inch into the keyway. Turn test key by hand; use the normal force required to open a lock. If the lock opens during inspection, it should be replaced immediately.

7. Locking Devices Maintenance Procedures. Maintenance procedures periodically performed on locking devices are varied. These include cleaning, lubricating and loosening "stuck" bolts. Also included is the removing of broken keys.

THIS PAGE LEFT BLANK INTENTIONALLY

LESSON 3

PRACTICE EXERCISE

REQUIREMENT. 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 discussing the control of keys for perimeter gates with the provost marshal. He correctly tells you that all keys used by the security force should be kept where?

   A. In a key depository which will be secured during nonworking hours.
   B. On one large key ring and maintained by the security supervisor.
   C. By security personnel who use them during nonworking hours.
   D. In the desk drawer of the security force CO during nonworking hours.

2. Combinations to safe locks and padlocks securing containers will be changed at least how often?

   A. Quarterly during each 12-month period.
   B. Twice during each 12-month period.
   C. Once during each 12-month period.
   D. every other month during each 12-month period.

3. Issuance of keys will be handled how?

   A. Kept to a minimum and retained under constant key control supervision.
   B. Receipted to anyone that desires access to a certain area.
   C. Kept to only immediate supervisors.
   D. Issued for personal retention; however, inventoried monthly.

4. A key custodian/alternate custodian is responsible for all of the following EXCEPT which one?

   A. Custody of master keys.
   B. Day-to-day account of keys.
   C. Investigation of lost keys.
   D. Inventory of keys.

LESSON 3

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item   Correct Answer and Feedback

1. A. In a key depository which will be secured
A key depository must be used... (page 3-4, para if).

2. C. Once during each 12 month period.
Annually. (page 3-3, para 4b(4)).

3. A. Kept to a minimum and retained under constant
Only those personnel with a... (page 3-2, para 3a(l)).

4. C. Investigation of lost keys.
Key custodian/alternate. (page 3-2, para 3a).

LESSON 4

MP WORKING DOGS

Critical Task: 191-386-0013

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to use and maintain MP working and sentry dogs.

TERMINAL LEARNING OBJECTIVE:

ACTION: Provide recommendations for maintenance and utilization of MP working and sentry dogs.

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

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

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-12, FM 3-19.30, FM 19-35, AFR 125-5, and DA PAM 190-12.

INTRODUCTION

The mission of the MP working dog is to detect intruders and alert his handler. When necessary, he is also to pursue, attack, and hold any intruder who tries to escape. Working dogs exert a strong psychological deterrent to criminal acts. Normally, the dog has done his job by detecting an intruder and alerting the handler. The handler then becomes responsible. He must identify and apprehend the subject.

1. General.

a. Working dogs augment other physical security measures. They do so by increasing the security given sensitive areas. Most advantageous is their keen sense of hearing and smell. During the hours of darkness or poor visibility a security guard's vision is restricted, but dogs are very good intrusion detections systems. Training is meant to develop distrust and suspicion. It is also designed to develop the will to attack all human beings other than its handler.

b. MP dogs are being trained in various aspects of law enforcement. Formal training programs are used. The mission of MP working dogs includes their use in law enforcement, physical security and as a deterrent to criminal activities.

2. Physical Requirements of Working dogs.

a. All dogs trained and used as working dogs by the Army are procured by the Department of Defense Dog Center (DODDC) at Lackland AFB, TX. Usually, only German Shepherd-type dogs are accepted for use by the Army, but other dog breeds are sometimes used for special purposes.

b. German Shepherd-type dogs are used as the standard breed, This is due to the unique combination of traits they have. Shepherds are intelligent, dependable and predictable. They are easily trained and usually moderately aggressive. Also, they can adapt readily to almost any climate conditions. Many dog breeds exhibit some or most of these same traits, but the shepherd most consistently exhibits all of these traits.

c. Dogs offered to the DODDC must be between 1 and 3 years of age. Either male or female dogs are acceptable. Dogs do not have to be pure bred or registered, but they must display the predominant characteristics of their breed. Shepherds must be at least 23 inches high at the shoulder and must weigh at least 55 pounds or more.

d. Since military duties demand strength and stamina, all dogs must be in excellent physical condition. There should be no missing canine teeth. Minor physical defects may be acceptable, provided they do not impair a dog's ability to work. They should be mildly to moderately aggressive, and they must not be gun shy. Overly aggressive dogs may not be acceptable.

e. After dogs have been accepted for military use by the DODDC, they are matched with new handlers. Then the dogs are entered into patrol training in the MWD Studies Branch. This is based at the Security Police Academy, Lackland AFB. If, during this training period, a dog fails to progress, it may be "washed back" to repeat training. When training is over, the dog may be shipped to fill vacancies in the field; or may be held over at Lackland to help in training other handlers. No dogs are entered into either narcotics and explosives detection courses until there is a need for that type of dog.

3. Definitions of Behavior Traits.

a. Sensitivity. Sensitivity refers to the type and degree of response a dog shows to a certain stimulus. An oversensitive dog is startled by a stimulus of low intensity; and undersensitive dog would not be disturbed by the same stimulus. The response of an oversensitive dog is often one of shyness or fright. The response of an under-sensitive dog, given the same stimulus, may only turn its head. He will show no response at all.

b. Aggressiveness. Dogs vary widely in levels of aggression. There are three general categories of aggressiveness.

(1) Overaggressive. Dog, when spotting agitator, usually becomes greatly excited. He lunges at his leash, barks, and continues to bark after the agitator leaves.

(2) Underaggressive. Dog reacts to agitator by cowering, hiding or trying to run away.

(3) Moderately aggressive. Dog reacts upon seeing agitator. He shows suspicion and eagerness to move toward the agitator. This is the best category of dog to train for patrol.

4. Characteristics of Working Dogs. Most of us think the only advantages dogs have over people are their superior senses of smell and hearing. We think the same about their superior ability to visually detect motion. While these beliefs are true, they are not complete. A more important advantage is that a dog can be trained to react consistently to certain stimuli; he can be trained to this consistency in a way that immediately alerts the handler. People quickly adapt to changes in their environment, but military working dogs are trained to react to changes. This includes particularly those changes beyond the detection abilities of people. The dog's reward reinforces his behavior and motivates him to repeat the actions. People react to what they think a stimulus means. Military working dogs simply react to the stimulus; they let their handlers decide what it means.

a. Patrol dogs. These dogs are the most versatile of the MP working dogs. Since they are always controllable and composed, they work around people with safety. Due to their ability to be controlled, a leash is not necessarily required. Patrol dogs are trained to attack only on command of the handler. However, a sudden aggressive movement toward the dog or handler may also trigger an attack.

b. Explosive detector dogs. These dogs are in high demand and have an acute sense of smell. Training teaches them to discriminate the scent of explosives.

c. Narcotic detector dogs. Specialized training allows them to detect marijuana, heroin, and other related substances.

5. Capabilities of the MP Working Dog.

a. MP working dogs give law enforcement and security personnel a degree of force in apprehending criminals. They can do so when lesser measures of force would not be effective. Before releasing a military dog during an apprehension, give an order to the suspect to halt. Releasing a sentry dog during apprehension is a greater measure of force than releasing a patrol dog. The stable temperament of patrol dogs allows safe apprehension and detaining of criminals.

b. Detecting intruders and alerting handlers of their presence is another capability of working dogs. Dogs are trained to give warning to their handler. They do so by growling or barking, or by silent reaction. The handler must be prepared to cope with the situation as circumstances dictate. The dog will attack on command of his handler.

c. Dogs may pursue, attack and hold offenders who resist apprehension. Working dogs can inflict great damage when released to attack. Release policies should not be too restrictive; if so, psychological deterrent is negated. However, these policies must prevent bites from occurring through careless actions of the handler.

d. Working dogs can be used effectively to search and clear buildings and large open areas of criminals or other unauthorized personnel. They are not effective in street crimes such as robbery, car theft, and assaults. Sabotage, arson, and pilferage can be combatted by using dogs. Buildings found open under suspicious circumstances can be searched without endangering the lives of security personnel.

e. Working dogs track fleeing criminals. They also track lost children or other persons who, for humanitarian reasons, must be found by the authorities. When use of tracking skill is contemplated, the crime scene should be secured; movement of personnel should be minimized. When done promptly, tracking skills can be used after burglaries and robberies. They can also be used upon discovery of abandoned stolen vehicles.

f. Detecting the presence of certain narcotics and explosives by scent alone is extremely valuable.

g. Working dogs provide a strong psychological deterrent to certain types of criminal acts. Public demonstrations, patrol routes on gates, and the escort of government funds are examples. At these times the use of dogs has a psychological impact. AR 190-12 permits the use of dogs for crowd control with CO's authorization.

6. Military Police Dog Team. An MP working dog and its handler are trained to work together. They are to perform law enforcement and/or physical security duties. (See Figure 4-1.)

a. Dogs are social animals that seek human companionship. Because of this, the relationship between the dog and its handler is a critical ingredient. It can greatly affect the team's effectiveness.

b. Dogs with suitable temperaments for police service do not give affection freely. However, once earned, it is not easily relinquished. Special considerations must be allowed to protect the relationship between a dog and its handler.

c. During the absence of the handler, the dog should not be used.

d. Personnel chosen for dog handlers must show qualities of reasonable intelligence, resourcefulness, and patience; they should also possess a high degree of affection for animals.

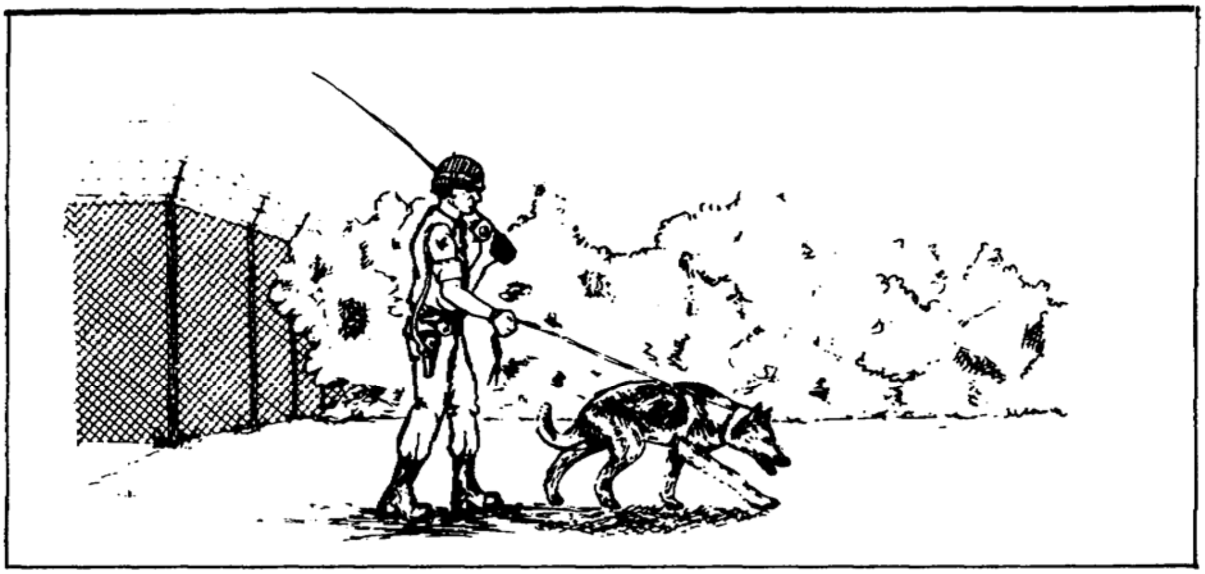


Figure 4-1. Military police dog team

7. Replacement of Military Working Dogs.

a. Using units should schedule military working dogs for replacement during the fiscal year in which they will reach 8 years of age. Dogs may be continued on duty when they are in good health and are performing well. This must be determined by the local unit CO and the attending veterinarian.

b. Sometimes the death of a dog creates an urgent need for replacement. Often, this need cannot be satisfied by normal programming. At these times, a replacement may be obtained from Air Training Command (ATC), Lackland AFB, TX. A special short course is available to provide previously trained working dog handlers with dogs. Major commands must request this service directly from ATC Headquarters. DA approval is not required.

c. MP working dogs may be judged retrainable and physically fit by the major command and the supporting veterinarian. If so, these dogs may be transferred from PCS to Lackland for retraining. Commands with retrainable dogs must report them to their major command; they will then determine whether an internal need exists within CONUS or the major command. This major command must approve all dog transfers for retraining at Lackland. Before the transfer, the post concerned must furnish Lackland AFB the following information; they must then await permission and shipping instructions.

(1) Age of dog and length of service.

(2) Reason for transfer.

(3) Statement regarding the dog's temperament.

(4) A report by the responsible veterinarian of a recent complete physical examination (within 14 days). This must include a statement that the animal has no contagious disease. It should also be stated that the dog has no health problems that prevent it from being placed in training immediately. The veterinarian's report will be very specific in certain parts of the examination. These would be the parts about the presence or symptoms of hip dysphasia. The report should include (should the veterinarian deem necessary) the results of radiological examination.

(5) A report of a blood test done, within the past 30 days, for filarial worms. A concentration technique, such as the Knott's method, must be used.

(6) A report of a recent feces examination for intestinal parasitism.

(7) Dates of the most recent immunization against rabies, canine distemper and infectious canine hepatitis, and leptospirosis. Specify the products used in each case.

(8) Statement as to whether a crate is required for shipment of the dog.

8. Patrol Dogs.

a. Patrol dog teams are the most versatile canine assets available. This is due to their stable temperament and multiple skills. Because of these attributes, they function effectively in many facets of law enforcement or physical security operations.

b. Versatility is a valuable commodity in any resource. With patrol dogs, it is probably their most important trait. They can expand law enforcement capabilities of an Army post; they can increase the physical security posture. These capabilities have been combined into one type of police working dog. Therefore, flexibility of employment is achieved; total cost effectiveness becomes attainable; and full use of each dog handler's police training is assured. Complete uniformity in performance among various teams is not possible, but all patrol dogs are able to perform many tasks in an acceptable way.

(1) Detect presence of unauthorized personnel.

(2) Alert handler to presence of intruders.

(3) Attack on command.

(4) Cease attack on command.

(5) Leave attack before consummation, if required.

(6) Track humans other than their handlers.

(7) Search buildings and open areas for criminals.

(8) Perform reliably off the leash.

(9) Work safely and effectively around people.

c. Some patrol dogs are trained to detect narcotics or explosives. This causes the dog to be more cost effective. All dogs are not suitable for this type of work. Therefore, only certain patrol dogs with exceptional senses of smell are chosen for this specialized training. Sometimes this capability is required at a particular post. If so, it should be indicated in the procurement request. (NOTE: This capability must be in the request for training quotas; it must be fully justified in MTOE documentation for dog/handler.

9. Employment Techniques.

a. Patrol dog teams can perform effectively any law enforcement or physical security-related task that requires canine skills. In doing those tasks, teams may be used in the following ways:

(1) Mobile patrols.

(2) Dismounted patrols.

(3) On fixed posts.

(4) A combination of the above.

b. For discussion purposes, operational functions may be divided into three principal classes:

(1) Law enforcement.

(2) Physical security.

(3) Deterrent operations.

Grouping functions in this manner is somewhat arbitrary, because canine skills used in one category can also be used in another. Furthermore, the deterrent aspects of patrol dog use apply across the board. Despite this fact, a functional grouping of this type aids the discussion of patrol dog techniques. Rigid adherence to these categories is not required during actual service. This is because of the flexibility inherent to patrol dog teams.

10. Law Enforcement.

a. During each shift, all patrol dog assets performing law enforcement should be under operational control of the MP desk sergeant; they should be capable of immediate response to his direction. For this reason, radio communications are necessary for dismounted as well as mounted patrol elements. Variance from this procedure may be required. Such variance may be needed to meet needs unique to a certain post of activity.

b. Normally, at least one patrol dog team should support each duty shift. Most teams should be assigned duties as mounted patrol; most should also be required to function in about the same capacity as a noncanine unit. This practice increases exposure to the public, and it helps develop a psychological deterrent to crime. It also contributes to the overall cost effectiveness of the team.

c. At times, dismounted patrols are extremely effective. This is especially true of dependent housing areas. Also included are areas near troop billets, adjacent to EM clubs, around PXs and theaters, or in poorly lighted parking lots. Immediately following payday, dismounted patrol dog teams may also be used to patrol recreation areas, parks, or heavily forested areas. These are sites where soldiers use shortcuts between post facilities and their barracks. Employment of this nature reduces loitering; it minimizes opportunity for criminal acts and should be used both day and night.

d. When buildings are found open, or a burglary is otherwise suspected, a patrol dog team should be sent to the scene. A building search should then be conducted by the dog and its handler. Actions of this type can be accomplished quickly and efficiently by the patrol dog. Such actions can take place without endangering the lives of law enforcement personnel. To do so without canine aid is hazardous and time-consuming; it stands only a limited chance of success. A voice warning must be given before a dog is released to search an open building.

e. Tracking skills may also be used to aid MPs in gaining information about a crime. These skills also aid in discovering evidence left at the scene and trailing suspects until captured. When used promptly, tracking skills can be extremely useful at the scene of burglaries, robberies and rapes. Tracking skills are also useful upon the discovery of abandoned stolen vehicles. Although an apprehension cannot be expected after each tracking, much valuable data can be obtained. Such data includes, but is not limited to, ascertaining the direction of flight, discovering abandoned articles or items of evidence, and determining whether or not the subject fled on foot or in a vehicle.

f. Crime scene searches should be done after using patrol dogs. All law enforcement personnel should be instructed accordingly. Above all, tracking skills should not be used as a last resort after all other efforts have failed. This is true regardless of whether the subject is a criminal, a lost child, an elderly person, or a mental patient.

11. Physical Security.

a. Patrol dog teams may also perform valuable service during physical security operations. This is especially true in cases where the highly aggressive nature of the sentry dog is unacceptable. Patrol teams may be used either as mounted or dismounted patrols, or, they may be used to augment security alert teams and backup alert forces that respond to emergencies. They are effective on perimeter security posts at isolated sites. However, the patrol dog's multiple skills make this type of duty inadvisable. This is true if the duty is to be performed on a permanent basis. Sentry dogs can be used to perform such tasks with equal effectiveness and at less cost. However, sometimes perimeter security is needed at sites where external distractions can be expected. Then the use of patrol dogs should be given consideration.

b. Patrol dog teams are also effective in and around freight yards, warehouse areas, and ammunition depots. They are useful also in and around maintenance facilities and public utilities that operate on a 24-hour basis. Distractions inherent to such operations have little impact upon the emotional stability or effectiveness of patrol dogs. In this type environment the psychological value of the animal's functional effectiveness, psychological deterrence is more of a threat than a useful enforcement tool. For that reason, this deterrent should not be relied upon.

c. Patrol dog teams are also useful in securing large depot complexes or like activities; they can greatly reduce the need for two-man security patrols. Such teams can be used to screen buildings for stay-behind pilferers, and they can respond to all situations where buildings are found unsecured. These teams can respond, also, when there are other reasons to suspect that a housebreaking has occurred. They also function well at points of entry and exit; there they bolster the effectiveness of pass and badge systems. If the perimeter of a sensitive area is penetrated, patrol dogs can be used to track the intruder. They can re-establish contact with him and make the apprehension.

d. Essentially, then, many patrol dog skills used in law enforcement functions are also valuable when used in physical security. For this reason, physical security planners should carefully assess operational requirements at their posts. By so doing, they can identify areas where patrol dog skills would be of value.

12. Deterrent Operations.

a. Deterrent operations include all activities in which patrol dog teams are used for the psychological impact of their presence. During those operations the actual use of their skills is possible but not expected.

b. Such activities include public demonstrations of patrol dog capabilities. They also include patrol routes that include main gates to the post and areas where prisoner work details are used. These dogs also act as deterrents when escorting government funds.

c. Deterrent operations can be implemented to reduce crime and to save manpower. They may also be used to minimize situations requiring use of patrol dog attack skills. All that is needed is initiative, imagination, and sound police planning.

13. Economy of Force.

a. Patrol dogs not only aid total use of canine skills, they also permit supervisors to make optimum use of personnel resources. Patrol dogs can be used as an economy of force measure. They can replace dismounted sentry posts; they can reduce the number of MPs used to conduct surveillances of large, open areas; and they can be used to spot-check warehouses containing material highly subject to theft.

b. When performing patrol duty, the dog handler does not require the presence of another MP to aid in performing routine tasks. Therefore, the police skills of the dog handler become a usable commodity, since he can perform any task normally assigned an MP. Unlike the handler who works specialty dogs, he is in no way restricted by the presence of his animal. Instead, the presence of the animal expands his potential use.

c. Experience also shows that the presence of canine units in high crime areas can reduce the need for other MP resources. This achieves further savings in manpower. Certainly the need for two-man patrols is lessened in cases where patrol dog teams can promptly respond to requests for aid. The need for two-man patrols is also lessened when the dog teams can routinely back up other patrol elements.

d. When used for routine law enforcement tasks, patrol dogs can normally perform 8-hour tours of duty. This is especially true when they are used as mobile patrols. Limiting factors in this respect stem more from climatic conditions and availability of suitable transportation than from job/task considerations. In contingency cases, patrol dogs can work 12-hour shifts on mounted patrols without great loss of efficiency. In determining length of duty tours, the following items must be considered:

(1) Needs of the command.

(2) Climate and terrain.

(3) Transportation available.

(4) Tasks to be performed.

(5) Ability of the dog.

14. Controlled Aggressiveness.

a. To be successful as a law enforcement tool, patrol dogs must be able to work around people. They must do so without becoming distracted.

b. On the other hand, some patrol dogs will become too friendly; they will fail to perform well when aggression is required. This is a particularly acute problem, since it affects the dog's reliability under stress. Generally, this can be remedied by emphasizing attack drills during training. Remedy may also occur by assigning the team patrol duties that lessen friendly associations with the public. An alternative is to rotate the team; move it from routine patrol to physical security duty at an isolated site.

c. The balance between socialization and aggressiveness is critical, and its maintenance requires keen observation and sound judgement by field supervisors. Lack of aggressiveness in a patrol dog is not permissible; it is enough justification for extensive in-service training. It may also justify rejection, if the condition cannot be remedied. Highly aggressive but controllable dogs are preferable to under aggressive ones which are not reliable under stress.

d. Operational safety does not require fawning or playful animals. These are dogs that prefer home and hearth to the patrol car. Operational safety requires controlled aggressiveness. Its ingredients are sound temperament and thorough training; another ingredient is absolute compliance with the commands of the handler. Upon completion of training, all patrol dog teams should exhibit these traits. Field supervisors must ensure these traits are maintained.

e. Controlled aggressiveness of the patrol dog must sometimes be shown if public acceptance is to be won. However, the showing of affection or petting of the dog should be restricted generally to the handler.

15. In-service Training.

a. Refresher training must be conducted as required. This will assure maintenance of technical proficiency in all facets of patrol dog skills. This is accomplished by an effective in-service training program. It should be one designed to meet the needs of the post concerned. In-service training can correct operational deficiencies in a particular patrol dog team. Deficiencies are identified by using evaluation procedures. For the most part, these procedures are separate from the in-service program.

b. Patrol dogs are required to demonstrate their skill on a regular basis. They are required to display these skills under a variety of operational situations. They must demonstrate skills under constant scrutiny from the public and the command structure, Many aspects of patrol dog use can be evaluated by personnel. Even those who have little or no knowledge of canine behavior or training can evaluate some aspects.

c. At this point, we can say that the sentry dog is best suited for areas that are isolated and relatively free of distractions, while the patrol dog is best suited for duty around populated areas. This dog is also more suited where the military mission requires both physical security and law enforcement.

16. Narcotic Detector Dogs. There is widespread increase today of drug trafficking and use. Because of this increase, narcotic detector dogs may be necessary. They must be available to assist law enforcement efforts.

17. Explosive Detector Dogs. The whole world has witnessed an alarming rise in bombing attempts against property of all types. This crime will continue and probably increase. Today more and more dissidents adopt this tactic to gain attention and achieve their goals. One of the best countermeasures to this increase is the deterrent value and the detection capabilities of the explosive detector dog team. They are known by both military and civilian security and law enforcement forces. These persons consider the team as the best weapon now available in the war against terrorism.

18. Use of Force. COs using MP working dogs will establish clear policies and procedures. These will govern the release of patrol and/or sentry dogs. Such release will be in accordance with the provisions of AR 190-28. This regulation covers Use of Force by Personnel Engaged in Law Enforcement and Security Duties. COs will also ensure that all MP working dog handlers are thoroughly familiar with these regulations. MP working dogs will not be used to get around restrictions on law officers imposed by law or regulations.

19. Team Concept. Two conditions dictate how a section is organized and managed: one is the size of the individual MP working dog section; the second is the concept of employment of the teams.

a. Dual Qualification/Dual Employment. Patrol detector dog teams perform normal patrol dog team duties. Sometimes these dogs are not required for detection work, so they should not be limited to these duties only. Failure to assign them to a full range of duties causes them to quickly lose their basic patrol dog capabilities.

b. Competitive Events. Teams are encouraged to take part in competitions. These may be conducted by civilian or MP agencies or recognized canine associations. These activities enhance MP and community relations programs. Competitions also promote higher levels of dog team proficiency.

20. Records. When a dog is procured, a permanent administrative record file will be initiated by the procuring post. Included must be a permanent veterinary health record. Together, the administrative and health records constitute a permanent record file. The record file must accompany the dog on every transfer, and it must be kept current by the organization to which the dog is assigned. Upon death or transfer of the dog to a non-military agency, the dog's permanent field record file will be forwarded to Lackland, TX, Central Repository for Military Dog Records.

a. Administrative Records.

(1) Work Dog Records. When a dog is procured, the procurement officer prepares Sections I and II of the Working Dog Record. When the dog leaves the service, the organization having the dog completes Section III.

(2) DA Form 2807-R covers Military Working Dog Training and Utilization Record. This is a record of the daily training activity. It shows the continuation training given to the dog and provides a daily record of the use of each military working dog.

(3) DA Form 2810-R concerns Working Dog Feeding and Weight Chart. This form is used by the handler to keep a permanent record of a dog's weight. This data is useful for reference purposes.

b. Medical Records. Only veterinary personnel are authorized to make entries on a dog's medical record.

21. Kennel Facilities. COs will ensure that kennels are built as described in DA Pam 190-12. MP working dog facilities will be placed in areas offering the least distraction. Also, they will be placed where the dogs will not become a nuisance to personnel. The following facilities and operational needs will be provided at all kennel areas:

a. A potable water supply (hot and cold) or, in case of emergency, water trailers and immersion heaters. This will be located in the vicinity of the kennel kitchen area.

b. Adequate lighting in and around the kennels.

c. Salvage tenting or tarpaulins to provide shade. These may also be used to aid in the isolation of one or more kennels.

d. Sanitary conditions. These will be maintained in the kennels, runs, food storage and preparation space, and surrounding area. Kennels will be thoroughly cleaned each day. Stools should be policed twice daily. The kennels will be thoroughly disinfected weekly.

e. Insect and rodent control. Immediate disposal of all waste material will aid in this control. Rodents are attracted to dry meal and scraps; therefore, all such material should be stored in rodent-proof containers.

f. Tall grass, weeds, and brush control. Areas such as these will be removed if infested with ticks. Preferably the method used will be controlled burning under fire department supervision.

22. Care and Grooming.

a. The MP working dog handler is responsible for its daily care and grooming. He is also responsible for the daily police of the dog kennel and run. His duties include the feeding of a balanced diet to the dog as recommended by a veterinarian.

b. Dog food will be requisitioned using Federal Specification N-F-170 under FSC, Class 8710; "Foraged Feed" or feed, high caloric, medicated, FSN 8710-403-4565 (MSD); or feed, high caloric, nonmedicated, FSN, 8710-144-6834

(MSD). COs may purchase food from local available sources if it is more economical.

c. Special diets may be procured and fed to individual dogs. Such diets are given when a veterinarian indicates other than standard is required.

d. The dog food must be manufactured, packaged, stored, and transported in conformance with sanitary standards for food plants (MILOSTD 668) as determined by the military veterinary services.

23. Veterinarian Support.

a. The Surgeon General (SG) provides professional support for military dogs. He does so through his veterinary service. This includes medical care and treatment of dogs at the training sites and assigned posts. The SG reviews plans for new construction and changes of kennels, support buildings, and sites. He provides for sanitary inspections of kennel areas. The training and instructing of dog handlers and supervisors in care, management, feeding, and first aid of dogs is provided by the SG. Additionally, special studies in matters affecting the health, kenneling, and feeding of dogs are conducted as required. The post CO must include veterinary requirements for medical material. This will be used in the treatment and care of military dogs. Civilian veterinary care of dogs is authorized in emergencies. Such might occur when a military veterinarian is not available; or it may occur when veterinary medical requirements for care are beyond the capabilities of the supporting facility in accordance with AR 40-3. Cross-servicing agreements may be used for veterinary services. This will depend upon available resources.

b. The dog handler is responsible for first aid treatment for his dog. He must also be able to recognize illness or injury that requires professional veterinary care. Veterinary drugs and supplies necessary for first aid treatment will be provided as directed by the command veterinarian. He will make provision to each dog team from resources available to the attending veterinarian. Each dog handler will receive a minimum of one hour training in first aid per quarter. Such training will be done in accordance with TM 8-450 and FM 20-20, and it will be recorded on the Sentry/Patrol Dog Training and Utilization Record.

24. The proper employment and use of MP working dogs have added new and more flexible support to all aspects of security and law enforcement. The MP working dogs' capabilities combined with your efforts in understanding and supporting their importance to physical security can add a new dimension of security to your facility or installation.

LESSON 4

PRACTICE EXERCISE

REQUIREMENT. 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 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. In accordance with what regulation can patrol dogs be used for controlling crowds?

   A. AR 190-12.
   B. AR 190-13.
   C. AR 190-50.

2. Which of the following is the most versatile MP working dog?

   A. Sentry.
   B. Narcotic.
   C. Explosive Detector.
   D. Patrol.

3. Which of the following applies to an MP working dog?

   A. Does not seek human companionship.
   B. Gives affection freely.
   C. Should not be used during the absence of the handler.
   D. Must possess a suitable temperament because it works with many handlers.

4. Which is best to use for security around a populated area?

   A. Sentry dog without handler.
   B. Sentry dog with handler.
   C. Patrol dog with handler.
   D. Patrol dog without handler.

5. To ensure accuracy, who makes all entries on a dog's medical records?

   A. Handler.
   B. Veterinarian.
   C. Kennel master.
   D. Legal office.

LESSON 4

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item   Correct Answer and Feedback

1. A. AR 190-12.
AR 190-12 permits the use... (page 4-4, para 5g).

2. D. Patrol.
Patrol dog teams... (page 4-6, para 8a).

3. C. Should not be used during the absence
During the absence of the (page 4-4, para 6c).

4. C. Patrol dog with handler.
Work safely and effectively... (page 4-7, para 8b(9)).

5. B. Veterinarian.
Only veterinary personnel are... (page 4-13, para 20b).

LESSON 5

INTRANSIT SECURITY

Critical Task: 191-386-0015

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to determine intransit security requirements.

TERMINAL LEARNING OBJECTIVE:

ACTION: Provide recommendations for port and vessel, motor, and railway security.

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

STANDARD: You must complete all exercises for each lesson. You must take the final subcourse examination and earn a score of 75 percent correct answers.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-11, AR 190-14, FM 3-19.30, and DOD 5100.76-M.

INTRODUCTION

The Army is a mobile operation. It is capable of responding to defense needs world-wide. To ensure mission success, safe transport of resources must be assured. Each movement of resource will be unique, because the type of shipment and mode of transportation differs.

1. General.

a. Cargoes in transit are vulnerable to both overt and covert threats. Enemy or guerilla attack or ambush are examples of overt threats; sabotage is an example of a covert threat. Either may occur while the carrier is at a standstill or while it is moving. MPs and security personnel must be constantly aware of all these hazards; they must be trained and prepared to cope with them. They should be able to handle these hazards from the point of origin of cargo to the final destination.

b. The responsibility of the cosigner, the carrier and the consignee must be clearly established. This will provide for the security of property and material in transit. The protection of such property and material is, in general, the responsibility of the one who has custody of it. However, this varies according to the size of the shipment and the means of transportation.

2. Modes of Transportation. Cargo is shipped and/or received by an installation in one or more modes of transportation. The modes are: aircraft, railroad, truck, or ship. Each mode has security problems peculiar only to that mode; therefore, security needs must be evaluated on an individual basis. Evaluation should include the type of threat, criticality, and vulnerability.

3. Types of Shipment. The modes of transportation are broken down into the types of shipment. These types include the following:

a. Classified. This is cargo containing material classified in the interest of national defense.

b. Hazardous. Cargo that is explosive, flammable, toxic, or any combination of these is hazardous.

c. General cargo. This describes cargo that is not classified or hazardous.

d. Combination of classified, hazardous, and general.

e. Protected cargo. Such freight is further broken down into the following categories.

(1) Sensitive. Items that have ready use during civil disturbances by criminal elements. If in the hands of militants or revolutionary groups this cargo presents a definite threat to public safety. Examples of such cargo are small arms, ammunition, and explosives.

(2) Pilferable. Items vulnerable and having a ready sale potential in illicit markets are in this category. These items include alcoholic beverages, radios, etc.

(3) Controlled. Items requiring added control and security in accordance with published regulations and statutes. Examples are money, negotiable instruments, and narcotics. Other examples are registered mail, precious metal alloys, and drug abuse control items.

4. Degrees of Cargo Control. There are three degrees of cargo control:

a. Minimum. This is provided for all cargo.

b. Medium. Provided for high-value cargo with a ready resale, medium control may also be given to other cargo as designated.

c. Maximum. This control is provided classified material, small arms and ammunition, and other materials requiring strict control.

5. Analysis of Security Needs. If adequate cargo security is to be provided, physical security personnel must consider several elements. They must

determine the threat and sensitivity of the cargo, and its vulnerability. They must also consider the mode of transportation in deciding the degree of security required. The degree and type of security needed is determined by a number of things.

a. Facility size and location.

b. Complexity of storage for shipment.

c. Volume/value of shipment.

d. Economic and geographic situation.

e. Security/law enforcement available.

f. Number and location of transit shipment.

g. Local crime statistics.

6. Cargo Security System.

a. During the movement of cargo, the terminal operation is the most vulnerable place during the loading and unloading. The fact that the carrier is at a stand still presents an opportunity for pilferage and sabotage. Both loading and unloading should be done as quickly as possible. When loading is complete, the carrier should be moved as soon as possible. Unloading should begin as soon as the carrier arrives at its destination. Immediate handling of cargo reduces the risk of loss.

b. Facility personnel who work with the cargo directly could be your biggest asset or liability. Personnel should be screened prior to employment. Once assigned, security education programs should be started, These should stress the moral wrong of pilferaging and individual responsibility for accounting for cargo. The following are guidelines within the control of the security officer's influence:

(1) Require piece counts when cargo is moved to and from vehicles. Require this also when cargo is moved in and out of storage areas, vessels, railcars, etc. Insist on clear identification of those who conduct such counts. These people include drivers, checkers, receiving personnel, or other designated parties.

(2) Each person handling a shipment at each stage of transit should be required to tally and sign certifying shipment intact.

(3) Verify identity of carrier and carrier employee.

c. False invoices and receipts for shipments present an area vulnerable to theft. Blank government bills of lading and uncontrolled documents for movement should be eliminated. Simple countermeasures such as the following, may be used:

(1) Shipping.

(a) Preparing legible bills of lading.

(b) Rotating driver among runs.

(c) Changing truck stops frequently.

(d) On multipiece shipments, labeling by shippers of each package.

(e) Segregating shipping operation from receiving operation.

(2) Receiving.

(a) Receiving personnel should use prenumbered forms. On these are recorded deliverable merchandise. Copies should be sent to purchasing and accounts payable.

(b) Personnel should report discrepancies immediately to the terminal manager and/or security officer for investigation.

(c) Personnel should compare delivery receipts by the local driver; terminal control copies and all bills should be accounted for.

7. Cargo Loss and Prevention. Many factors add to the loss of billions of dollars to the government in cargo each year. Unfortunately, no program could possibly eliminate all losses; however, an awareness, re-enforced with appropriate countermeasures, could minimize loss.

a. Cargo plus apathy equals loss. Personnel charged with the responsibilities of shipping, transporting and receiving of cargo must be indoctrinated; they must be kept proficient in security procedures. All personnel must be aware of their responsibilities. Ensuring high employee morale is a valuable management tool. Such morale aids the solicitation of cooperation in security matters.

b. As stated before, there is one way of ensuring the security of cargo in transit: that is by having the responsibility of the cosigner, the carrier and the consignee clearly established. The protection of property and materiel in transit is the duty of the one who has custody of the shipment. Designating responsibility encourages supervision. No supervision invites pilferaging and sabotage.

c. Preparation of a packing list is necessary on all shipments; this aids the transportation officer in determining shortages.

d. The lack of perimeter fencing and port lighting contributes to the loss of cargo. Such security measures are a must around cargo warehouses, railways, and vehicle and pedestrian gates.

e. Entrance gates to activities should be limited to the minimum required for safe and efficient operation. Too many entrances and exits demands more manpower than is possible at times. Conditions such as these allow for unauthorized movement of cargo.

f. Unauthorized personnel or vehicles (especially private vehicles) in areas makes removal of cargo easy.

8. Physical Security Measures to Enhance Cargo Security.

a. Perimeter barriers. These include fences, walls, grills, and roadblocks, designed to deter access. Entry control stations should be provided at main perimeter entrances.

b. Protective lighting. This measure is desirable for sensitive areas or structures within a perimeter, which are under specific observation. Such areas or structures include pier and dock, cargo storage areas, railcar and truck loading points where night operations occur.

c. Locking devices. Used on railroad cars, trucks, and other containers, these devices serve to delay access. They are not, however, positive bars to entry; other security measures are required as back-up.

d. Intrusion detection alarm systems (IDS). If applicable, these are used to detect unauthorized persons at the entry point. Each need must be analyzed individually to determine proper use.

e. Positive personnel movement control system. Such a system must be established and maintained to preclude unauthorized entry. This system will also facilitate authorized entry to personnel control points. Security ID cards and badges add to effective movement control.

f. Security education programs. Inspire security consciousness by personnel (military and civilian). In turn, active support by personnel is secured.

g. Spot searches. Searches of individuals and vehicles may occasionally detect attempts of theft if done at unannounced times and places. This serves as a psychological deterrent.

h. Containerization of supplies and equipment. This action results in reduction of loss of or damage to cargo. It does so only if emphasis is placed on security during filling, sealing, storage (shipper/receiver), and shipment (on-loading and off-loading). One disadvantage may be that loss of cargo may not be determined for some time. Such would be the case unless periodic inspections of containers are done to detect tampering.

i. Seals. Devices used to show whether the integrity of a shipment has been compromised. A lock is not necessarily a seal, and a seal is not necessarily a lock. Each seal should be strictly accounted for from the manufacturer until the seal is destroyed, after its use for a shipment.

Serial numbers are embossed on each seal, and a log must be recorded serially by the seal custodian. Freight cars are seldom padlocked; numbered seals are used. The doors cannot be opened unless the seal is broken. A broken seal indicates breach in security, and an immediate investigation is warranted.

j. Prompt delivery of cargo. Delivery to designated consignee that is prompt lessens the risk of theft or pilferage at terminals. A 24-hour advance notice should be given consignee before arrival of sensitive shipments.

9. Railway Physical Security.

a. Physical security of railways. Railways provide both an economical and expeditious mode for maintaining a sustained flow of large quantities of supplies over long distances, providing protective security measures are implemented. Security measures are determined by the situation and area of operations.

b. Problem areas for railroad cars.

(1) Railyards, where cars stand loaded, are vulnerable to sabotage or pilferaging. These areas invite access to cargo by unauthorized personnel (See Figure 5-1).

(2) A single car breakdown stops the movement of a train. Cars left behind, on the side, encourage criminal acts.

(3) Derailment of cars can occur as a result of tampering with the tracks or control switches.

c. Physical security of railways. Security measures for railroad operation are determined by the situation and area of operation. Following are general protective measures:

(1) Inspection. Before loading, each railway car should be thoroughly inspected. If possible, avoid using cars with damage to their roofs, floors, or sides, for they do not provide effective security. If a damaged car must be used, minor repair should be made. The Transportation Railway Service (TRS) persons and commander of the train security force should be told of the problem cars. In organizing for a rail movement, MP personnel will likely serve as the railway security force. They function as a security team in support of TRS. The security force and train COs combine their support to get the train to its destination with its freight intact. The guard force commander will have the responsibility for security. The TRS is to get the train there on time.

(2) Loading and sealing. Freight should be loaded carefully to avoid loss or damage caused by train movement. Loading under the surveillance of security personnel provides a desirable deterrent to criminals. The standard method of sealing railroad car doors is by means of a soft metal strap. This is actually a numbered seal. It shows that the car has been loaded and

inspected, and it also reveals tampering. However, the seal offers little protection. Rigid accountability of seals should be maintained. This will prevent the undetected replacement of the original seal with another. Protection is provided by a heavy duty padlock, or it is provided by tightly twisting a length of heavy wire through the locking eyes and closely clipping the loose ends of the wire. Padlocks, however, advertise valuable cargo.

Figure 5-1. Railyard

(3) Grouping cars. It is standard railroad practice in making up trains to group cars according to their destinations. However, cars having sensitive or pilferable freight should be grouped together if possible. This will aid the most efficient use of security forces.

(4) Open cars. Open, flat, or gondola-type cars cannot be locked or sealed. When this type of car is used, the security force must take certain steps. They must place themselves so as to permit continuous observation and protection of the open cars.

(5) Security force. As mentioned before, train guards will usually be MPs, although other troops may be assigned to this duty. Their mission, is to ensure that the train arrives at its destination with its freight essentially undamaged.

(a) The strength of the security force is dictated by the sensitivity of the cargo, the priority of its need, and the circumstances in the area to be traversed. In the zone of the interior, only certain cars may be guarded; in a theater of operations, the entire train and trackage may require all available protection.

(b) Sometimes a few security persons are enough to secure cars having sensitive freight. If so, they may ride either in the specific car to be protected or in the caboose. There may be times when they ride in a security car(s). If only one security car is used, it should be near the center of the train; if more than one is used, spacing should be arranged to provide the best protection.

(6) Communications. There should be radio communication between two or more locations. Such communication should be used, when possible, between the train, the MPs and tactical units in the area.

d. Security measures for railroad operations.

(1) Trains should run on irregular schedules.

(2) Railroad security elements should both precede and follow individual trains, and critical terrain features along the route should be occupied if personnel and equipment are available.

(3) Locomotives should be preceded by two or more cars loaded with sandbags, rocks, or scrap material for protection against mines and obstructions.

(4) Use should be made of special armored security guard cars or gondolas. These may be prepared for defense by sandbags, machine guns, mortars, or rocket launchers. They must not be placed next to cars loaded with gasoline, ammunition or other flammables.

(5) Guard posts may be established at critical installations and rail facilities. Examples are tunnels, bridges, and stations.

10. Port, Harbor, and Vessels Physical Security. The entire responsibility for a US Army terminal is the CO's. It is his from the time military cargo arrives in a port until it leaves the terminal. The CO is responsible for the security of the cargo at the post, and for personnel assigned to, passing through or working within the terminal. A terminal is composed of areas such as storage areas, piers, beaches and shores, entrances/exits, and ships tied up at piers. The protection of waterborne traffic presents the CO with special problems. These relate to security planning, command and control and

coordination of combined and joint security forces (to include the host country). Other problems relate to intelligence information requirements, communications, and protection measures. Security needs depend mainly upon the nature of the threat to inland waterways, waterborne traffic and port installations. The security measures will vary. They will depend upon the seriousness of the threat and the vulnerability of shipping and terminal facilities.

a. Problem areas for port, harbor and vessels.

(1) Physical security of docks and vessels have threats unique to port security. Water adds another dimension to the security problem, for the water side of a port cannot be fenced off. Saboteurs or pilferers may use boats to get into the port area. Underwater swimmers are another threat. Floating objects may contain explosives or mines.

(2) Other threats, related to any physical security situation, are also present. Explosive devices may be placed in pilings, under docks, or on board vessels. Pilferage is likely on board ships and during unloading operations. It's also likely in storage or when material is removed from port for delivery. Natural threats, such as flooding, hurricanes, and fire can be damaging to a port facility.

b. Physical security of port, harbor, and vessels.

(1) Physical layout of the port area must be considered: size of the land area covered; length of the waterfront; surroundings; types of docking facilities (piers, quays, beaches, and off-shore anchorages); storage and warehouse facilities, and their construction; type of water area serving the port (river, bay, harbor, open water); and characteristics of the waterfront (tides, currents, and depth).

(2) Protection of the landward side of the port facility involves all of the principles of standard compound security.

(a) Perimeter barriers should be sufficient to deter illegal entry and to delay an intruder. They should serve to direct authorized persons to proper entry points.

(b) Lighting is important around the perimeter as well as within the port area.

(c) Intrusion detection devices, if available, may be installed to provide security in depth.

(d) The identification and control system has its first point of enforcement at the perimeter gates.

(3) Materiel and equipment brought into the port will affect the measures necessary to provide adequate security.

(a) High dollar items, such as electronic parts and automotive parts.

(b) Ammunition and weapons.

(c) Medical supplies.

(d) Clothing and personal equipment.

(e) PX supplies such as cameras and jewelry.

(f) Rations.

(4) Security of the port against waterborne attack does not mean protection against armed ships or torpedoes. This is a responsibility of the Navy and Coast Guard. Rather, it means protecting the port against enemy entry, acts of sabotage, and pilferage by people in the port area.

(a) Basic security of the waterside port can be provided by boat patrols. These make constant checks of docking facilities to locate sabotage devices. Watercraft entering the dock area are checked and turned back from the restricted zone. Boat patrols are also alert for underwater swimmers and floating objects.

(b) Physical barriers can be built to aid in securing a port facility. For example, cable supported by floats (empty 55-gallon drums, buoys, etc.) will stop floating objects; they will also stop or deflect small surface craft. Nets made of chain link fencing will help protect an area from torpedoes, and they will stop or delay swimmers. Sonar can detect underwater swimmers up to a distance of about 200 meters.

(c) Protective lighting of the port area provides a deterrent to saboteurs and pilferers. This is especially true underneath piers and other structures.

(5) Vessels at anchorage during offshore loading can be protected by the following:

(a) Physical barriers such as nets.

<u>1</u> Barriers must be watched to detect and counter swimmers who attempt to cross them.

<u>2</u> Barriers must be movable to allow ships to enter or leave the docking facility.

(b) Clear zones maintained around ships at docking positions.

1 No authorized watercraft or personnel should be allowed closer than 100 meters of the docking facility. Ammunition ships or barges cannot be approached within 300 meters.

2 Ship anchor chains must be checked frequently. This will prevent mines from being attached by infiltrators.

3 The clear zone should extend on both the waterside and land side of the ship. This zone should be enforced by ship guards on the deck and dock.

(c) Clearing of the docking area prior to the anchoring of any ship.

1 Frogmen may be used to detect mines or other planted charges.

2 Floating material should be checked and cleared by taking large objects in tow. Patrol boats should be operating skim nets between two crafts can accomplish this.

3 Dropping concussion grenades in the water is a way to detonate mines or explosives. These are mines and explosives which may have been overlooked. This method may also be used to discourage swimmers. However, assistance of EOD and Naval of Coast Guard personnel should be sought first.

(6) Hatch guards act as security during unloading operations. Port documentation personnel examine inbound manifests to identify sensitive or pilferable cargo. Hatch inspectors or guards examine the cargo before and during unloading to determine damage or pilferage. Discrepancies are documented by statements and pictures (hatch guards should have access to a Polaroid camera). Also, copies of tally sheets and Transportation Control and Movement Documents (TCMD) provide documentation.

(a) During loading or unloading, the hatch guards should always try to be on the same level as the workmen. The guards are to report on damaged cargo and evidence of pilferage or sabotage.

(b) The gangplank should serve as a security checkpoint for the control people.

(c) As materiel is unloaded, it should be transported under supervision directly to its storage.

(7) Control measures at the pier and warehouse must conform to physical security standards. Measures must include documentation, personnel identification and movement control, rapid movement, and security personnel.

(a) Proper documentation is the best method for control of materiels. The Transportation Control and Movement Document (TCMD) is the control document for all cargo shipments. TCMDs are issued in serial numbered blocks and are accountable by serial number. The TCMD, which describes the cargo and authorizes the shipment, is a release document. All cargo shipped from the port must have a TCMD. Also, cargo stored in warehouses or moved from place to place must have a TCMD.

(b) Restricted access is a primary means to control the discharge and storage areas. The fewer people who have access to the materiel, the fewer chances for theft there are.

1 Clear zones and off-limit areas around vessels should be enforced on the land side as well.

2 The identification and control system helps regulate personnel entering the port.

(c) Rapid removal of cargo to the warehouse or to the first consignee (receiver) will reduce pilferage.

(d) Removing damaged cargo to a central warehouse will reduce accessibility to potential pilferable cargo.

(e) Guards should be posted at warehouses containing pilferable or sensitive materiel. They are to provide security and to control movement.

(f) Materiels in open storage should be arranged in an orderly manner in a well lighted area.

(g) Towers, for observation of the dock area, will act as a deterrent to pilferage and will provide control.

(8) Communications must be provided as a part of the port security operation. Requirements exist for communication between shipboard security and MP patrol craft. Also, communication for a reaction force must be planned and coordinated.

(9) Security requirements in preparation for shipments leaving the port facility are as follows:

(a) Blot out markings on supplies which would be highly desirable to criminals.

(b) Secure loads moving by motor transport. Do so by banding or strapping and covering by tarpaulin when necessary.

(c) Seal, wire, and lock Army vans and CONEX containers used to transport cargo. Write the seal number on the TCMD.

11. Motor Movement Security.

a. Motor transportation is perhaps the most economical; therefore, it is the primary mode for moving supplies. Most supplies can be transported by this mode over trafficable terrain. In the combat zone, motor transportation is the main mode for distribution operations. It is also the main mode for logistical support operations. Weather, terrain, or enemy action, however, may present obstacles that interfere with over-the-road operations. The actual overall responsibility for the convoy is the convoy commanders. Military police assist in the area of security.

b. Problem areas.

(1) Shortages in shipments create a major problem in motor transportation. These shortages are caused by factors such as poor accounting, improper handling, and lack of any method for spot checks. The greatest chance for loss of cargo occurs at loading and unloading points. An employee can give property to a truck driver and help in hiding it aboard a truck for unauthorized removal.

(2) Most truck drivers and employees are honest, but a few of them may succumb to temptation. One example might be a receiving clerk who certifies the receipt of property that the truck driver actually disposed of before his arrival.

(3) Trash disposal and salvage disposal activities offer great opportunities to unauthorized persons to take valuable materiel. Property may be hidden in waste material to be recovered by a cohort who removes trash from the post (See Figure 5-2). Serviceable or even new items of equipment may be classified as salvage and stolen.

Figure 5-2. Example of trash/salvage disposal

c. Control measures for trucks.

(1) An ID system should be used to establish customer identification, i.e., truck driver and driver's helpers. The most common ID systems are: single card or badge; card or badge exchange; and multiple cards or badges.

(2) Register trucks by license number and description, especially rental vehicles.

(3) Establish an effective package and materiel control system.

(4) Establish security surveillance of all exits from the post.

(5) Maintain a truck register. Include in it the name of the truck owner, signatures of driver and helper, description of load, and date and time of entrance and departure.

(6) Use an effective package and materiel control system.

(7) Provide for examination of the truck or other conveyance, if feasible, for detection of unauthorized items.

(8) Loading. The methods of loading can aid security by placing sensitive items where they are not easily accessible. A typical area would be forward or in the middle of the truck bed. If van-type trucks are not available, one or more large items placed in the rear of the load will offer some concealment protection. Large trucks and trailers should be used to deter diversion by drivers en route. Loads are checked for completeness by using the TCMD for the cargo. Traffic into and out of loading and unloading areas should be carefully routed. It should facilitate ample opportunity for the security force to check all vehicles.

(9) Routing. Provide each driver specific route and strip maps. Make arrangements for alternate routes, refueling points, parking and billeting as needed. Any truck which leaves the prescribed route should be investigated by escorting MPs. Whenever possible, avoid routes with steep grades and obstructions. Avoid routes with one-way streets, or heavy traffic. Such avoidance will reduce vulnerability to theft caused by slow speeds or halts. Sometimes such routes cannot be avoided and pilferage attempts are expected. If so, extra measures may be taken by assigning MPs to the critical parts of the route. In the theater of operations, planning and preparation of convoy routing must include both physical and tactical security. This is especially true in regard to convoy halts. Select the locations for halts before the convoy departs; ensure the area is relatively secure and under surveillance of a security force. One of the benefits of an aerial reconnaissance before convoy departure is the identification of problem areas along the route.

12. <u>Pipeline Security</u>. Pipeline systems are used widely for delivery of bulk petroleum products in theaters of operations. These systems consist of

discharging facilities for tankers at ports of other points of entry. These systems also include inland tank farms and dispersing facilities; pump stations; and extended pipelines. These systems are vulnerable to a variety of security threats at all points. That vulnerability reaches from point of entry to point of final delivery.

a. Petroleum receiving procedures and safeguards.

(1) Check vessels to reveal quantities received and intransit ocean losses. These checks should be based on the ship's tank gauges. The petroleum is discharged into barges or tank trucks for further shipment.

(2) The receiver of the delivery should sign receipt only for the quantity of product received. He should maintain a dispatch-receipt log on all commercial truck deliveries. It is his duty to verify transit time from the main terminal to the receiving site-by checking the delivery receipt dispatch time. The receiver must check all hatch covers and discharge points to make sure they are secured by numbered seals. Finally, before discharge of the tank truck, he is to check the items listed below for discrepancies.

(a) Check the fuel level; ensure that it reaches the upper surfaces of the calibration ring in each compartment.

(b) Inspect the calibration ring; ensure it is fixed in place by a numbered lead seal or by welding. In addition, check for any indication of tampering or readjustment of this ring. This is a common means of deception.

(c) The depth of the calibration ring below the manhole should be measured. This will assure that it corresponds with the height listed on the truck's calibration table. Do so by measuring the distance from the upper surface to the brim of the manhole to the bottom of the calibration ring.

(d) Sample each component for purity.

(3) After fuel is off-loaded, inspect each compartment. Check that it is empty and there are no hidden compartments or other changes intended to divert fuel. A review of "Lessons Learned" disclosed that two 3,000 gallon commercial tanker trucks were confiscated in one operation. One truck had two special compartments containing approximately 1,000 gallons of diesel fuel (one-third of the truckload); the other truck had one special compartment containing 700 gallons.

(4) Receiving personnel must inspect each shipment of package products. This will ensure that each package or drum is sealed. It will also assure that there is no sign of leakage and the exact number of containers is received. Personnel should also spot check a few containers. They should ensure the containers are full of the items receipted for.

(5) Liquefied petroleum gas (LPG) cylinders are highly desired for the black market. Without the cylinders, local demand for the gas is reduced.

Control procedures include not only inspecting and accounting for full cylinders but also accounting for empty cylinders as well.

b. Protective measures. Pilferage is the most common hazard concerning pipeline systems. Sabotage is always a security threat, too. MPs may well have the security responsibility. They should coordinate closely with petroleum operating units. They should also coordinate with other units' security officers responsible for areas through which the pipelines pass. Lastly, MPs should coordinate with the command engineer responsible for construction.

(1) The location of a pipeline and its sensitivity determine the security measures required. From a security standpoint, the ideal location is parallel to a highway and close enough to the road for observation. When local conditions or terrain prevent this, other means or protection, such as air surveillance or foot and motor patrols, must be used.

(2) Initial security is provided by operational and maintenance personnel, but where their strength is not enough, guard patrols may be required. Particularly vulnerable sectors of the pipeline may be protected by guard detachments. Examples are isolated areas and pumping stations. MP working dogs may also be used to advantage in such locations. An industrial monitoring system can save manpower and ensure rapid repair. This system can detect tampering and localize the area of interference.

(3) Certain general guidelines are important in establishing pipeline security. For example, in a peaceful environment, the chief threat will probably be theft. As the level of hostility increases from low through mid-intensity to high-intensity, the threat of sabotage will become more greater. Of importance is the coordination of all tactical and non-tactical effort toward observing, reporting, and immediately acting to protect the system. The physical security officer must be instrumental in organizing and coordinating the elements of support.

13. Carriers Protective Services. Carriers can provide a variety of protective services to increase the security of intransit cargo. Negotiate with the carrier to implement services which will be based on the type, classification, size, etc. of the cargo. Included in the types of protective services are:

a. Signature security. A signature and tally are required from each person handling the shipment at each stage of its transit from point of origin to destination. Thus, individual responsibility for shipments is fixed.

b. Dual driver protective service. The vehicle is constantly attended by two persons.

c. Armed guard surveillance. Armed guards maintain constant surveillance of specific shipments.

LESSON 5

PRACTICE EXERCISE

REQUIREMENT. 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 examination score will tend to be lower than if you had not followed this recommendation.

1. Which of the following statements concerning port and vessel security is CORRECT?

   A. Security measures vary with the threat.
   B. Pilferage is not a problem on board ship.
   C. Port security requirements are the shared responsibility of vessel commanders.
   D. Water acts as an effective barrier against saboteurs.

2. Which of the following statements concerning train guards is CORRECT?

   A. The train guard's mission is to see that the freight on board remains intact.
   B. Train guards are required to be military police.
   C. Train guards are always spread throughout the train.
   D. The strength of the security is dictated solely by the commander of the train.

3. Security measures for protecting rail shipments include all of the following EXCEPT which?

   A. Irregular scheduling.
   B. Lead and rear security elements.
   C. Packaging control, gun-emplaced petroleum cars.
   D. Armored security cars.

LESSON 5

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

<u>Item</u> <u>Correct Answer and Feedback</u>

1. A. Security measures vary with the threat.
The security measures... (page 5-9, para 10).

2. A. The train guard's mission is to see that the freight...
Their mission is to ensure... (page 5-8, para 9c(5)).

3. C. Packaging control, gun-emplaced petroleum cars.
Security measures for... (page 5-8, para 9d).