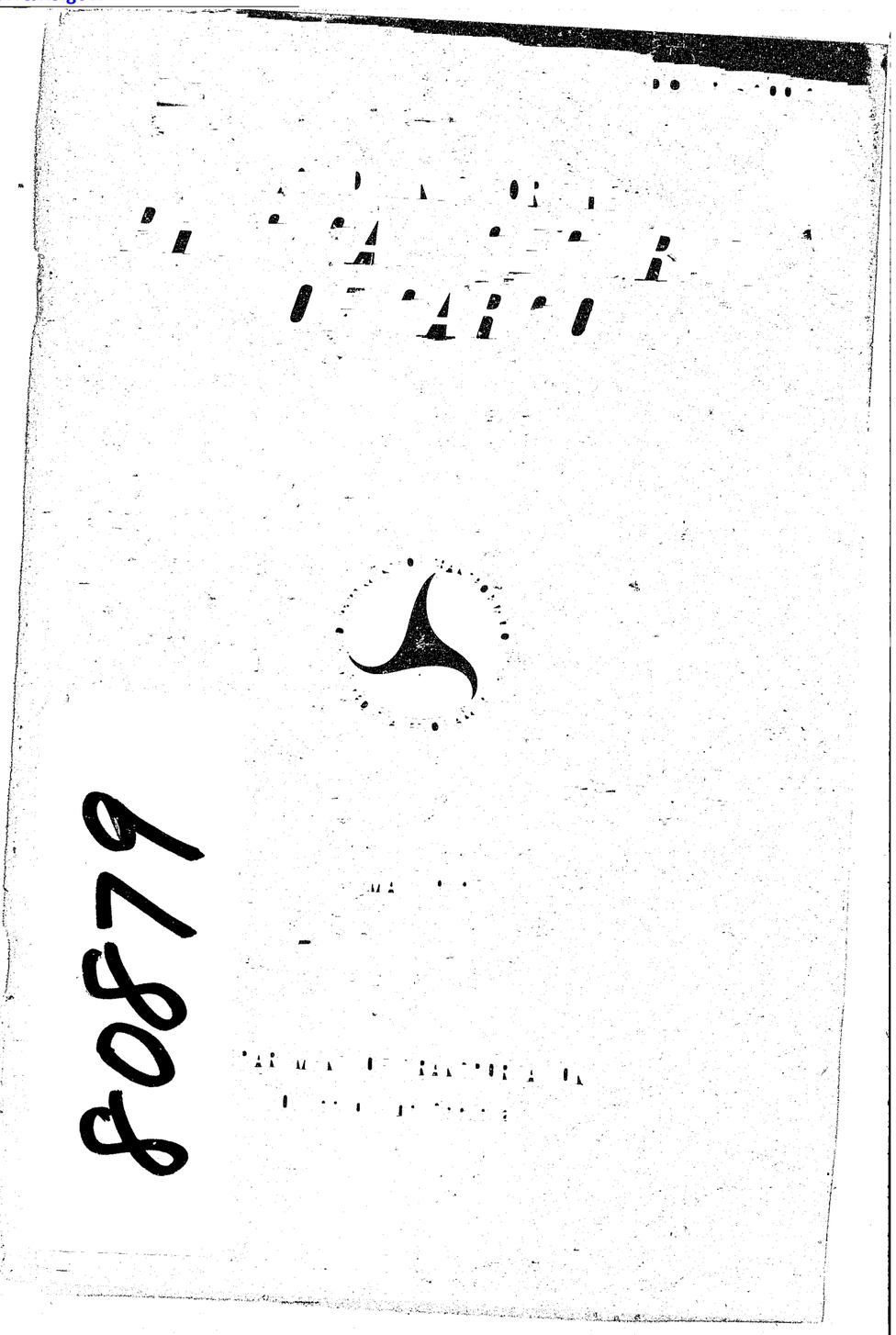

GUIDELINES

for the

PHYSICAL SECURITY OF CARGO

May 1972

DEPARTMENT OF TRANSPORTATION
Office of the Secretary
Washington, D.C.

PREFACE

Losses resulting from cargo theft and pilferage in the transportation industry have been conservatively estimated to exceed $1 billion annually. These losses constitute a major drain on the commerce of the United States. By establishing an effective cargo security system, transportation management can eliminate these losses, increase profits, provide more reliable and efficient transportation services to the Nation, and ultimately make goods available to the public at lower costs.

The guidelines contained in this handbook are intended to assist transportation management in that undertaking. They are suggestions and not regulatory in nature. Upon them, management can model a security system to meet a particular situation.

There are wide extremes in the nature of theft and pilferage across the Nation ranging from the theft of a 40-foot container or the hijack of a tractor-trailer to the pilferage of individual items of cargo from transportation facilities.

The Department of Transportation has made an analysis of cargo theft and pilferage on a national basis which encompasses all modes of transportation. The analysis was made in consultation with leading security experts and corporate executives in the industry. It reflects that about 85 percent of goods and materials stolen go out the "front gates" on persons and vehicles authorized to be in loading and unloading areas of transportation facilities. Only some 5 percent involves the after-hours break-and-enter burglar. Although catastrophic and highly publicized, the armed hijack or grand larceny of a tractor-trailer or a complete container amounts to only some 10 percent of the total loss picture.

Returning to the 85 percent—goods and materials going out the "front gates" of yards, docks, piers and terminals on authorized vehicles and persons—the DOT analysis shows that about 60 percent consists of thefts in quantities of one case or more but less than a full load. The remaining 25 percent is in the nature of pilferage of less than one case.

Burglary and hijacking obviously cannot be ignored. However, special attention by top management to the 85 percent loss area can dramatically reduce cargo theft and pilferage. Simply stated, that 85 percent is the theft of cargo from transportation facilities by people authorized to be at those facilities and on vehicles controlled or similarly authorized by transportation management.

Analysis of claims data from the transportation industry shows that nine commodities (clothing, electrical appliances, automotive parts, food products, hardware, jewelry, tobacco products, scientific instruments, alcoholic bever-

ages) make up about 80 percent of total national losses due to theft and pilferage. While these commodities make up the bulk of national and industry-wide losses, the kinds of things stolen and the cause and method of theft may vary from place to place and facility to facility. It is essential therefore that transportation industry managers and executives know the high loss items at their locations and within their areas of responsibility.

The main text of the handbook develops the rationale for cargo security measures and provides the basis for establshing and maintaining a cargo security program. Appendix I, "Cargo Security Standards," is a quick-reference summary of the recommended physical and procedural matters essential to cargo security. Appendix II, "Cargo Security Checklist," provides a series of questions to be answered in surveying a facility to insure comprehensive consideration of the many aspects of cargo security.

Nothing contained herein is to be construed as replacing or modifying any legal or regulatory requirement enacted or promulgated by proper governmental authority.

This handbook has been developed under the auspices of the Department of Transportation with support from the Departments of Treasury, Defense, Justice, the U.S. Postal Service, General Services Administration, other Government agencies, the transportation industry, transportation associations and concerned insurance groups.

Contents

Chapter I

THE BASIC APPROACH

From cargo theft and pilferage losses in today's multi-modal transportation system are coming higher operating costs, increased insurance rates and lower net profits. Time, at high rates per hour, is lost performing many unproductive activities. The adjustment of claims alone diverts managerial talent from normal tasks. Customers, unhappy over nondelivery, seek other means of moving their cargo. What was once a minor annoyance to the industry has become a persistent, chronic threat.

There are no universal one-time solutions to the problem of cargo security. Each mode of transportation, each terminal, each transfer point is unique. Each has particular strengths and weaknesses to be considered in the preparation of a security plan. There are, however, certain basic principles of cargo security which will be discussed in this handbook. They can be adapted by management to accommodate any mode of transportation or any facility, large or small.

Beginning

Certain general considerations will dictate how the transportation manager should proceed:

1. Management may either exercise its obligation directly or through a security officer. But if a security officer is employed, management cannot delegate and then forget it.
2. Each shipment, regardless of type or size, must be identified and accounted for continuously. Such accountability is difficult because cargo is in motion, exists in large quantities which defy piece-by-piece tallying, undergoes frequent changes of accountability, and is transferred rapidly by modern mechanical handling devices.
3. Absolute security is attainable. However, costs usually dictate the degree of protection which will be provided to discourage intruders and guard against loss or damage.
4. It is not necessary to provide the same degree of security for all facilities. The protection warranted for any particular facility is determined by two factors: criticality and vulnerability. Cargo is critical if it has high strategic value or if it has high value and can be easily handled and sold. A facility is vulnerable if it can be easily penetrated or if it is confused by the constant movement of large volumes of cargo. If a facility is both highly critical and highly vulnerable, an extensive physical security program is necessary.

5. The degree or type of physical security needed for a facility is affected by its size and complexity as well as by the volume and value of the cargo handled in it. Other factors to be taken into account are the economic and geographic situation of the facility, the availability of local law enforcement agencies and the crime statistics of the area.
6. When a number of firms use the same facility, such as a large metropolitan airport, all of the managements must coordinate their activities. Close cooperation with the facility management is also necessary.

Consideration of these factors will allow development of a plan that will provide neither more nor less security than is warranted by the situation. Development of the plan, however, does not end management's responsibility. The criticality or vulnerability of a facility may change from time to time. Therefore, the plan must be periodically reviewed and modified to accommodate changing circumstances. (See Appendix II, "Cargo Security Checklist.")

The costs of implementing a cargo security system will normally be more than justified when compared to the costs incurred in the past in cargo loss, theft, or damage. However, the development of an effective cargo security system should be based on future loss potential as well as past experience.

Building and maintaining an effective security program challenges the skill and leadership of those who administer it. They must instill interest in the success of the program in employees at all levels within the organization, impressing upon each employee the fact that he has a personal stake in the success of the security plan.

The Plan

The cargo security plan is the foundation upon which the success or failure of the entire program depends. It must be stated simply, yet in sufficient detail to cover all contingencies. Above all, it must be flexible and dynamic, adjusting to new problems as they arise.

The first step is to identify the hazards that threaten cargo within the transportation system or facility to be protected. It is the purpose of the plan to circumvent these hazards. They can be both natural and man-made threats.

Storm, flood, and fire are the most frequently experienced natural hazards. They cannot be totally prevented by physical security measures; however, their consequences can be minimized by implementation of a good disaster plan. Any one of them can reduce the effectiveness of existing security measures. Perimeter fences may be down, lights and alarm systems may be inoperative, vehicles may be out of service and cargo may be scattered over a wide area in danger of loss, theft, or pilferage. These eventualities demand preplanning for immediate reinforcement of the guard force and implementation of disaster procedures to protect the facility and cargo that has been made vulnerable.

Man-made hazards are more diverse. To protect the system against them requires a correspondingly greater amount of management's attention.

Every security plan must be based on the assumption that the transportation system is vulnerable to the risks of theft and pilferage.

Pilferage

Pilferage is difficult to detect, evidence of it is hard to obtain, and its consequence is costly to ignore. Thus, the prevention of pilferage becomes one of the primary concerns of the security program and the guard force.

A pilferer usually acts alone, frequently on impulse. He will remove a small amount of merchandise when the opportunity presents itself and when there is little risk of detection. Although unsystematic, his depredations may attain a high cumulative effect if permitted to continue unchecked.

Pilferage most commonly occurs in a terminal while cargo is awaiting transshipment from one vehicle or mode of transportation to another. Here cargo is apt to be left unprotected on handcarts, dollies or other intra-terminal vehicles. During this time, it is most susceptible to pilferage.

Small items capable of being concealed on the person or in an automobile are the customary pilferage targets. As a pilferer usually does not intend to sell the property he steals, the items he takes may be of either high or low value.

Specific measures for the prevention of pilferage can be based only on an analysis of existing conditions at a particular facility. Among the deterrents to be considered are:

1. Personnel movement controls.
2. Parcel check system, requiring that all parcels be declared upon entry to a facility and inspected upon departure.
3. Exclusion of privately owned vehicles from the area inside the parcel checkpoint or immediately adjacent to a terminal building or exposed cargo.
4. A continuing security education program, stressing the moral wrong of pilferage and encouraging employees to be alert and report thefts.
5. Cargo accountability controls, to provide rapid, accurate information of losses.
6. Sustained high employee morale and the development of mutual respect between security personnel and other employees.

Theft

At the present time, planned theft has become so widespread that it constitutes the most serious threat to the flow of commerce and the transportation system. It is management's first responsibility, working with law enforcement agencies, to identify occurrences of theft and report them.

It is not easy to determine the amount of loss experienced at any one point in the transportation system. Consequently, many losses are not discovered until a shipment is received by the consignee. He may be a long distance from the scene of the crime and the company accountable for the

288-637 O - 79 - 2

delivery may be different from the company responsible at the time of the theft.

Since a thief steals for profit, he does not usually act on impulse but plans his crimes and frequently works with accomplices. Often these will be employees of the companies to be victimized. Most frequently, their function is to provide information to the thief concerning the movement of high-value cargo. This is the thief's first task, for he will normally be selective according to his available market.

Obtaining possession of the cargo is his second problem. If physical safeguards are effective, he may attempt to bribe a member of the guard force, falsify shipping documents, or commit an act of vandalism to create a diversion while the actual theft is taking place. When employees are involved, obtaining possession of the cargo presents few problems, especially where management accountability procedures are weak or nonexistent.

The thief must remove the stolen cargo from the facility and this is most often accomplished by authorized vehicles present at the terminal for legitimate pickups or deliveries.

In some instances due to inadequate gate control, the thief will steal an entire truck or trailer.

Finally, he must profitably dispose of the goods he has stolen. Usually, he will sell the stolen cargo to a fence. For maximum personal profit, he seeks out items that currently fence for the highest prices and enjoy a ready market.

Certain elements of the transportation system are more vulnerable to theft than others. Terminal operations are extremely vulnerable. Facility personnel and truck drivers have direct contact with each other and a ready opportunity for collusion. A receiving clerk can certify receipt of property the driver has actually disposed of prior to his arrival. Conversely, a facility employee can provide a driver with cargo and assist in concealing it aboard the vehicle for unauthorized removal from the terminal. An employee can also execute a false invoice that will appear to be legitimate when inspected by security personnel.

Railway employees assigned to switching duty at a terminal can operate in a similar manner. By diverting a railway car to a siding outside the terminal, it can be made accessible to a thief's confederates. However, transferring the cargo from the car to another means of transportation demands more people. As the size of the gang increases, so does the possibility of discovery and apprehension.

Trash disposal and salvage activities provide excellent opportunities for theft. Items of value can be concealed in waste material to be recovered by a confederate employed to remove trash from the facility.

It is not necessary for a thief to be an employee or be in collusion with employees. Forged credentials will often allow him to represent himself as an employee of a real or nonexistent company. This is particularly true in overcrowded terminal facilities in large metropolitan areas.

Unlike a casual pilferer, a professional thief will not be deterred by psychological measues. Only active physical security measures will effectively eliminate losses from this source. Some of these measures are to:

1. Establish guard surveillance at entrances and exits to the facility or to certain controlled areas.
2. Establish an effective personnel and cargo movement control system.
3. Locate vehicle parking areas for employees and transients outside the perimeter fencing of the cargo handling area.
4. Employ a careful screening procedure during the hiring procedure.
5. Investigate all cargo losses quickly and efficiently.
6. Establish an effective key control system.
7. Provide adequate security patrols to inspect all perimeter fencing, buildings, yards and docks for suspicious or unauthorized movements.
8. Install mechanical, electrical and electronic intrusion detection devices.
9. Install appropriate fencing and lighting.
10. Store all cargo in enclosed, controlled security areas.
11. Maintain close liaison with law enforcement agencies.
12. Require strict adherence to existing procedures and maintain continual management supervision and presence to insure that procedures are followed, especially in the warehouse and loading areas.

In addition to the above, information concerning the movement of high-value cargo must be safeguarded. Without information a thief cannot act.

Physical Security

Planning the physical security measures necessary to circumvent the hazards discussed is the responsibility of management and its appointed security officer. These measures cannot interfere with the operating requirements of the facility. The receipt, sorting, processing and moving of cargo must proceed unimpeded by the security measures.

To determine the type and extent of physical protection required, the following factors should be considered:

1. The volume of cargo moved through the facility.
2. The value of cargo in the facility at normal peak periods.
3. The amount of time required for cargo to move through the facility.
4. The area to be protected, the kind of activity within it, and the number of personnel working there.
5. The vulnerability of the type of cargo to loss, damage or theft.
6. Maintenance and custodial services needed in the facility.
7. Environmental factors affecting the operation of the facility.
8. Current labor-management relations.
9. Cost to purchase, operate and maintain physical protection for critical areas and activities.
10. The possible expansion, relocation or retrenchment of the facility.
11. Alternative methods of providing protection.

The plan must provide that all security measures employed complement and supplement each other. In large facilities, where a number of companies operate, individual security plans must be integrated. Failure to do this can waste resources and jeopardize the security of all.

Outline Plan

A security plan will provide for proper and economical use of personnel, be flexible to allow changes to meet emergencies, and should contain the following:

1. Purpose of the plan.
2. Define the areas considered critical and establish priorities for their protection.
3. Establish restrictions on access into security areas, including personnel, cargo, vehicle, and key control.
4. Mechanical aids to security, including perimeter barriers, protective lighting, alarm systems and communications.
5. Guard force organization with general instructions for all guards. Detailed instructions for special areas, added restrictions and standard operating procedures should be appended.
6. General instructions for emergency actions. Detailed plans, such as for fire or flood, should be appended.
7. Instructions to assure coordination with shift management, other security forces, and law enforcement agencies.

When the security plan has been completed and implemented, it should not be considered inflexible. It should be a dynamic document, readily modified to reflect changing conditions or requirements. To assure that this is the case, management should conduct frequent critical physical security surveys to identify the deficiencies in the system. Security personnel are able to make specific recommendations for the elimination or minimization of any weaknesses found. Circulation of the overall security plan within the organization should be controlled and on a need-to-know basis. If the security plan is sound and the physical security survey shows that it is properly implemented and up to date, the loss and theft record of the facility will show improvement.

Chapter II

PERSONNEL IDENTIFICATION AND CONTROL

Many people employed in every mode of the transportation system are involved in handling cargo or its documentation. To ensure that the few unscrupulous persons are not permitted to hide in the large body of law-abiding workers, a positive identification and control system should be established. This will permit necessary compartmentalization of activities and preclude unauthorized entry to restricted areas. Simple, easily understood identification and control measures should be used. At the same time, care should be exercised to prevent these measures from interfering with the primary function of the facility—the expeditious and efficient movement of cargo.

Personnel control is achieved by determining who has a valid need to be in a specific area, then allowing only those to enter the areas. Access lists, personnel identification, identification cards and badges, badge exchange procedures, and personnel escorts contribute to the effectiveness of identification and control systems. Unauthorized personnel will not be able to penetrate a properly administered control system.

Employment Screening

A basic management responsibility is the screening and evaluation of job applicants and employees. In addition to their ability to perform the duties required, related factors such as honesty, integrity and reliability are important considerations. Management usually has adequate opportunity to make these judgments prior to final job commitments. Generally, security officers can advise management on the most efficient and effective methods to attain this goal.

Employment applications should be designed to provide the basic facts needed to accomplish security screening. The application should contain basic identifying data, including full name, date and place of birth, social security number, and current and prior (last 10 years) residences. Space should be allowed for tabulation of the applicant's employment history, accounting for his full adult life. This should include the identity of his employers, their addresses, supervisors, and the reason for termination. Space should also be provided for listing any court convictions other than minor traffic violations. Prospective employees should be fingerprinted. The completed employment application and the fingerprint card provide the bases for preemployment investigation and evaluation.

Identification Systems

A system should be established at each facility, both to identify all employees and to regulate visitors such as service or maintenance personnel. The size of the facility, type of cargo handled, and complexity of the operation will dictate the type of system to be used. These systems range from personal recognition to a photo identification badge system. The manager of a facility requiring an identification card system can prescribe a basic identification card for all personnel which will allow access to areas that are administrative in nature, contain no cargo and are not in the controlled area category. Individuals who need access to controlled areas can be issued separate, distinct cards or badges. Access to areas requiring a high degree of security (e.g. high-value cages and cribs at a large airport cargo terminal) within a facility can be indicated by color coding or otherwise marking the card or badge. Identification devices should be designed as simply as possible while providing for control of personnel movement. Increased security for cargo is provided by limiting the number of people who have access to it.

The provisions for identification by pass or badge should be a part of the security plan. Definite instructions should be prepared covering:

1. Designation of the areas in which passes or badges are required.
2. Description of the identification devices in use, with the authorizations and limitations placed upon the bearer.
3. Methods of identification upon entering or leaving an area.
4. Details of when, where, and how the identification device should be worn.
5. Procedures to be followed in case of loss or damage to an identification device.
6. Procedures for the disposition of identification devices upon suspension or termination of employment.
7. A procedure to issue new identification devices if more than one percent of those in use are unaccounted for.

Identification systems may use either passes carried on the person or badges worn on the outer clothing.

With a **single pass** or badge system, authorization to enter specific areas is indicated by letters, numerals, or colors. A weakness of the system is that passes or badges frequently remain in the bearer's possession during off-duty periods. This provides an opportunity for loss, alteration or duplication.

The **pass-exchange** system requires the use of two passes or badges. One is presented at the entrance and exchanged for the other which is identical except for certain coding allowing access to specific areas. In this system the second badge or pass never leaves the controlled area, thereby decreasing the possibility of forgery or alteration.

The **multiple-pass** system is a further development of the pass exchange system. Instead of markings on the facility badge indicating authorization to enter various areas, an exchange is made at the entrance to each area. Exchange badges are kept at each area only for those who are authorized

to enter. Because of the localized exchange requirements, this is the most secure system.

Identification devices should be designed and constructed in a manner that will make them virtually tamper-proof. To protect the system, strict accountability of all identification device components, including engravings or special paper, must be maintained at all times. To be effective, this control must extend to the manufacturer or supplier.

Identification device control should be maintained by the security officer so that a minimum time elapses between a change in the status of a pass or badge and notification of the guard force. Care must be exercised to assure that passes or badges are returned and destroyed upon termination of employment. Lost or mutilated identification devices must be invalidated immediately.

In addition to passes and badges, there are other methods of personnel control. Primary among these is maintenance of an access list of all persons authorized by management to enter a controlled area. When a permanent addition or deletion is made, the old list should be destroyed and a new one prepared. Current, verified lists should be issued to access control points. Admission to other than those individuals on the authorized access list is subject to specific approval by the facility manager.

A person whose name is not on the access list must be escorted from the entrance to a controlled area to his destination. The escort may be either a guard or a representative of the person visited.

The surest method of positive identification is a personal recognition system. It can be used with an access list if the work force is small enough to be known to the guards personally. Personal recognition can also be used in controlled areas where large groups are admitted at one time. This is done by having the group enter and leave the controlled area with a responsible supervisor who personally identified all members to the security guard.

Enforcement is the most vulnerable part of an identification system. Lax performance of his duty by a guard will invalidate the most carefully planned program. Therefore, guard personnel assigned duty at entrance control points must be alert, tactful, perceptive and able to demonstrate good judgment. Frequent, unscheduled inspections of guards at their posts will help to maintain the established program.

A uniform method of handling or wearing identification devices should be prescribed. A pass should be removed from the wallet or pocket and handed to the guard. A badge should be conspicuously displayed on the outer clothing.

Controlled entrances and exits should be so arranged that personnel are forced to pass in single file in front of the guard. At times, it may be advisable to use turnstiles to assist the guard in maintaining control. Artificial lighting should illuminate arriving and departing personnel and be of sufficient intensity to allow the guard to see the pass or badge clearly.

Visitors

The screening and control of visitors is a necessary precaution against pilferage, theft, and vandalism. This can be accomplished by establishing the need for a visitor's admission and any limitations placed upon him. Positive identification should be made of a visitor by personal recognition, a visitor's permit or other identifying credentials. Visitor passes or badges should be numbered serially and contain the following information:

1. Bearer's name.
2. Areas to which access is authorized.
3. Escort requirements.
4. Time period for which the visit is authorized.
5. Signature.
6. Photograph, if desired and available.

Racks at control points for passes issued to visitors should be located so they are accessible only to guard personnel.

The enforcement of an identification and control system is primarily the responsibility of the guard force. However, guards should have full cooperation from other employees who should be instructed to consider every unidentified or improperly identified person a trespasser.

Service and Maintenance Crews

Particular care has to be exercised in the admission of service and maintenance personnel. No group of occupations has been used as successfully or as often as a cover for unauthorized entry. Appropriate clothing, a tool kit and a smattering of technical knowledge are all that is needed to pose as a telephone repairman, an electrician, a plumber, a cleaner, or a business machine maintenance man. Legitimate employees of public utilities and some commercial service organizations carry company identification. They should not be admitted until a telephone check has been made to establish their identity and the request for service. Their movement within a controlled area is subject to the same escort procedures as are prescribed for other visitors.

The guard force should maintain a logbook in which is recorded the name, pass or badge number, and departure time of anyone who remains in a controlled area after normal working hours. Such a record will serve as a deterrent to a pilferer or thief. It will also provide the names of potential witnesses if they are needed.

Package Control

A package control system is an invaluable aid to preventing or minimizing pilferage, theft, and vandalism. No packages, except those with proper authorization, should be admitted into controlled areas without inspection. If practical, all outgoing packages should be inspected. If this is not possible, frequent unannounced spot inspections should be made. For the convenience of employees and visitors, a package checking service can be provided at the entrance to a controlled area.

Chapter III

CONTROLLED AREAS

Controlled Areas

A controlled area is any area whose access is governed by special restrictions and controls. In establishing controlled areas, consideration must be given to preserving the facility's cargo-moving capability as well as to its past loss and theft record.

All high-value cargo should be under surveillance or in a controlled area unless it is locked or sealed in the vehicle that transports it. Carrier vehicles, particularly trucks, trailers and railway cars, containing high-value cargo must be guarded or protected by a controlled area until they are released to authorized personnel for movement.

To be fully effective, a controlled area should be under surveillance by physical or electronic methods and movement within the area controlled. A barricade providing limited access does not, in itself, constitute a controlled area.

The transportation industry provides a public service. As a result, some of its operations must be open to the general public. The general offices, personnel office, and freight receiving offices may need to be outside the controlled area. Where practical, consideration should be given to the installation of convex mirrors in warehouse storage areas so that supervisory and guard personnel can have additional surveillance capability.

A controlled area can extend over many acres and include vehicle marshalling yards, docks, warehouses and service or supply buildings. Such an area is a first line of defense for the protection of cargo in the transportation system.

Limited Area

Within the controlled area, a limited area can be established. This will provide a higher degree of security. A different pass, issued to fewer people, should be necessary for entry to a limited area. Sorting, recoopering of crates, and storage may be accomplished here.

Exclusion Area

An exclusion area can be located inside the limited area. Again, a different pass should be required and the number of people granted access strictly limited. The exclusion area is used only for handling high-value, low-volume cargo. The crib, vault, or cage that comprises the exclusion area should be kept locked or under surveillance at all times.

288-637 O - 79 - 3

Access points to any controlled area, regardless of the degree of security involved, should be locked at all times they are not under physical or electronic surveillance. Strict control of the keys or combinations to locks is essential. Management should make periodic checks to determine the integrity of controlled areas in addition to any checks conducted by security representatives.

Vehicle Control

Only bona fide cargo-carrying or handling vehicles should be allowed inside a controlled area. Employee and visitor parking lots should be located outside the controlled area. This is an especially important principle. If the controlled area is not fenced, then private vehicles should be required to park behind a clearly defined line well removed from cargo or storage buildings.

Generally, there are three types of vehicles that operate within a controlled area: (1) the facility work vehicles, primarily small trucks, cargo-handling vehicles and cargo-loading vehicles; (2) the freight pickup and delivery and freight-forwarder vehicles; and (3) the cargo carrier vehicles.

Facility vehicles usually remain in a controlled area but, if it is necessary for them to leave, their departure should be recorded. The freight pickup and delivery vehicles and the freight forwarder vehicles should be checked in and checked out, with records maintained to assure that they are the authorized vehicles for particular cargo. Cargo carrier vehicles should be inspected and manifested upon arrival at or departure from the facility.

All vehicles entering or departing a controlled area should pass through a service gate controlled by physical or electronic means. The size of the facility will determine the complexity of the gate procedures used. Where guards are considered necessary, the inbound procedures should include, but not be limited to:

1. Truck register on which should be noted driver's name (obtain from driver's license), truck or tractor license (obtain from registration), trailer or container number, company name, number of waybill, delivery notice, prelodge, or other document being used to authorize pickups and deliveries, time of entry.

   NOTE.—A Regiscope or similar camera could be used to record all the above data and that record could be a substitute for, or used in conjunction with, a truck register.

2. A seal check on inbound loaded trailers.
3. A pass or time-check card identifying the vehicle and driver which will be time-stamped on entering and leaving the facility. The pass should also indicate the building or door designated for the pickup or delivery.

The procedures for outbound vehioles should include, but not be limited to, the following:

1. Pick up gate pass or time check card and verify for discrepancies.
2. Check seal against documents and record number.
3. Open doors and check vehicles if not sealed. Interline vehicles should not be locked until checked by gate control. (Partial loads, especially those containing numerous marks, are effectively checked only by returning vehicles to dock and restripping cargo under security supervision. This should be done on a periodic, random basis as a deterrent to use of these vehicles for removing stolen cargo.)
4. Inspect cabs of vehicles for possible stolen items.

Loading and unloading operations should be carefully supervised and under periodic unobserved surveillance to prevent unauthorized material from leaving the facility in the vehicles. It is widely accepted that the majority of the cargo loss occurs at the dock during the operating hours. Continuing and efficient supervision and security at this point is essential if losses are to be reduced.

Chapter IV
BARRIERS

The most basic protection for cargo is a barrier which prevents the would-be thief from approaching his cargo target. Physical and mechanical barriers are the subject of this chapter along with a discussion of recommended procedures to be followed outside the terminal facility.

Types

Barriers can be used to create physical and psychological deterrents to accidental entry; to prevent deliberate unauthorized entry; to delay intrusion, making detection and apprehension by guards more likely; to make guards more effective; and to direct the flow of pedestrian and vehicular traffic.

There are two kinds of physical barriers—natural or structural. Natural barriers include rivers, marshes, or terrain difficult to negotiate by vehicle. Structural barriers include fences, walls, buildings, grills, bars, and gates. A barrier should be under physical or electronic surveillance to be fully effective.

The kind of barrier to be used depends upon the size of the controlled area, the flow of traffic during the busiest and least busy periods, and the most prevalent local hazards.

The perimeter of a large controlled area may be a combination of natural and structural barriers. A limited area, however, must generally be bounded by a structural barrier.

Fencing

Fences should be chain link; No. 9 gauge or heavier wire; no less than 8 feet high, with mesh openings no larger than 2 inches per side and with a twisted, barbed selvage at the top. It should be stretched taut and securely fastened to metal posts set in concrete. The bottom should be within 2 inches of hard ground or paving. On soft ground, it should extend below the surface to compensate for shifting soil or sand. Culverts, troughs or other openings larger than 96 square inches in area should be protected by fencing or iron grills to prevent unauthorized entry yet allow proper drainage.

A top guard should be attached to perimeter fences and interior enclosures for greater security. A top guard is an overhang of barbed wire along the top of a barrier facing outward and upward at an angle of 45 degrees. The supporting arms, at least 2 feet long, are attached to the top

of the fence posts. Four strands of standard barbed wire are tightly stretched between the supporting arms. Some fences have a double overhang, facing both outward and inward, which makes it more difficult to enter or leave the facility by scaling the fence.

The top guard can be firmly fixed or mounted on springs. The spring type guard further increases the difficulty of scaling the fence. If a building less than three stories high forms part of the perimeter, a top guard should be used along the coping to deny access to the roof.

The fence line should be as straight as possible to provide ease of observation by the guard force. If practicable, fences should be located no closer than 50 feet to buildings or cargo in a controlled area. Twenty feet of clearance should be allowed between the perimeter barrier and exteiror features, such as buildings or parking areas, which would offer concealment to a thief.

Fencing for **limited areas** should conform to the same specifications as for controlled areas, although it is recommended that the height be increased to 10 feet and that a top guard be used.

Exclusion areas should be located in secure buildings and consist of separate cribs, cages or vaults. If fencing is used, it should be at least 10 feet high, extend to the ceiling or be topped by a wire mesh roof, and be under observation by a guard.

If a wall serves as the barrier, or a part of it, it should be constructed to provide protection equal to that specified for each of the areas above. If it is less than the height specified, it should be topped with chain link fence and barbed wire to match the minimum requirements. If a fence connects with a building, it should extend within 2 inches of the wall of the building.

A body of water, whether it be a river, lake or ocean, does not, in itself, constitute an adequate barrier. Additional measures, such as a fence, frequent security patrol and floodlighting, usually are necessary.

To be effective, barriers have to be well maintained. Breaks or damage to the structure should be repaired as soon as they are discovered. Frequent inspections of the barriers must be made by the guard force to locate defects. In addition, the security officer should periodically tour the barriers, giving particular attention to cuts or openings in the barrier which may be camouflaged.

If the perimeter barrier encloses a large area, an interior all-weather road should be provided for guard force vehicles. The road should be in the clear zone and as close to the barrier as possible. Its use should be limited to guard and emergency vehicles.

Entrances

The number of gates and entrances to controlled areas should be limited to the minimum required for safe and efficient operation of the facility. A top guard, equal to that on the adjoining fence, should be attached to each gate. The bottom of the gate should be within 2 inches of hard ground or paving. Adequate lighting should be provided for fast efficient inspection.

When gates or doors are not manned by guards so that all those entering will be challenged, they should be securely locked, illuminated during hours of darkness, and periodically inspected by a roving guard.

Semiactive entrances, such as railroad siding gates, or gates and doors used only during peak traffic flow periods, should be locked except when actually in use. Keys to these entrances should be in the custody of the security officer or the chief of the guard force and should be strictly controlled. Periodic inspection should be made of these entrances.

Inactive entrances, which are used only occasionally, should also be kept locked. They are subject to the same key control and inspection as semiactive entrances.

Emergency exits should have alarmed break-out hardware installed on the inside.

Sidewalk elevators and other unusual entrances that provide access within controlled area barriers should be locked and patrolled.

Control signs stating the conditions of entry to a facility or controlled area should be erected at all entrances. They should inform the entrant that he is subject to search of his person, vehicle or packages and of any prohibitions against packages, matches, smoking or entry for other than business. The signs should be legible under normal conditions at least 50 feet from the point of entry.

To maintain the integrity of the barriers to controlled areas, guard control stations should be established at all entrances in service.

Locks

Locks are an essential and integral part of barriers and the security they provide. To be effective, however, keys and combinations to locks must be strictly controlled. If they are compromised, the security of the entire facility is compromised.

Regardless of their quality or cost, locks can only be considered as delay devices. They are not positive bars to entry. Many ingenious locks have been developed, but equally ingenious means have been devised to open them surreptitiously. Some locks require considerable time and expert manipulation to open, but will eventually succumb to force and the proper tools. The protection afforded by a well-constructed lock can be measured in terms of the time the locking mechanism will resist picking, manipulation, or drilling.

To determine a facility's lock requirements demands specialized knowledge. Few security officers, and fewer transportation managers, have the necessary expertise. It is advisable, when selecting the equipment to be used to consult a professional locksmith.

Locks commonly used in the transportation system include:

1. Key locks, some of which can be opened by an expert in a few minutes. The ease with which a key may be lost and compromised or with which an impression may be made should be considered in determining the security value of a key lock.

2. Conventional combination locks, which may be opened by a skillful manipulator able to determine the settings of the tumblers of a common three-position dial-type through his sense of touch or hearing. Although some combination locks may require several hours to open, a skillful man can open the conventional combination lock in a few minutes.
3. Manipulation-resistant combination locks, which are designed so the opening lever does not come in contact with the tumblers until the combination has been set. This lock provides a higher degree of protection for important material.
4. Other combination locks with four or more tumblers that afford still greater protection for very important items.
5. Relocking devices, which furnish an added degree of safety against forcible entry to a safe or vault door. This device increases the difficulty of opening a combination lock by punching, drilling, or blocking. It is recommended for heavy safes and vaults.
6. Interchangeable core locks, which have a core that can be removed and replaced by another using a different key. The cores can be replaced quickly, instantly changing the matching of locks and keys if their security is compromised. Other advantages are that all the locks in a facility can be keyed into an overall master-keyed system.

   Interchangeable core locks are economical, involving lower maintenance and new lock expenses. The system simplifies recordkeeping, is flexible and can be engineered to the needs of the facility.
7. Kingpin locks, which are placed on the kingpin of a trailer or container chassis to make it impossible to connect a tractor. They provide a medium to high degree of security, depending on the type of lock. Although expensive, one lock can protect a number of trailers simultaneously if the locked trailer is parked in a blocking position. As the lock can provide positive security, it is recommended for use in an area where only periodic surveillance, rather than constant observation is possible.

For effective control of locks, keys, and combinations, accurate records must be maintained and periodic physical inventories made. Combinations and keys should be issued only to those whose official duties require them.

Combinations to safe locks and padlocks securing containers should be changed at least once during each 12-month period; immediately following the loss or possible compromise of a combination or key; after the discharge, suspension or reassignment of anyone who knows the combination; or upon receipt of a new container with a built-in combination lock.

The facility key and combination control should be exercised by the security officer. Records containing combinations and keys should be securely stored, with only limited and controlled access allowed. Lists of persons authorized to draw keys to controlled areas should be kept in the key storage container. Key containers should be inventoried at the end of each shift and all keys accounted for. Above all, keys should not be

issued for permanent retention or removal from the facility. Keys should be logged out at the beginning of each shift and logged in at the end.

Each facility will have requirements for key and lock control systems peculiar to itself. A survey should be conducted to determine the actual need for additional protection afforded by locking devices. When this determination has been made, an annex to the security plan can be drafted, showing:

1. The location of key depositories.
2. The keys (by building, area, or cabinet number) to be held in each depository.
3. The method of marking or tagging keys for easy identification.
4. The method of control for issue and receipt of keys, including register maintenance and identification of personnel authorized to receive keys.
5. The action required if keys are lost, stolen, or damaged.
6. The frequency and method of lock rotation.
7. The assignment of responsibility and accountability by job or position title.
8. The availability of emergency keys to the guard supervisor.
9. A list of persons to whom this plan is made available.

288-637 O - 79 - 4

Chapter V
LIGHTING

At night, a protective lighting system enables the guard force to maintain a level of security approaching that observed during the day. Adequate lighting is relatively inexpensive. If it cannot be provided, management has to consider other more costly alternatives, such as additional guards, sentry dog patrols, or expanded alarm systems.

The amount and intensity of light needed will vary from point to point within the facility. Designing a system for a large facility is a specialized task. Material is available from the manufacturers of lighting equipment that will assist management, but consultation with an expert in the field will save time and expense. It will undoubtedly produce a more satisfactory lighting system.

Protective lighting will permit guards to observe activities around or inside a facility. It is achieved by providing even light on areas bordering the facility, directing glaring light into the eyes of a potential intruder, and maintaining a low level of light on guard patrol routes.

Planning

When planning a protection lighting system, the creation of high contrast between an intruder and the background is a primary consideration. The ability of a guard to distinguish a darkly clothed man against a dark background improves significantly as the level of illumination is increased. Predominantly dark, dirty surfaces require more light to facilitate observation than those of clean concrete or light-colored paint. This is also true inside buildings where ceilings and walls redirect and diffuse light.

Generally, lighting should be directed downward and away from the structure or area to be protected, and away from the guards assigned to patrol the facility. It should create as few shadows as possible.

Units for lighting perimeter fences of controlled areas should be located within the protected area and above the fence. The light pattern on the ground should include an area both inside and outside the fence. Adjacent highways, waterways, railroads, or residences may limit the depth of the light pattern.

Similarly, piers and docks forming part of the facility perimeter should be safeguarded by illuminating both the pier area and the water approaches. The area beneath the pier flooring should be lit with low-wattage floodlights arranged to dispel shadows.

Movable lighting that can be controlled by the guards is recommended as part of the protective system for piers and docks. Lighting in these areas cannot be allowed to violate marine rules. The U.S. Coast Guard should be consulted to assure that proposed lighting systems adjacent to navigable waters do not interfere with aids to navigation.

The lighting of open areas within a perimeter should be the same as the illumination required at the perimeter. Lighting units in outdoor storage areas should be so placed as to provide an even distribution of light in aisles and recesses to eliminate shadows where an intruder may conceal himself.

Special Terms

Special terms used in describing lighting must be understood to discuss and develop a protection lighting system:

One **candlepower** is the amount of light emitted by one international candle.

One **foot-candle** is the amount of light on a surface 1 foot from the source of 1 candle power. The amount of light varies inversely as the square of the distance between the source and the surface; so the foot-candles decrease rapidly as the distance is increased.

Horizontal illumination is the amount of light expressed in foot-candles on a horizontal surface.

Vertical illumination is the amount of light expressed in foot-candles on a vertical surface.

Continuous lighting *(stationary luminary)* is the most common protective lighting system. It consists of a series of fixed luminaries arranged to flood a given area continuously with overlapping cores of light.

Glare projection lighting provides a band of light with great angular dispersal. It directs the glare at an intruder while restricting the downward beam. It is a strong deterrent to a potential intruder and protects the guard by keeping him in comparative darkness. It should not be used if it would interfere with adjacent facilities.

Controlled lighting allows adjustment of the lighted strip to fit a particular need. If a highway, airport, or railroad adjoins the perimeter, this method will permit illumination of a narrow strip outside the fence and a wide strip inside the fence. The weakness of this method of lighting is that it often illuminates or silhouettes guards as they patrol their routes.

Standby lighting *(stationary luminary)* is similar to continuous lighting as described above. The luminaries, however, are not continuously lit but are activated manually by the guard force or automatically by the alarm system only when required.

Movable lighting *(stationary or portable)* consists of manually operated movable searchlights that can be lighted during hours of darkness or only as needed. The system is a supplement to those described above.

Emergency lighting can duplicate any or all of the above systems. Its use is limited to emergencies which render the normal system inoperative. It needs an alternate power source such as installed or portable generators.

Incandescent lamps are common glass light bulbs which produce light by the resistance of a filament to an electric current. Special purpose bulbs are manufactured with interior coatings to reflect the light or with a built-in lens to direct or diffuse the light. A regular bulb can be mounted in a shade or fixture to secure similar results.

Gaseous discharge lamps are of two kinds—mercury vapor and sodium vapor. They are limited in their use for protective lighting as they require a 2- to 5-minute period to light when cold and a slightly longer period to relight, when hot, after a power interruption.

Mercury vapor lamps emit a blue-green light caused by an electric current passing through a tube of conducting, luminous gas. They are more efficient than incandescent lamps of comparable wattage. They are used widely for interior or exterior lighting where people are working.

Sodium vapor lamps are made on the same general principle as mercury vapor lamps but emit a golden yellow glow. They are more efficient than mercury vapor or incandescent lamps and are used where the color is acceptable, such as on streets, roads, or bridges.

Power Sources

Normally, the primary power source for a transportation facility is the local public utility. The concern of the security force begins at the point at which power feeder lines enter the facility. Feeder lines should be located underground or, in the case of overhead wiring, inside the perimeter to minimize the possibility of vandalism to the lines.

An alternate source of power should be available to supply the system in the event of interruptions or failure. Standby gasoline-driven generators that start automatically upon the failure of the primary source will insure continuous light. They may, however, be inadequate for sustained operation. Generator or battery-powered portable or stationary lights should be available at key control points for use by the guards in case of a complete power failure that makes the secondary power supply inoperative.

Circuit Design

Both parallel and series circuits can be used to advantage in protective lighting systems. However, circuits should be arranged so the failure of one lamp will not leave a large portion of the perimeter or a segment of a critical area in darkness.

The design should be simple and economical to maintain. It should require a minimum number of shutdowns for routine repair, cleaning and lamp replacement. It should facilitate periodic inspections to replace or repair worn parts, tighten connections, check insulation, and clean, focus and aim lights.

Chapter VI

ALARMS AND COMMUNICATIONS

Intrusion detection devices can be used as a supplement to, but not a substitute for, the facility security force. They are intended to alert guards to an intrusion or attempted intrusion into the facility. Their effectiveness is dependent upon the reaction time of the guard force once an alarm has been activated.

Management responsible for physical security must understand the strengths and weaknesses of the equipment available if it is to be effectively incorporated into the security plan. If an effective alarm system is installed, management may conserve manpower by using smaller, mobile, responding guard units instead of larger numbers of patrols and fixed guard posts. However, in drafting a plan, alarm systems must be treated for what they are—aids to, not substitutes for, an alert, well-trained guard force.

Systems

There are a variety of commercially manufactured devices available that are designed to detect intruders. Certain systems are suitable only for external protection while others can be used only inside a structure. Although an alarm system can be neutralized or circumvented by a resourceful individual, consultation with a reputable expert in the field will help to design the most tamper-proof system for a particular situation.

An alarm system consists of:

1. Detection elements located at the protected area designed to initiate an alarm upon entry of an intruder into the area.
2. Transmission lines which conduct signals to a signalling device in the immediate area or to a central annunciator panel that can be continuously monitored.
3. A panel which announces by visible and/or audible signals the structure or area in which an alarm is activated.
4. Fail-safe features to provide a signal at the annunciator panel if any part of the system is malfunctioning.

Many types of alarm systems are in common use. Frequently, two or more different systems will be installed in the same facility.

A **local** alarm system is one in which the protective devices activate a visual or audible signal in the immediate area to be protected. The light or sound device should be mounted on the exterior of the building, protected against weather or vandalism. It should be visible or audible for a distance

of at least 400 feet. Although response to the alarm is made by facility guards or other employees, it can also be answered by the local police and fire departments.

A **police connection** system is one in which the facility-owned system is a direct extension of the police and fire alarm systems. This type has the disadvantage that the consequent dual responsibility for maintenance is difficult to administer.

The **central** station system is leased by the facility from a commercial agency. The agency designs, installs, maintains, and operates the system to safeguard against fire, theft, or intrusion. Alarms are transmitted to a central station outside the facility. The agency then takes appropriate action, such as notifying the police or fire department. Most agencies also have their own private guard force which is dispatched to the scene upon receipt of an alarm. Audible signals can be provided to alert employees or guards at the facility.

A **proprietary** system is similar to a central station system except that it is owned or leased by, and located entirely within, the facility. Its main controls should be in or near the security headquarters. Response to an alarm is by the facility's own security personnel. This system can also be connected to a central control station for immediate notification of appropriate authorities.

Detection Devices

A variety of devices are available to activate alarms. Although they employ different principles, each one will transmit an immediate warning signal to the security force.

Points of entry to buildings or enclosures can be protected by an alarm which is activated by breaking an electrical circuit. For this purpose, electrically charged strips of foil or wire can be used on window panes. Doors and windows can be equipped with magnetic or spring-activated contacts which sound an alarm if they are opened. Such devices consistently provide the most trouble-free service and cause few nuisance alarms. They may be costly to install at a large number of entry points. Sometimes they can be defeated by bridging, or jumping, the circuit.

The photoelectric device uses a light sensitive cell and a beam projected by a light source. If an intruder crosses the beam, he breaks contact with the photoelectric cell which activates the alarm. The light source may be hidden and/or an infrared filter over it may make the beam invisible to intruders. The beam can be crisscrossed in a protected area by means of mirrors until it strikes the light sensitive cell. A projected beam of visible light can be effective for approximately 500 feet.

The photoelectric device affords effective, reliable notice of intrusion when properly installed. There are certain disadvantages. Some kind of permanent installation is necessary. Mirrors must be locked into very precise adjustment. Sufficiently dense smoke, fog, rain, or dust will cause activation of the alarm. Frequent inspection is needed to assure that the system components have not deteriorated.

A protective device that detects sound and vibration can be used to safeguard vaults, special security storage bins, or warehouses. Extremely sensitive microphones are installed in the area on the walls, ceilings and floors. Sounds or sound vibrations caused by an attempt to force entry will activate the alarm. The device is economical and easily installed. When an alarm is received, the amplifier can be adjusted to monitor further sounds from the protected area. It can only be used in vault-like installations or other enclosed areas where a minimum of extraneous sound is encountered. It cannot be used effectively out-of-doors, or in proximity to heavy construction or rail or vehicular traffic.

Another device that can detect motion indoors uses ultrasonic waves travelling at approximately 1,130 feet per second with a frequency of about 19,200 cycles per second. The high pitch of the sound is inaudible to the average person. The transmitter is a small metal case mounted on the wall or ceiling. The receiver, mounted similarly, listens continuously to the sound pattern broadcast by the transmitter. The device hears what is issuing from the transmitter as well as the echoes that bounce from the walls, furniture, and other objects in the enclosure. When motion disturbs the sound pattern, the change in ultrasonic frequency activates the alarm.

As much as 4,000 square feet of floor area can be protected by a single transmitter and receiver unit. The device can be installed relatively easily by unskilled personnel. However, the unit's sensitivity controls must be carefully adjusted and frequently serviced. Nuisance alarms may lead security personnel to reduce the system's sensitivity, thus destroying its usefulness. It is not adaptable for use in areas where quantities of absorbent materials are stored as they do not reflect sound waves.

As electromagnetic or capacitance alarm can be used for point protection of specific objects requiring a high degree of security, i.e., safes, file cabinets, or other metallic storage containers. The system may be connected to windows or door grids of metallic tubing to provide protection for such openings.

It forms an electromagnetic field around the object to be protected. The field is tuned by achieving a balance between the electric capacitance and the inductance. An intruder entering the field unbalances the electromagnetic energy of the field, which activates the alarm. The field cannot be penetrated without triggering the alarm. An electromagnetic device is easily installed at moderate cost.

A contact microphone has been developed for the protection of masonry structure fitted with heavy steel doors. It is capable of detecting the attempted penetration of any part of the enclosure as a result of explosive, hammering, cutting, drilling, or burning attacks. The contact microphone detects vibrations caused in the walls of the structure by attempted penetration. It amplifies the vibrations and sounds an alarm in security headquarters. Because the contact microphone senses wall vibrations rather than sound, the system is not affected by ambient noise.

Although closed-circuit television is not an alarm device, it is frequently used to complement an alarm system. This may be accomplished by placing

288-637 O - 79 - 5

fixed television cameras at critical locations to provide direct visual monitoring from a central vantage point. Or a single camera remotely controlled by the monitoring guard can sweep across a wide area. Television is particularly useful to provide direct monitoring of very sensitive or exclusion areas and to observe gates equipped with electrically operated locks. Closed circuit television can also be used with Image Sensors or Video Motion Detectors, to signal unauthorized entrance to a facility. An alarm can be sounded and a video tape recorder activated.

Care should also be taken where choosing CCTV equipment that the type of lighting used, (i.e., gaseous discharge, or incandescent) is compatible with the cameras selected.

Protection

Protection for an alarm system can be provided by built-in technological features or by simple physical security measures. If the system is made more sophisticated to protect itself, greater ingenuity is needed to breach or violate it. However, as it becomes more advanced technologically, the cost of the system and the cost of maintenance increase accordingly.

Physical security measures usually cost less, and afford less protection. Such measures may involve locating transmission lines high above ground or burying them deep below ground, recessing detection devices in armored boxes or walls, and rigid control of access to communication centers. Through a combination of technological and physical security measures, a balance should be achieved in which the maximum time is required to defeat the system and the lowest cost is experienced in its construction and operation.

Maintenance

Intrusion detection devices should remain in continuous operation during nonoperational hours if they are to be effective security aids. Therefore, preventive and corrective maintenance must be performed promptly.

Manufacturers will train and advise designated security personnel on the maintenance of the equipment. To prevent malfunctions, trained personnel should inspect and test components as recommended by the manufacturer, and should be capable of effective immediate minor repairs. To do this, spare parts recommended by the manufacturer must be kept in stock. A contract, providing service on a 24-hour basis, should be negotiated with the manufacturer for all other service and parts. Plans, diagrams and data charts for all alarm systems installed should be kept in a locked file in the custody of the security officer.

Standards

The transportation facility manager or security officer developing an alarm system can receive guidance from the standards established by Underwriters Laboratories, Inc. Detailed system requirements are given in the following publications:

UL 609—Local Burglar Alarm Units and Systems.
UL 611—Central Station Burglar Alarm Units Systems.

UL 634—Connectors and Switches for Use with Burglar Alarm Systems.
UL 639—Intrusion Detection Units.
UL 681—Installation, Classification, and Certification of Burglar Alarm Systems.

Communications

Allied to, but independent of, the alarm system is the protective communication system, which will vary in size and complexity with the importance, vulnerability, size and location of a specific facility. Its design is subject to local determination. Normally, the regular communication system is not adequate for protective security purposes. Security forces should have a separate system with direct lines outside and an auxiliary power supply.

Although dependence is placed on the telephone, teletype and automatic alarm systems, internal and external radio communications may play an important part in the security program plan of large facilities. One or more of the following means of communication should be included in the protective system:

1. Local exchange and commercial telephone service.
2. Intrafacility, interfacility and interoffice telephone systems using rented circuits and equipment that is not interconnected with commercial exchange telephone service.
3. Radiotelephone facilities for either point-to-point or mobile service.
4. Hand-carried portable radios or receivers, with transmitters strategically placed throughout the facility.
5. Key-operated electric call boxes located throughout the facility for guard supervision. By inserting a key in the call box, a guard can make a routine tour report or summon emergency assistance.

Alternate communications systems must be restricted to the use of the security force or to report emergencies. The wiring for alternate communications systems should be separate from other lines and placed in underground conduits. For emergency communication with agencies outside the facility, leased wires or a radio that can be tuned to police and fire department frequencies should be available.

The facility communications center, as the nerve center of the entire security program, should be designated a controlled area and access to it closely restricted.

All alarm and communication circuits should be tested at least once during each 8-hour period, preferably when a new shift comes on duty. At small facilities that do not employ guards, a test should be made just before closing for the night.

Chapter VII

GUARDS

No matter what structural, mechanical or electronic supplements are employed, the human element in the security program makes the difference between success and failure. The guard force is the enforcement arm of the program. It should be specifically organized, trained, and equipped to protect the security of cargo in the transportation system.

Authority

The authority of facility guards varies with the location and ownership of the facility and must accord with applicable Federal and State laws. Competent legal advice should be obtained before guards are instructed in their duties.

In all instances where civilian guards are employed, their power of arrest is limited to that of a private citizen. If they are deputized under Federal or State law, their arrest authority is only that specified in the deputization.

Investigations of pilferage or theft frequently require search and seizure actions. Unpleasant social, political and legal consequences can be suffered by the company and/or guard if an individual is subject to an overzealous assumption of authority.

Duties

Acting within the scope of its authority, the guard force should have standing orders to:

1. Safeguard cargo, material and equipment against sabotage, loss, theft, and damage.
2. Enforce the personnel identification system.
3. Patrol designated perimeters, areas, structures, and activities.
4. Apprehend intruders attempting to gain unauthorized access to the facility or persons in possession of stolen merchandise.
5. Determine that vaults, rooms, buildings, and access points are locked and secure during other than working hours.
6. Perform escort duties.
7. Enforce the system of control governing the entry or exit of cargo, property and documents at facility access points.
8. Respond to alarm signals or other emergencies.

9. Take all necessary action required in emergency situations affecting the security of the facility.
10. Enforce regulatory traffic controls to expedite the flow of cargo and prevent, or reduce the number of, accidents.
11. Report all matters affecting the security and safety of the facility.

Qualifications

Management has the responsibility to determine that guards are screened, selected or disqualified, based on rigorous mental and physical standards. Most of the qualities desired in a security guard are developed through training and become instinctive with experience.

Alertness, more than any other quality, will determine the effectiveness of a security guard. Even though hundreds of individuals show proof of the right and need to enter a restricted area, one contact could be with a person who should *not* enter. To detect this one exception, the guard must be constantly alert.

Sound judgment is essential to a guard. It is more than the application of common sense—it is the ability to arrive quickly at a wise decision. It involves the comparison of an unfamiliar situation with a similar situation of known values. The ability to compare, discriminate and decide must be developed by the guard. Security instructions cannot cover every situation. They can only provide guidelines, as each situation is unique and must be treated accordingly. Guards should be trained to call security headquarters when in doubt concerning a particular event.

The *courage* required in a security guard is more than bravery when confronted with potential physical assault. It involves the moral courage to apprehend an acquaintance caught thieving, to carry out his duties in the face of threats or ridicule, and to report all threats or offers of bribes.

Confidence is a state of mind free from doubt or misgivings. Confidence gives faith in one's self and one's abilities. Nothing can inspire self-confidence as much as a thorough knowledge of the job. An effective security guard must also have confidence in his leaders and other members of the security force. It is best achieved through training and competent supervision.

Physical fitness is indispensable in a security guard. His duty is arduous, difficult and demanding. He is exposed to all kinds of inclement weather and may be subject to physical attack by an intruder. The security of the facility and the life of the guard depend upon his physical fitness.

Tact, the ability to deal with others without giving offense, is desired in guards. He must be able to give instructions clearly and concisely, firmly and authoritatively, but without arrogance or discourtesy.

Security guard duty requires constant *self-control*. The security guard must be impersonal in the performance of his duty. If he loses control of his temper, he will lose control of the situation.

Loyalty is not the least important quality that a guard must have. An uncompromising commitment to the interests of his employer is essential.

Supervisors must be alert to any change in this attitude that might affect the guard's performance. Only a man of known integrity, responsibility, and trustworthiness should be assigned as a security guard.

Organization

Guard forces will differ organizationally from facility to facility. In every case, however, one man must be placed in charge of each shift. His authority must be clearly understood by all concerned. Divided authority can only lead to chaos and erosion of the security program.

Usually the guard force is organized on the basis of three or four shifts of 8 hours each. Shift changes should be made before peak periods of activity in the normal operation of the facility. The requirement for guard personnel on each shift is determined by dividing the total number of man-hours needed by the hours in the shift. To this figure must be added sufficient manpower to provide relief, which is normally based on one-half hour per man per shift.

The high cost of establishing a guard force dictates that care be taken to insure that posts and patrols are used only where necessary. If less expensive security measures will suffice, they should be used.

To determine the posts and patrols necessary at a facility, consideration must be given to the criticality, sensitivity, and vulnerability of the terminal and the cargo it processes. (See Chapter I.)

A stationary guard post will be required where cargo is so critical and vulnerable that loss or damage may occur if it is left unattended, where continuous human observation is required, or where mere access by unauthorized personnel is prejudicial to cargo security.

Motor or foot patrols will be required if two or more security areas are protected by passive security measures yet need periodic inspection by guards. If one or more guard posts exist that require periodic reinforcement, a mobile patrol can provide it. Similarly, such a patrol can provide periodic traffic control, emergency aid and relief as required.

Some posts and patrols need to be operational 1 hour or less per day, while others must be manned all 24 hours. When determining the requirements for specific hours of operation, factors to be considered are:

1. The operational hours of the facility.
2. The periods when employees are not present in certain buildings or areas.
3. The peak hours of vehicular and pedestrian traffic.
4. The hours of limited visibility.
5. The schedules of incoming and outgoing shipments.
6. The movement of critical items within the facility.
7. The scheduled activities that require special security measures.
8. The weekends and holidays when the facility will be nonoperational.
9. The passive security measures that are in effect.

Patrols are normally the most flexible segment of a guard force. If sufficient personnel are not available to fulfill all requirements, it is often possible to consolidate patrol functions. For short periods of time, one patrol may perform the duties assigned to two patrols without seriously affecting overall security. If two-man patrols are used, one man can be assigned to other duties temporarily.

It is more difficult to reassign a man from a stationary post. If a post is manned by two or more men, however, one man can assume other duties for a short time during slack periods in the movement of personnel, cargo and vehicles.

Manpower Requirements

The security officer must determine his manpower requirements in a systematic manner, with due regard for the capability of his force in both normal and emergency situations. The number of men needed for the guard force can only be determined by a detailed study of the posts, patrols and escorts necessary, the times during which each job must be performed, the amount of supervision required and allowances made for reserves, leave, sickness, and other contingencies. The security officer seldom will have sufficient manpower to provide all of the guards desirable. Therefore, he must carefully program for their economical and efficient use.

Annual requirements for posts and patrols are expressed in man-hours per year. The man-hours required to operate a post or patrol are obtained by multiplying the number of men required, the number of hours per day, the number of days per week and the number of weeks per year.

The number of man-hours per year which will be performed by one guard must be calculated based on personnel practices of the employer. If a guard is allowed 2 weeks vacation and averages 1 week sick leave, then he can be expected to be on the job 40 hours a week for 49 weeks, or 1,960 hours per year.

Two examples of a manpower requirement computation are shown below:

Post #1 requires two men, is operated 24 hours per day, 7 days each week:
2 (men) x 24 (hours) x 7 (days per week) x 52 (weeks per year) equal 17,472 (man-hours per year), divided by 1,960 equals 8.9 men.

Post #3 requires one man, 16 hours per day, 5 days per week:
1 x 16 x 5 x 52 = 4,160, divided by 1,969 equals 2.1 men.

Sentry Dogs

While the requirement for physical protection of cargo facilities continues to increase, funds for manpower and the availability of competent personnel is always limited. Properly trained and used sentry dogs help relieve the personnel shortage caused by this situation.

The mission of the sentry dog is to detect intruders, alert his handler and, if necessary, pursue, attack, and hold a trespasser. A sentry dog patrol is particularly effective in areas of little activity, such as isolated perimeters, remote storage areas, pipelines, and open storage areas.

The dog and the handler work as a team. As the outstanding qualifications of a sentry dog are his senses of smell and hearing, he can be used to best advantage during the hours of darkness or when the guard's vision is restricted. The dog keeps the guard on post more alert, increases his self-assurance, and relieves the monotony and loneliness of patrol duty.

The dog can be used as a warehouse guard. He can be placed in the building at the close of the working day and removed before the start of the next. This eliminates the need for a guard, requiring only a roving patrol to check on the dog. The dog will alert the guard force if an intruder attempts to enter his guard area.

There are both advantages and disadvantages to the use of sentry dogs. The presence of sentry dogs is a strong psychological deterrent to intruders. A dog is more effective during inclement weather than a guard and is better able to apprehend intruders during hours of darkness. Finally, there is less chance of a fatality through the release of a dog than through firing a weapon at an intruder.

The disadvantages are that attrition of personnel trained as handlers reduces the efficiency of a sentry dog program. The training period, to enable man and dog to work as a team, results in many unproductive hours. Personnel who like and understand dogs are not always available as handlers. Those who do volunteer may suffer a morale problem as most of the work is at night. The odor of petroleum will decrease the effectiveness of a dog's sense of smell, just as noise will affect his hearing. Many people disapprove of the use of dogs for sentry duty. The public relations impact of this practice cannot be ignored.

Although these problem areas cannot be disregarded, the value of the sentry dog should not be underestimated. Used as a supplement to other physical safeguards, he can be an invaluable asset to the security program.

Chapter VIII

CARGO ON THE MOVE

Responsibility

The responsibilities of the shipper, the carrier and the consignee must be clearly established if cargo is to be adequately protected in transit. Custody varies according to the size of the shipment and the means of transportation.

For shipments of less than the total capacity of a truck, railroad car, aircraft or ship, the carrier assumes responsibility when his agent acknowledges receipt at the shipping point and is relieved when delivery is made to the consignee.

The responsibility of the carrier for large shipments depends upon the mode of transportation used. If transportation is by truck, the carrier assumes custody when the vehicle is loaded. His responsibility ceases when the truck is unloaded at its destination. The railroad carrier's responsibility begins when the loaded and sealed car is coupled to a locomotive. He relinquishes custody when the car is spotted in the consignee's yard or unloaded at its destination.

Air and water carriers assume responsibility when an agent takes possession of the cargo from a shipper. This responsibility ends when the cargo is removed from the vessel or aircraft and is delivered to a freight forwarder, another carrier for transshipment, the consignee or his agent.

A shipper load and count (SL & C) movement in any of the above modes relieves the carrier of liability for shortages provided an accurate seal record is maintained.

Trucking Operations

Inclement weather and the possibility of accident are ever-present dangers to cargo in transit. They are hazards in addition to those discused in Chapter I. It is incumbent upon the security officer to develop preplanned procedures for road operation, which should be part of the security plan.

The integrity of those responsible for line haul should be unquestionable. Only responsible, screened employees should be assigned as drivers and helpers to transport high-value cargo. The equipment used must be in excellent condition to avoid breakdowns that require emergency security protection. This is often difficult, sometimes impossible and always expensive to provide. Modifications to equipment are often desirable. They can include added locking and alarm devices, removal of outside door hardware and installation of over-size fuel tanks where permissible.

Employees should receive strict instructions concerning procedures to be followed during relief or meal stops while in transit. The vehicle should be locked and parked where it can be observed. The nature of the cargo carried should not be discussed with anyone. The driver should not deviate from the preplanned route. In the event of equipment failure, he should notify the nearest terminal immediately. If it is necessary to move high-value cargo over a weekend or on a holiday, it should be delivered to a terminal where maximum security can be provided.

To further protect vehicles on the road. large. brilliant-hued numerals should be painted on the roof and sides. This will help identify the equipment if it is stolen or hijacked and a helicopter search is initiated.

In states where the use of double bottoms is permitted, the most valuable cargo should be loaded in the lead van.

Seals

Seals are invaluable to the protection of cargo in transit, but they are only as effective as the controls maintained over them. The responsibility for seal control must be vested in a specific individual who will maintain a record of all seals issued and to whom. Unissued seals should be stored in a locked container with limited access.

All cargo under seal entering a facility should be checked and the seal numbers recorded. If a seal is found to be broken or removed, or if the number does not agree with the one on the shipping document, an immediate item-by-item inventory of the shipment must be made.

Transfer Points

Transfer points, where cargo is transshipped from one mode of transportation to another or between two carriers of the same mode, are frequently areas where large losses can be expected. Cargo is often left unprotected, particularly in remote parts of the facility or yard. Shipping documents are apt to be carelessly handled at these points and shipments can be intentionally misrouted into the hands of the criminal.

To reduce loss by theft or misrouting at a transfer point, management must maintain strict accountability of all cargo and demand that a carrier who receives cargo from another accept custody for it in its original condition. Shipping documents must be examined carefully to guard against falsification or tampering. Employees of carriers using the facility must be able to prove their identity.

In-Transit Storage

While cargo is in the custody of the transportation system, it must frequently be stored for varying periods of time. During these intervals it is highly susceptible to loss, theft, or damage. A few elementary precautions will help reduce the claims filed against the responsible carrier.

Individual shipments of cargo should be kept intact and stacked as a unit. This will prevent accidental separation and loss of a portion of a shipment.

Fixed position lights in a storage area should be diffused to eliminate deep shadows. Each guard should be equipped with a strong, high-beam flashlight. Stacks should be arranged in accord with existing lighting to avoid creation of deep shadows.

Greater emphasis should be placed on personnel control than upon structural or mechanical protection in those areas where cargo is stored for short periods of time. The increased traffic generated in this situation, and consequent increased vulnerability of cargo to pilferage and theft, requires more alertness by guard patrols and more careful checking of the credentials of all individuals who are given access to the area. If possible, the storage area should be broken into sub-areas, with cargo handlers and truckers limited to the one sub-area compatible with their credentials and business purpose.

Protected cargo, a term common to shippers of Department of Defense material, consists of items which require special handling because of their value or sensitive nature. DOD places protected cargo in three categories:

a. *Sensitive.* Small arms, ammunition, and explosives which have a ready use during civil disturbances and other types of domestic unrest and which, if in the hands of militant or revolutionary organizations, present a definite threat to public safety.

b. *Pilferable.* Items vulnerable to theft and having a ready sale potential in illicit markets, as alcoholic beverages.

c. *Controlled.* Items which require additional control and security in accordance with published regulations and statutes, including: Money, negotiable instruments, narcotics, registered mail, precious metal alloys, ethyl alcohol, and drug abuse items.

High-value pilferable (Protected) cargo should be kept separate from other material and provided a greater degree of security. This material is best stored in a crib or security cage.

High-value, low-volume cargo, such as fissile radioactive materials, jewelry, furs, and securities require special handling and special security measures during storage. Cargo of this nature should pass from accountable officer to accountable officer. It should be under close surveillance contsantly and always be stored in an exclusion area. When placed in an exclusion area it should be registered, including time, date, accountable party and witness. The same procedure should be followed when the cargo departs from the facility.

Chapter IX

THE SECURITY OFFICER

A security officer is one of the most important employees transportation management hires. His background and qualifications should be carefully checked for it is he who will be formulating a security plan, selecting and training a guard force, and setting standards of conduct for that force and all employees.

Large facilities can recruit from experienced security officers with demonstrated track records. Experienced military officers who are leaving active duty may also provide the kind of expertise in planning, organization, training, and leadership required to develop a dynamic and reliable security program. Smaller facilities may find younger men with military police experience in one of the armed forces or experience on municipal police forces who are eager to demonstrate their ability in this field. There is an increasing realization that the market for career security officers is expanding and that satisfying and remunerative positions are opening up as security directors for large operations.

However, management cannot hire a security officer and then forget him. It must support him. It must show the personnel director who is screening applicants, the sales or marketing manager who is soliciting traffic, the shift foreman in the terminal, and the treasurer or accountant who is looking for reduced costs and increased profits, that top management appreciates the importance of security to efficient, profitable corporate operations. It has to listen carefully to the security officer's recommendations and, if he presents a convincing plan, be prepared to invest in the necessary resources to ensure safe and secure handling of cargo in its charge. The security officer should report directly to the highest organizational level consistent with good management.

The security officer, for his part, will find his responsibilities divided into planning (covered in preceding chapters), surveys, investigations, and education.

Surveys

The security officer will be continually occupied with security surveys, which he must conduct at a variety of times to assure that security hazards or deficiencies are noted and corrected.

An initial survey must be conducted at the time the security plan for the facility is being developed. It will provide the information needed to determine what safeguards are required to protect cargo processed through the terminal.

A supplementary survey will determine what security changes are required to compensate for altered organizational or operational functions within the facility, or for seasonal variations. It will also discover whether existing safeguards are operational, need maintenance or should be eliminated.

A follow-up survey will discover whether or not there has been compliance with the recommendations made as a result of the initial or supplemental surveys.

Special surveys can be scheduled to audit specific features of the security plan and to appraise the adequacy of security measures at various hours and under varying weather conditions.

Security surveys should be conducted by the security officer or designated, trained guard force personnel. Frequently, it is advisable to have technical advisers accompany the survey team to render assistance, particularly in the fields of lighting, alarms, and communications.

The security officer should establish an inspection schedule for specific areas of interest within the terminal. Activities that benefit from regular inspections include cargo receiving areas; cargo handling procedures; controlled areas, including limited and exclusion areas; disposal areas; truck entrance, loading/unloading and exit procedures; entrance and exit procedures for personnel; electric and electronic safeguards; and perimeter barriers. From time to time, the security officer should personally inspect the night and early morning shifts of the guard force.

Investigations

Any breach of physical security or loss of cargo should be promptly reported to the security officer, who will initiate an investigation and recommend corrective action.

The investigation of a security violation may be conducted by the facility security officer alone or, depending upon the type and location of the terminal, in cooperation with one or more of the following agencies: the local police, the Bureau of Customs, the Federal Bureau of Investigation, various commission authorities, airport authorities, port authorities or the Postal Service.

Employee Education

If the security program is to be truly effective, it must be actively supported and endorsed by employees in all positions throughout the facility. A continuing indoctrination and education program provides the understanding required to secure this support. Such an educational effort must have the backing of corporate headquarters and the facility manager.

All personnel should receive a complete indoctrination at the time of employment. Advanced, continuing programs should be established for supervisors and other key personnel to inform them of current problems and countermeasures. Periodic distribution should be made of posters, placards and leaflets dealing with specific aspects of the security program and the individual's participation in it.

In the general indoctrination of all employees, the instructor should stress not only the importance of security to the company, but also its meaning to the individual and his job. He should detail general measures in effect throughout the installation, including the pass system, personnel and vehicle control, controlled areas and parcel inspection. Further instruction should be applicable to the individual's work assignment.

Suggested personnel groupings and the level of security education required for each include:

1. Managers, supervisors, and security officers should receive instruction on the general responsibilities of their positions, the physical aids available as safeguards, the enforcement policies of the company and the procedures to be followed in an emergency.
2. Clerks, technicians, craftsmen, and other laborers should receive instruction in the need for constant surveillance, the identification of personnel in controlled areas, accident procedures and the importance of avoiding loose talk.
3. Drivers, equipment operators, and cargo handlers should receive instruction on the responsibilities of their positions, cargo accountability, cargo hazards, the danger of unrestrained talk, and emergency procedures to be followed in the terminal and in transit.

Security reminders can also be useful in keeping the topic before all employees. Large, bold posters carrying an attractive illustration and brief message can be effectively displayed at entrances, in lunchrooms or in corridors. Placards, which are smaller, may carry a longer, more detailed message and are designed for use on bulletin boards, in telephone booths, in washrooms or at counters. Leaflets or pamphlets can contain a greater amount of detail and are frequently distributed to the individual as a pay envelope enclosure.

Appendix I

CARGO SECURITY STANDARDS

Contents

Appendix I

CARGO SECURITY STANDARDS

Buildings

All terminal buildings housing cargo should be constructed of a material that will deter unlawful entry.

Ground floor windows should be steel barred. Bars should be spaced at intervals of not more than 6 inches and set in a steel frame which is securely affixed to the structure. All windows of buildings which adjoin other structures should also be barred.

Delivery and receiving doors should be constructed of a material that will deter unlawful entry and should be equipped with a self-locking device that will engage immediately when the door is closed. All delivery and receiving doors should remain closed and locked when not actually in use.

Pedestrian doors should be capable of being locked with a substantial lock. Work force facilities such as rest rooms, locker rooms and eating or lounging areas should be separated from the area in which cargo is stored.

Maximum security cribs, constructed of a substantial material which deters entry on all four sides, overhead and from the floor, which provides adequate space for storage of high value cargo, should be incorporated in each terminal building. They should be constructed in an area that is visible to management or security personnel or under frequent surveillance by the security patrol. (Only designated personnel should be allowed to enter this area and it may be desirable to secure it with a double lock requiring keys held by two different persons.)

The office in which delivery and pick-up orders are processed should be an area to which only authorized personnel have access. Room arrangements should be such that documents being processed are not available to or observable by unauthorized persons.

Fencing and Gates

Whenever possible, perimeter fencing should be provided around terminals in which merchandise is stored. The number of entrances and exits should be held to the minimum.

Fencing should normally be of the chain-link type, maximum 2-inch mesh, at least 9 gauge, and no less than 8 feet in height surmounted by an additional 2 feet of barbed wire. Where installed in soft earth, the bottom of the fencing should be anchored below grade and then backfilled. Where installed over concrete, the bottom of the fence should be no more than 2

inches above the surface, but high enough that, when sagging, it does not touch the surface. The top of the fence should be surmounted by at least three strands of barbed wire occupying no less than 2 feet vertically, but positioned at a 45-degree angle to the vertical.

Gates should be constructed of the same chain link fence material, be surmounted by an additional 2 feet of barbed wire, be within 2 inches of hard ground or paving, and be capable of being locked.

The fence line should be maintained in good condition and provisions made to avoid bumping and distortion of the fence by motor vehicles and other equipment. Fence lines should be kept free of shrubbery and other objects impeding the line of sight.

Gatehouses

Gatehouses should be self-contained units, equipped with at least two modes of communications for assured redundancy. These may be commercial telephone, radio, private telephone, or alarms. The exit gatehouse should be set back from the gate so that exiting vehicles can be stopped and examined on terminal property without the gate being opened.

It is essential that adequate lighting be provided in the area of the gatehouse so that documents and identifying features and contents of incoming and outgoing vehicles can be examined by the guard.

The area around the gatehouse should be free of encumbrances that restrict the guard's line of vision. Procedural signs advising drivers and visitors of the conditions of entry should be prominently displayed on the exterior of all entry gatehouses, preferably where they can be read by drivers before turning off the public street or road into the approach to the gate.

When warranted, photo recorders should be installed in gatehouses to provide a photo record of persons and their documents entering the terminal facility.

Locks and Key Control

All padlocks should be of a single standard type for control purposes. The use of other than the approved type is then easily determinable. When possible, the base of the padlock should indicate the company name. These padlocks should have multiple pin tumblers (at least six), interchangeable cores, a minimum tension pull resistance of 6,000 pounds on the shank portion, and shrouded shackle.

The use of other than company supplied padlocks should be prohibited. All lockers, gear boxes, gang boxes, cooper and/or carpenter shanties should be locked only with padlocks as described above.

No gates or exit areas should be secured by padlocks with the use of chains. All gates and exits should have proper latches which are secured to the surface with nonexposed bolts. The area surrounding the lock, particularly on the exposed side, should have metal backing to prevent accessibility.

The use of electrical switch locks is recommended in gate and exit areas. These permit use of a microswitch to record and indicate the opening of a given lock on a panel or central control indicator.

Key control should be rigid. For every key given out, a signature should be required and a card file maintained which would indicate the history of each key. Duplicate keys should be secured under absolute control. The distribution of submaster, master or grand master keys should be highly restricted. The key control of all equipment, particularly that which could be used in the commission of a theft, such as hi-los, stackers and yard tractors, should be very strict. No keys should be left in any equipment overnight or when not assigned. This should also apply to equipment held in the maintenance or repair shops.

Alarm and Communications Systems

All terminal buildings in which and through which merchandise in the transportation scheme is moving should be equipped with an intrusion detection system. However, alarm systems should be considered as an adjunct to fencing, lighting or guard forces, and not in lieu thereof.

Circuit boards, lines and control panels for alarm systems should be placed in such locations and constructed in such a manner that they are protected from vandalism or deliberate attempts to disrupt or destroy their usefulness.

There are various recognized alarm systems; the type that meets the needs of a particular facility can best be determined by a qualified security specialist.

The three most popular alarm systems are:

(1) **The Audible Alarm,** which, when activated, draws attention to the facility or a portion thereof.

(2) **The Silent Alarm,** which is designed to alert private guard forces or municipal police departments. When considering this system, managers should determine the time required for the guard force to respond to the alert.

(3) **The Visible Alarm,** which increases light intensity in a given area by utilizing additional lights, by explosive flares, or by rockets.

(NOTE.—Alarms should not be so sensitive that they can be activated by rodents, birds, or windblown debris.)

Lighting

Adequate lighting should be provided between dusk and dawn at all entrances and exits, along all boundary lines, around all storage structures, and in all parking areas.

The primary power source at a facility is usually a local public utility. However, to protect against a public power failure an alternate source of power adequate to provide lights at key control points should be provided.

A gasoline-driven generator that starts automatically upon the failure of outside power is the preferred alternate, although battery power may also be used.

Tables I and II, following, provide standards for area coverage and lighting intensity.

TABLE I.—Lighting area coverage

Type of area	*Type of lighting*	*Width of lighted strip (in feet)*	
		Inside fence	*Outside fence*
Isolated perimeter	Glare	25	200
Isolated perimeter	Controlled	10	70
Semi-isolated perimeter	Controlled	10	70
Nonisolated 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 II.—Lighting intensity

Location	*Foot-candles on horizontal plane at ground level*
Vehicular and pedestrian entrances	2.0
Vital structure and other sensitive areas	2.0
Unattended outdoor parking area	1.0

Guard Requirements

Standards for the guard force should include complete background investigations, physical and mental examinations to meet established standards.

The guard should be physically capable of vigorous physical training in self-defense.

Uniforms should be distinctive and complete. Uniforms and equipment should meet high standards of cleanliness and maintenance.

Prior to any duty assignment, basic training must be given to all guards. Training should include such techniques as patrol, both mounted and dismounted, report writing, log and recordkeeping, use of security equipment, fire and safety regulations, self-defense, crowd and riot control, and firearms instruction.

Under most conditions, guards should not be allowed to remain too long in a given post; they should be rotated periodically. However, under certain conditions, keeping the guard at one post could be an asset, especially when personal recognition of people is desired. Examples are personnel entrances to an office building, tradesmen gates, monitoring stations, areas where recognition and protocal are required, and administrative posts.

Vehicle Control

Movements of all vehicles within the terminal should be strictly controlled. The controls must be a standard operating procedure and prominently posted.

All trucks and conveyances entering the facility should be examined by gate guards. Guard check should include registration of truck, name of driver and helper, license check of vehicle operator and his driver or helper. If possible, a photo record of the driver and his documents should be made before he enters the terminal. Strict supervision of loading and unloading operations should be incorporated into procedures. No vehicle should be opened except when actually being loaded, unloaded, or inspected.

Other procedures for vehicle control and operations should include a record on all inbound and outbound trailers and containers and, when not being moved, their storage locations, and a report of any seal discrepancies noted.

Parking lots for personal vehicles of employees and visitors should be located outside of and separated from freight handling areas. Only cargo-carrying or handling vehicles should be permitted in controlled areas.

It is advisable to separate entry and exit roadways and gates if the facility permits. Flow of traffic then is essentially one-way.

Special Problems—High-Value Cargo

Transportation of merchandise such as fissile radioactive materials, jewelry, furs, optical goods, cameras, electronic articles, whisky, and ammunition present special security considerations. Precautions include scheduling arrival of goods at hours which permit prompt pickup, use of secure areas, continuous guards, selected reliable drivers, delivery in vehicles with two-way radio equipment, a check-point system, convoying and "shotgun" guards, use of antihijack equipment (locked doors, no steps, high cab) and coordination with Federal and local police agencies.

All protective measures for movement of high value mechandise must be set out in a standard operating procedure.

Only that equipment which is sound should be utilized in transport of high-value cargo.

When regular accounts requiring regular handling of high-value cargo are acquired, modifications to equipment should be made. This cound include removal of running boards, addition of extra locking devices, alarm equipment, and oversize gas tanks (where permissible). Routing of vehicles should be varied continuously where practicable.

Key control for all equipment undergoing maintenance should be stressed. Often, a breakdown in key control takes place when equipment is turned over to the maintenance department for service. When equipment breaks down while on the road, a preplanned procedure should be effected to safeguard high-value cargo.

The shipper can be advised as to how to avoid security pitfalls, whether in packaging or advertising. He must carefully control information regarding shipments, destinations, times of arrival and departure and routes to be traveled among his own employees, and on labels and packaging. Further, the consignee must plan for immediate pickup at destinations to avoid high-value cargo being needlessly exposed.

Appendix II

CARGO SECURITY CHECKLIST

Contents

Appendix II

CARGO SECURITY CHECKLIST

The checklist below may be used for many different types of facilities. It permits each facility manager to select those elements pertaining to his establishment and location in making his own security survey.

1. Barriers

a. Is the perimeter of the facility or activity defined by a fence of other type physical barrier?

b. If a fence or gate is used, does it meet the minimum specifications?

(1) Is the top guard strung with barbed wire and angled outward and upward at a 45° angle?

(2) Is it at least 10 feet total height?

(3) Is it located so that it is not adjacent to mounds, piers, docks, or any other aid to surmounting it?

c. If building walls, floors and roofs form a part of the perimeter barrier, do they provide security equivalent at least to that provided by chain link fence? Are all openings properly secured?

d. If a masonary wall or building forms a part of the perimeter barrier, does it meet minimum specifications of perimeter fencing?

e. If a river, lake or other body of water forms any part of the perimeter barrier, are security measures equal to the deterrence of the 10-foot fence provided?

f. Are openings such as culverts, tunnels, manholes for sewers and utility access, and sidewalk elevators which permit access to the facility properly secured?

g. List number, location, and physical characteristics of perimeter entrances.

h. Are all portals in perimeter barriers guarded, secured, or under constant surveillance?

i. Are all perimeter entrances equipped with secure locking devices and are they always locked when not in active use?

j. Are gates and/or other perimeter entrances which are not in active use frequently inspected by guards or management personnel?

k. Is the security officer responsible for security of keys to perimeter entrances? If not, which individual is responsible?

l. Are keys to perimeter entrances issued to other than facility personnel, such as clearing, trash removal, vending machine service personnel?

m. Are all normally used pedestrian and vehicle gates effectively and adequately lighted so as to ensure—

(1) Proper identification of individuals and examination of credentials,

(2) That interiors of vehicles are clearly lighted, and

(3) That glare from luminaries is not in guard's eyes?

n. Are appropriate signs setting forth the provisions for entry conspicuously posted at all principal entrances?

o. Are clear zones maintained for the largest vehicles on both sides of the perimeter barrier? If clear zone requirements cannot be met, what additional security measures have been implemented?

p. Are automoblies permitted to park against or too close to perimeter barrier?

q. What is frequency of checks made by maintenance crews of condition of perimeter barriers?

r. Do guards patrol perimeter areas?

s. Are reports of inadequate perimeter security immediately acted upon and the necessary repairs effected?

t. Are perimeters protected by intrusion alarm devices?

u. Does any new construction require installation of additional perimeter barriers or additional perimter lighting?

2. Lighting

a. Is the perimeter of the installation protected by adequate lighting?

b. Are the cones of illumination from lamps directed downward and away from the facility proper and away from guard personnel?

c. Are lights mounted to provide a strip of light both inside and outside the fence?

d. Are lights checked for proper operation periodically and inoperative lamps replaced immediately?

e. Do light beams overlap to provide coverage in case a bulb burns out?

f. Is additional lighting provided at vulnerable or sensitive areas?

g. Are gate guard boxes provided with proper illumination?

h. Are light finishes or stripes used on lower parts of buildings and structures to aid guard observation?

i. Does the facility have a dependable auxiliary source of power?

j. Is there alternate power for the lighting system independent of the plant lighting or power system?

k. Is the power supply for lights adequately protected? How?

l. Is the standby or emergency equipment tested periodically?

m. Is emergency equipment designed to go into operation automatically when needed?

n. Is wiring tested and inspected periodically to insure proper operation?

o. Are multiple circuits used? If so, are proper switching arrangements provided?

p. Is wiring for protective lighting securely mounted?

(1) Is it in tamper-resistant conduits?

(2) Is it mounted underground?

(3) If above ground, is it high enough to reduce possibility of tampering?

q. Are switches and controls properly located, controlled and protected?

(1) Are they weatherproof and tamper resistant?

(2) Are they readily accessible to security personnel?

(3) Are they located so that they are inaccessible from outside the perimeter barrier?

(4) Is there a centrally located switch to control protective lighting? Is it vulnerable?

r. Is the lighting system designed and locations recorded so that repairs can be made rapidly in an emergency?

s. Is adequate lighting for guard use provided on indoor routes?

t. Are materials and equipment in shipping and storage areas properly arranged to permit adequate lighting?

u. If bodies of water form a part of the perimeter, does the lighting conform to other perimeter lighting standards?

3. Alarms

a. Is an alarm system used in the facility?

(1) Does the system indicate an alert only within the facility?

(2) Does it signal in a central station outside the facility?

(3) Is it connected to facility guard headquarters?

(4) Is it connected directly to an enforcement headquarters outside the facility proper? Is it a private protection service? Police station? Fire station?

b. Is there any inherent weakness in the system itself?

c. Is the system supported by properly trained, alert guards?

d. Is the alarm system for operating areas turned off during working hours?

e. Is the system tested prior to activiating it for nonoperational periods?

f. Is the alarm system inspected reguarly?

g. Is the system tamper resistant? Weatherproof?

h. Is an alternate alarm system provided for use in the event of failure of the primary system?

i. Is an alternate or independent source of power available for use in the event of power failure?

j. Is the emergency power source designed to cut in and operate automatically?

k. Is the alarm system properly maintained by trained personnel?

l. Are periodic tests conducted frequently to determine the adequacy of response to alarm signals?

m. Are records kept of all alarm signals received to include time, date, location, action taken, and cause for alarm?

4. Communications

a. Is the secuity communications system adequate?

b. What means of communications are used?

(1) *Telephone.*
- (a) Is it a commercial switchboard system? Independent switchboard?
- (b) Is it restricted for guard use only?
- (c) Are switchboards adequately guarded?
- (d) Are there enough call boxes and are they conveniently located?
- (e) Are open wires, terminal boxes, and cables frequently inspected for damage, wear, sabotage, and wire-tapping?
- (f) Are personnel cautioned about discussing cargo movements over the telephone?

(2) *Radio.*
- (a) Is proper radio procedure practiced?
- (b) Is an effective routine code being used?
- (c) Is proper authentication required?
- (d) Is the equipment maintained properly?

(3) *Messenger.*
- (a) Is the messenger always available?

(4) *Teletype.*
- (a) Is an operator available at all times?

(5) *Public address.*
- (a) Does it work?
- (b) Can it be heard?

(6) *Visual signals.*
- (a) Do all guards know the signals?
- (b) Can they be seen?

c. Is security communications equipment in use capable of transmitting instructions to all key posts simultaneously?

d. Does the equipment in use allow a guard to communicate with guard headquarters with minimum delay?

e. Is there more than one system of security communications available for exclusive use of security personnel?

f. Does one of these systems have an alternate or independent source of power?

g. Has the communications center been provided with adequate physical security safeguards?

5. Personnel Identification and Control

a. Is an identification card or badge used to identify all personnel within the confines of the controlled areas?

b. Is the identification medium designed to provide the desired degree of security?

c. Does the identification and control system include arrangements for the following:
- (1) Protection of the meaning of coded or printed components of badges and passes?
- (2) Designation of the various areas requiring special control measures to which the badge holder may be authorized entrance?
- (3) Strict control of identification data?
- (4) Clear explanation and description of the identification data used?
- (5) A clear statement of the authorization and limitations placed upon the bearer?
- (6) Details of where, when, and how badges shall be worn?
- (7) Procedures to be followed in case of loss or damage to identification media?
- (8) Procedure for recovery and invalidation?

d. If a badge exchange system is used for any restricted area, does the system provide for:
- (1) Comparison of badge, pass, and personnel?
- (2) Physical exchange of restricted area badge for general authorization badge at time of entrance and exit?
- (3) Logging a record of each badge exchanged?
- (4) Inventory of badges issued by security personnel at the start and completion of tours of duty?
- (5) Location of personnel who have not checked out of the area at the close of each tour of duty?
- (6) Security of badges not in use?

e. Are messengers who are required to traverse areas of varying degrees of security provided with special identification?

f. Are the prescribed standards for access to exclusion areas supplemented with arrangements for the following:
- (1) At least one representative of management or security is in the area at all times when work is in progress?
- (2) No other persons are permitted to enter the area until one representative of management or security has entered?
- (3) A representative of management or security remains until all others have departed?

g. Are personnel, who require infrequent access to a critical area and who have not been issued regular security identification for the area, treated as "visitors" thereto, and issued either (1) a visitor's badge or pass, or (2) a special pass?

h. Are all personnel required to wear the security identification badge while on duty?

i. Do guards at control points compare badges to bearers both upon entry and upon exit?

j. Is supervision of personnel charged with checking identification badges sufficient to insure continuing effectiveness of identification and control system?

k. Are badges recorded and controlled by rigid accountability procedures?

l. Are lost badges replaced with one bearing a different number or one that is otherwise not identical to the one lost?

m. Are procedures relative to lost, damaged, and/or forgotten badges adequate?

n. Are temporary badges used?

o. Are lists of lost badges posted at guard control points?

p. Are badges of such design and appearance as to enable guards and other personnel to recognize quickly and positively the authorizations and limitations applicable to the bearers?

q. How long ago were currently used badges originally issued?

r. Do existing procedures insure the return of identification badges upon termination of employment?

s. Are badges similar to or identical to employee badges issued to outside contractor employees working within the installation?

t. Have local regulations governing identification and control been revised in any material respect since first established?

u. Are all phases of the system under supervision and control of a security officer?

v. Is an effective visitor escort procedure established?

w. Are visitors required to conspicuously display identification on outer garments at all times while on installation?

x. When visitors leave the installation, are they required to turn in their identification badges, and is the departure time in each case recorded on the visitors' register?

y. What procedures are invoked when visitor identification badges are not turned in prior to departure of the visitor?

z. Is there a central receptionist?

(1) If "yes," specify functions.

(2) Are functions performed under the supervision of a security officer?

aa. Are receptionists (or guards) stationed at different focal points to maintain visitor control?

bb. Are there special procedures applicable to visitors requiring access to cargo handling documents?

cc. Are special visitors, e.g., vendors, tradesmen, utility servicemen or special equipment servicemen, issued a special or destinctive type of visitor badge?

dd. What measures are employed, other than the issuance of identification badges, to control the movements of personnel from other transportation companies working within the perimeter of the facility?

ee. Does the system used for identification of truck drivers and helpers conform with security regulations?

ff. Is the security officer the single responsible official for all aspects of visitor control?

6. Package and Material Control

a. Is there standard procedure on control of packages and materials?

b. Are all guards conversant with the package control measures?

c. Are notices on restriction and control procedures prominently displayed at each active entrance and exit?

d. Is there a checkroom where employees and visitors can leave their packages?

(1) Is an adequate receipt system in effect?

(2) Are packages inspected in the owner's presence before a receipt is issued?

(3) Is access to the checkroom restricted to authorized personnel only?

(4) Is a policy established for disposition of items left beyond a specified period?

e. Are spot checks of persons and vehicles conducted and, if so, are frequency and scope thereof indicated?

(1) Regular search.

(2) Spot search.

(3) Special search.

f. Are detection devices used?

(1) X-ray or other similar device.

(2) Metal detector.

(3) Other; evaluate effectiveness.

g. Is a property removal slip, signed by an authorizing official, required when property is being removed from the facility?

h. Are removal slips available in the security office for signature by officials authorizing property removals?

i. Are property removal slips surrendered to guards at exit points?

j. Are special rules established for package and material handling?

(1) Is package and material pass used to exempt bearer from search?

(a) Is time, date, bearer's name, using agency, and description of the contents, properly recorded thereon?

(b) Is preparation and issue rigidly controlled?

(c) Is it serially numbered?

(d) Does it provide for signature of validating officials?

(e) Is signature card readily available to guards for comparison?

(2) Is a trustworthy and identified courier used at all times?

k. Are special clothing issued for wear in the facility to prevent the introduction or removal of unauthorized items?

l. Is an effective procedure used for control and search of special vehicles?

(1) Emergency vehicles.
(2) VIP vehicles.
(3) Special courier vehicles.
(4) Vendor's vehicles.
(5) Vehicles with loads which are impracticable to search.

m. Is there close coordination between security headquarters and the activities that handle cargo movements?

n. Are new employees given appropriate instructions relative to the handling and safeguarding of cargo?

7. Vehicle Control

a. Are vehicles which are allowed regular access to the facility registered with the security officer?

b. Have definite procedures been established for the registration of private cars and are they issued in writing?

c. Do the vehicle registration requirements apply also to motor vehicles owned or operated by employees of any individual, firm, corporation or contractor whose business activities require daily or frequent use of vehicles on the facility?

d. Is annual or more frequent registration required?

e. What information is incorporated in registration application forms?

f. Do the prescribed prerequisites for registration include a valid State registration for the vehicle and a valid State operator's license?

g. Is mechanical inspection of vehicles and/or proof of financial responsibility required as a prerequisite of authority to operate a vehicle within the facility?

h. Are decalcomania or metal permit tags affixed to all vehicles authorized to operate within the facility?

i. Do registration permits bear a permanently affixed serial number and numerical designation of year of registration?

j. Do the regulatory controls for registration include:

(1) Prohibition against transfer of registration permit tags for use with a vehicle other than the one for which originally issued?
(2) Replacement of lost permit tags at the registrant's expense?
(3) Return of tags to the security officer when the vehicle is no longer authorized entry into facility?
(4) Destruction of invalidated decalcomania or metal tags?

k. What is the nature and scope of registration records maintained by the security officer?

l. Do the gate guards make periodic checks to insure that vehicles are operated on the premises only by properly licensed persons?

m. Is a specified system used to control the movement of commercial trucks and other goods conveyances into and out of the installation area?

n. Are loading and unloading platforms located outside the operating areas, separated one from the other, and controlled by guard-supervised entrances?

o. Are all trucks and other conveyances required to enter through service gates manned by guards?

p. If trucks are permitted direct access to operating areas, are truck drivers and vehicle contents carefully examined?

q. Does the check at entrances cover both incoming and outgoing vehicles?

r. Are truck registers maintained?

s. Are registers maintained on all company vehicles entering and leaving the facility?

t. Are escorts provided when vehicles are permitted access to operating or controlled areas?

u. Does the supervision of loading and unloading operations insure that unauthorized goods or people do not enter or leave the installation via trucks or other conveyances?

v. Are company trip tickets examined?

w. Is a temporary tag issued to visitors' vehicles?

x. Are automobiles allowed to be parked within operating or controlled areas?

y. Are parking lots provided?

z. Are interior parking areas located away from sensitive points?

aa. Are interior parking areas fenced so that occupants of automobiles must pass through a pedestrian gate when entering or leaving the working area?

bb. Are separate parking areas provided for visitors' vehicles?

cc. What is the extent of guard surveillance over interior parking areas?

dd. Are there restrictions against employees entering private vehicle parking areas during duty hours?

ee. Are automobiles allowed to park so close to buildings or structures that they would be a fire hazard or obstruct fire fighters?

ff. Are automobiles permitted to be parked close to controlled area fences?

gg. Are parking facilities adequate?

8. Lock Security

a. Has a key control officer been appointed?

b. Are the locks and keys to all buildings and entrances controlled by a key control officer?

c. Does the key control officer have overall responsibility for issuance and replacement of locks and keys?

d. Are keys issued only to authorized personnel?

e. Are keys issued to other than facility personnel?

f. Is the removal of keys from the premises prohibited?

g. Are keys not in use secured in a locked, fireproof cabinet?

h. Are current records maintained indicating:

(1) Clear record of person to whom key is issued?

(2) Time of issue and return of keys?

(3) Buildings and/or entrances for which keys are issued?

(4) Number and identification of keys issued?

(5) Location and number of master keys?

(6) Location and number of duplicate keys?

(7) Location of locks and keys held in reserve?

i. Is a current key control directive in effect and understood?

j. Are locks changed immediately upon loss or theft of keys?

k. Are inventories and inspections conducted by the key control officer to insure compliance with directives? How often?

l. If master keys are used, are they devoid of markings identifying them as such?

m. Are losses or thefts of keys promptly investigated by the key control personnel?

n. Must all requests for reproduction or duplication of keys be approved by the key control officer?

o. Are locks on inactive gates and storage facilities under seal? Are they checked periodically by guard personnel?

p. Are locks rotated within the installation at least semiannually?

q. Where applicable, is the manufacturer's serial number on combination locks obliterated?

r. Are measures in effect to prevent the unauthorized removal of locks on open cabinets, gates, or buildings?

9. Guard Forces

a. Is a guard force provided? Is it responsive to management authority?

b. Indicate authorized and actual strength, broken down by positions.

c. Have there been changes since the last survey in either the authorized or actual guard force strength?

d. Is present guard force strength commensurate with the degree of security protection required?

e. Is the use of guard forces reviewed periodically to assure effective and economical use?

f. Is supervisory responsibility for guard force operations vested in the security officer?

g. Is a guard headquarters provided?

h. Does the guard headquarters contain control equipment and instruments of all alarm, warning, and guard communications systems?

i. Are guards familiar with the communications equipment used?

j. Does the guard headquarters have direct communication with local municipal fire and police headquarters?

k. Do members of the guard force meet the minimum qualifications standards?

l. Are guards armed while on duty? If so, with what type of weapon?

m. Are the weapons kept in arms racks and adequately secured when not in use?

n. Are ammunition supplies properly secured and issued only for authorized purposes?

o. Is each member of the guard force required to complete a course of basic training and take periodic courses of in-service or advanced training?

p. Are the subjects included in the various training courses adequate? Does the training cover:

(1) Hand-to-hand combat?

(2) Care and use of weapons?

(3) Common forms of pilferage, theft, and sabotage activity?

(4) Types of bombs and explosives?

(5) Location of hazardous materials and processes?

(6) Location and use of fire protective equipment, including sprinkler control valves?

(7) Location and operation of all important steam and gas valves and main electrical switches?

(8) Conditions which may cause fire and explosions?

(9) Location and use of first aid equipment?

(10) Duties in the event of fire, explosion, natural disaster, civil disturbance, blackout or air raid?

(11) Use of communication system?

(12) Proper methods of search?

(13) Observation and description?

(14) Patrol work?

(15) Supervision of visitors?

(16) Preparation of written reports?

(17) General and special guard orders?

(18) Authority to use force, conduct searches, and make arrests?

q. Are periodic examinations conducted to insure maintenance of guard training standards?

r. Are activities of the guard force in consonance with established policy?

s. Is supervision of the guard force adequate?

t. Are general and special orders properly posted?

u. Are guard orders reviewed at least semiannually to insure applicability?

v. Are periodic inspections and examinations conducted to determine the degree of understanding and compliance with all guard orders?

w. Do physical, functional, or other changes at the installation indicate the necessity for, or feasibility of, (1) establishing additional guard posts, or (2) discontinuing any existing posts or patrols?

x. Is two-way radio equipment installed on all guard patrol cars?

y. Are duties other than those related to security performed by guard personnel?

z. Are guard patrol cars equipped with spotlights?

aa. Does each guard on patrol duty carry a flashlight?

bb. Do guards record or report their presence at key points in the installation by means of (1) portable watch clocks, (2) central watch clock stations, (3) telephones, or (4) two-way radio equipment?

cc. Are guard assignments and patrol routes varied at frequent intervals to obviate an established routine?

10. Recommendations

Any recommendations for correction of observed deficiencies must be reasonable in cost. Each recommendation must be carefully weighed to insure that the additional security obtained is worth the expense involved. In laying out the long-range security programs involving extensive construction, hiring of additional guards, installation of illumination and other protective devices, as well as specifying immediate remedial actions, primary consideration must be given to dollar value received versus dollar value spent. Whenever possible, maximum use will be made of existing facilities, supplies and equipment by renovation in order to reduce expenditures. It is also possible to improve security by improving discipline in administrative procedures. This step is probably quickest to produce results and most cost effective.

To The Reader:

It is the intention of the Department of Transportation and the affiliated agencies responsibible for preparation of this manual to maintain it as a useful and timely tool for the transportation industry.

If additional information, the inclusion of photographs and illustrations are desirable or if some of the information contained in the handbook is superseded by newer practices, please inform us. We are particularly interested in receiving illustrations, sketches, or photographs showing application of the principles contained in the *Guidelines*. These suggestions will be incorporated in future revisions.

We welcome all sugestions that will improve the content of the handbook. Our purpose is to improve the security of all cargo in the transportation system. To assure the accomplishment of this goal, please send your recommendations to:

Director
Office of Transportation Security (TSA–60)
Department of Transportation
Washington, D.C. 20590

U.S. GOVERNMENT PRINTING OFFICE : 1979 O—288-637

END