AC NO: 107-1

DATE: 19 May 1972

ADVISORY CIRCULAR

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

SUBJECT: AVIATION SECURITY - AIRPORTS

1. PURPOSE. This document furnishes guidance to those individuals and organizations having responsibilities under Part 107 of the Federal Aviation Regulations. It also provides recommendations for establishing and improving security for restricted or critical facilities and areas the security of which is not dealt with by Part 107. The information is provided regarding the preparation of an airport security program. This Circular describes minimum acceptable standards for (a) preparation of a master security plan, (b) establishing and maintaining a suitable authorized persons identification program, and (c) establishing and maintaining an adequate identification system for certain ground vehicles. It also makes recommendations concerning conducting an airport security survey, establishing security committees, security education for airport personnel, the proper use of law enforcement personnel and liaison with appropriate law enforcement agencies and FAA Air Transportation Security Field Offices.

2. OBJECTIVE. To improve the overall security of airports in the interest of aviation safety.

James T. Murphy

JAMES T. MURPHY
Director of Air Transportation Security

Initiated by: SE-320

3. BACKGROUND. The safety and security of civil aviation and its ground facilities are endangered by an ever increasing variety of unlawful acts.

There were 123 hijacking incidents involving U. S. carrier aircraft during the period from 1 May 1961 to 16 March 1972. Most have occurred since 1968. Bomb threats against U. S. air carrier aircraft averaged approximately 500 annually from 1966 through 1970. There were 1,145 bomb threats made against U. S. carrier aircraft in 1971. The number of bomb threats and extortion attempts increased dramatically in early 1972. Live bombs were discovered on three air carrier aircraft. One bomb exploded aboard an air carrier aircraft on the ground causing extensive damage to the aircraft. In this specific instance it appears the bomb had been placed on the aircraft prior to its departure but fortunately did not explode until several hours after it had landed.

President Nixon, on 9 March 1972, ordered the Secretary of Transportation to make effective immediately a Federal Aviation Regulation requiring certain air carriers and commercial operators operating large aircraft (other than helicopters) to institute certain security measures. The President also ordered that final rulemaking action be expeditied regarding a proposed Part 107, Airport Security, of the Federal Aviation Regulations.

4. RESPONSIBILITIES. Part 107 assigns the responsibility for airport security to the airport operators. Part 107 defines "airport operators" as "operators of airports regularly serving scheduled air carriers holding certificates of public convenience and necessity issued by the Civil Aeronautics Board and commercial operators engaging in intrastate common carriage covered by /section/ 121.7...., operating aircraft other than helicopters." Certain air carriers and commercial operators have the responsibility for controlling access to their own aircraft as required under FAR 121.538. Air carriers and airport operators should coordinate plans as necessary to achieve the desired security goals. Under Part 107, airport operators are required to establish master security plans for all air operations areas except those which are occupied or controlled exclusively by a certificate holder required to have a security program under FAR 121.538 (or is an "adjacent" area as described in paragraph 7 below). Security in these instances is the responsibility of the carrier.

5. GENERAL. A sound airport security program will be the result of detailed advance planning. All facilities have varying degrees of vulnerability to identified security hazards. The degree of risk from each specific hazard depends upon such variables as the type of facility or area involved, value or criticality, physical layout and protective measures which have been established. It does not appear that it is economically feasible or physically possible to establish the same degree of protection for all facilities. The degree of protection warranted is dictated by its criticality and relative vulnerability, and qualified by the effect of the protective measures on its operational effectiveness.

The first step toward achievement of adequate protection is a detailed physical inspection of all areas, facilities and operations existing at the airport. The inspection, which is more appropriately called a security survey, should assess the existing safeguards and procedures for adequacy as well as indicating potential or actual security deficiencies or hazards. The security survey is the recommended basis from which to develop a plan to provide for adequate safeguards which can deny unauthorized personnel access to restricted or critical facilities and areas. Further discussion of the security survey may be found in paragraph 13 of this Circular.

Of great importance to the security of any airport is the selective application, from a variety of protective measures, of those necessary to achieve "security-in-depth." Security lighting systems, alarms, locks, gates, fences, guards, access controls, and badge systems are but a few of the measures which can be utilized to increase the security of an area.

6. IMMEDIATE ACTIONS. Under Part 107 each airport operator is required to immediately adopt and put into use facilities and procedures designed to prevent or deter persons and vehicles from unauthorized access to air operations areas. A threat to aviation safety exists now. Every reasonable attempt should, therefore, be made to limit access to air operations areas to authorized persons only. At least the following measures should be instituted immediately.

a. Designate Air Operations Areas.
b. Post signs or notices which read "Authorized Persons Only" or similar language.
c. Lock or control all doors and entrances to the air operations areas as fire or safety regulations permit.
d. Concentrate law enforcement activities on airport security matters to the extent possible.

e. Illuminate air operations areas during the hours of darkness to the degree possible with existing lighting.
f. Preclude unauthorized vehicles from entering air operations areas.
g. Challenge all persons in air operational areas who appear to have gained unauthorized access.
h. Provide escorts for visitors to air operations areas.
i. Advise affected personnel of their security responsibilities.
j. Implement other security measures as appropriate and practical.

7. AIRPORT SECURITY PROGRAM. Under Part 107 each airport operator is required to prepare in writing and submit to the Regional Director for the region in which the airport is located a security program for approval by the Administrator. Section 107.3(a)(2) requires that the program include a master security plan which "identifies separately each air operations area and each other area of the airport, including those areas exclusively occupied or controlled by another person under a lease or other contractual arrangement with the airport operator or owner;" and designates each identified area of the airport "that has no protection or inadequate protection against unauthorized access to air operations areas;" and (except as to access from a non-air operations area to an air operations area where both areas are adjacent and exclusively occupied or controlled by a certificate holder that is required to have a security program under § 121.538); "sets forth a plan for improving or establishing protection against unauthorized access to air operations areas showing a time schedule" for each designated area. Under section 107.3(a)(2) the security program must also include means and procedures for the identification of authorized persons and ground vehicles.

a. Master Security Plan. Airport operators are requested to submit clear and comprehensive plans. The following items should be covered as a minimum.

(1) Description of Airport. Describe to include location, acreage, wooded areas, water areas, parking lots, buildings, etc. Particular attention should be given to all air operations areas. Maps, plats, schematics, photos, etc., should be provided which show the airport as a whole and the surrounding areas.

(2) Airport Activity. Identify all air carriers that serve the airport. Indicate scope of the airports operation, such as

number of flights and passengers, amount of cargo handled, normal peak and slack periods of operation and other pertinent details.

(3) Security Responsibilties. List names of airport operator and person responsible for airport security. Also indicate the security responsibilities of other officials involved in the security program.

(4) Air Operations Areas. This section should describe and identify separately each air operations area and each other area of the airport, including those areas exclusively occupied or controlled by another person under a lease or other contractual arrangement with the airport operator or owner. The security posture of each should be described as having no protection or inadequate protection against unauthorized access to air operations areas. Specific reference should be made to the following:

(a) Physical Security Measures. Describe physical security measures that are intended to protect against unauthorized access, to include barriers, lighting, locks, alarms and guards.

(b) Identification of Persons. Describe the existing personnel identification system.

(c) Identification of Ground Vehicles. Describe the existing vehicle identification system in use.

(5) Planned Improvements. Under Part 107 each airport operator is required (except as to access from a non-air operations area to an air operations area where both areas are adjacent and exclusively occupied or controlled by a certificate holder that is required to have a security program under § 121.538) to set forth "a plan for improving or establishing protection against unauthorized access to air operations areas showing a time schedule for each area designated...." Significant progress should be planned to be achieved within reasonable time limits.

(a) Designation of Air Operations Areas. Air operations areas should be designated by the posting of signs which provide notification to all concerned that entrance into these areas must be authorized. The signs or notice should be of sufficient size and clarity to be readily

observed and understood. The signs should be positioned at locations and in such numbers that all persons will be aware of the perimeters of these areas. Clearly designated and properly secured air operations areas will normally reduce the need for stringent security measures for the airport as a whole. Bilingual signs should be used where appropriate.

(b) Security of Air Operations Areas. Air Operations Areas should be secure to achieve the objectives of this program. The following measures are recommended:

1 Identify affected areas.
2 Post signs prohibiting unauthorized access.
3 Utilize natural or artificial barriers as necessary to prevent unauthorized entry.
4 Provide artificial lighting so as to sufficiently illuminate aircraft parking areas during the hours of darkness.
5 Secure or control doors, gates, and other openings in the perimeter of the air operations area to minimize the possibility of unauthorized entry.
6 Establish an effective locking and key control system.
7 Install anti-intrusion devices when appropriate.
8 Utilize guard or police services as necessary.
9 Install electronic or other type surveillance equipment.
10 Provide security communications system.

(c) Separation of Air Operations Areas. The air operations area should be separated from non-air operations areas by some medium that is visable and recognizable to the general public, such as a fence, barriers, or signs.

b. Identification of Persons. Under section 107.9 each airport operator after approval of his security program must require all persons authorized access to any air operations area (except as to access from a non-air operations area to an air operations area where both areas are adjacent and exclusively occupied or controlled by a certificate holder that is required to have a security program under § 121.538) to have identification on them when in that area. Procedures acceptable to the Administrator must be implemented after approval of the operator's security program.

(1) Identification System. Provisions for identification and control of all authorized persons should be included in a written document that includes the following criteria as applicable:

(a) Designated areas where identification is required.
(b) Type of identification media to be utilized and issuing authority.
(c) Procedure for checking identification of personnel.
(d) Details of where, when, and how identification media should be worn or carried.
(e) Disposition of lost or damaged media.
(f) Termination of access authorization (transfers, terminations or suspensions, etc.).
(g) Production and control of identification media.
(h) Designated points of entry to controlled areas.
(i) Job title of individuals who have authority to issue identification media and/or grant access to controlled areas. (These individuals should be strictly limited.)

In addition to providing for identification as required by section 107.9, it is recommended that appropriate limitations be placed on the bearer, such as escort privileges, areas of access, etc., and that procedures be established for escorting visitors whose identification media require an escort and for disciplining airport personnel who violate access controls.

(2) Identification Media Standards. Identification cards and badges should meet the following standards as a minimum:

(a) At least credit card size.
(b) Tamper-resistant (plastic or laminated equivalent).
(c) Wearable (by pouch, holder, chain or removable clip).
(d) Color photograph as an integral part of the card (photo should cover at least 50% of front of card).
(e) Individual's name.
(f) Individual's signature.
(g) Employer's name and/or insignia or emblem.
(h) Issuing authority's signature.
(i) Date of expiration.
(j) Height, weight, color of eyes and hair.
(k) Date of birth.
(l) Preprinted serial number on each identification card for accounting and security control purposes.
(m) All information except signatures should be typewritten; no erasures or alterations are permitted.

Identification cards should contain only a minimum of information on the front side so as to make it simple for guards and others to match the card with the person quickly. Usually, a photo, the individual's name and the employer's name or insignia is adequate. Color coding or other indications of access authority should also be displayed on the front of the card. The more detailed information should be contained on the reverse side where it can be reviewed as necessary.

(3) Accountability of Identification Cards. Identification cards and badges must be accounted for and safeguarded so as to prevent unauthorized persons from obtaining them. Inadequate control of active cards and blank forms can necessitate the complete reissuance of new cards. Airport operators will be expected to institute strick accountability procedures for all such cards and badges.

(4) Lost or Stolen Cards. Employees should be required to report the loss of a card or badge immediately to the issuing office. A "Stop List" of missing cards should be made available to responsible personnel. This list must be kept current in order to be effective.

c. Identification of Ground Vehicles. The numbers of ground vehicles permitted in the air operations areas should be held to a minimum consistent with operational needs. Vehicle control at airports can prevent or deter crimes against air transportation.

(1) Vehicle Identification Standards. All authorized vehicles should display visual identification in such a manner as to make them readily recognizable. Regularly assigned vehicles should normally have permanent type markings, either painted on or affixed by some other means insuring a similar degree of permanence. Company paint designs, insignias, and other such markings which are clearly visible would be acceptable. Other authorized vehicles should be provided with temporary identification such as a large decal, a magnetic numbered sign, or other conspicuous devices or markings. An exception to the display requirement is provided in section 107.11(b)(1) under which any "emergency vehicle when responding to an emergency situation while escorted by a vehicle, authorized by the airport operator, that has two-way contact with the control tower or established emergency control unit at that airport" need not display visual identification.

(2) Accountability and Control. The accountability and control of vehicular identification media should be consistent with the procedure as recommended for personnel identification cards and badges.

d. Fencing. Security fencing can vary in design, height and type depending on local security needs. Generally, however, the following standards are acceptable:

(1) Fencing of number 10 gauge, galvanized steel, chain link fabric, which is installed to a height of no less than eight feet and which is topped with a three stand (12 gauge) barbed wire overhand with a minimum of six inch separation between strands. The overhang installed at a forty-five degree angle from the horizontal and extending outward. Installation of a double apron barbed wire overhang, and fencing in excess of eight feet, is considered highly desirable when an area to be protected is located in a high risk area.

(2) Fence posts installed at ten foot intervals on-center.

(3) Top and bottom selvages of the fence having a twisted and barbed finish. The bottom of the fence installed to within two inches of hard surfacing or stabilized soil; however, in areas where unstable soil conditions are prevalent, the fabric installed to extend at least two inches below the surface or imbedded in concrete curbing.

(4) All fencing grounded. Care should be taken that metallic fencing is not installed when it will interfere with the operation of navigation aids.

(5) Where traverse culverts, troughs, or other openings larger than ninety-six square inches in the perimeter are unavoidable, the openings protected by fencing, iron grills, or other suitable barriers to preclude unauthorized access into the area. These barriers should be of materials at least equal in strength and durability to the fence and should be installed in a manner so as to deter unauthorized removal and not deter drainage.

(6) Fencing installed to within two inches of any wall that forms a part of the perimeter.

(7) If practical, where property lines, location of facility buildings, and adjacent structures permit, the fence located not less than fifty feet from any interior structures.

At least twenty feet clearance allowed between the perimeter fence and interior parking lots, or natural or aesthetic features. Such installations restrict ease of access and minimize the means of concealment in the immediate vicinity of the fence. Where property lines or other limiting factors restrict installation in accordance with these recommendations, the height of the fence should, therefore, be increased to compensate for these conditions.

(8) Clear zones can be provided around a facility through installation of perimeter fencing ten to twenty feet inside the property line. Care should be taken to insure that such a fence installation does not come closer than a minimum of twenty feet to interior structures and that prior to such an installation legal advice pertaining to local statutes with regard to retention of property rights is obtained. Local conditions will in most cases dictate the feasibility of such an installation.

(9) Fencing alarmed in areas considered as high risk areas in order to provide early warning of an attempt by an intruder to enter the area.

(10) Perimeter fencing should be inspected on a daily basis by the facility guard force or operational personnel at manned facilities.

e. Gates. The number of gates should be limited to the minimum required for the safe and efficient operation of the facility. Active perimeter entrances of manned sites should be designated in order to enable guard force personnel the opportunity to maintain full control without unnecessary delay in traffic or reduction of operational efficiency. This largely is a matter of having sufficient entrances to accomodate the peak flow of both pedestrian and vehicular traffic and adequate lighting for rapid inspection. Unmanned gates should be secured, illuminated during the hours of darkness and should be periodically inspected by guard or assigned operational personnel. Gates should be constructed of materials of equal strength and durability to the fence and should open to at least a ninety degree angle. Hinges of gates should be installed to preclude unauthorized removal. Gates should be topped with a barbed wire overhang meeting the specifications of that for the fence.

f. Security Lighting. Protective lighting provides a means of continuing, during the hours of darkness, a degree of protection approaching that which is maintained during daylight hours. (This safeguard also is a considerable deterrent to thieves, vandals and the potential saboteur.) These security lighting systems should be connected to an emergency power source if available. Requirements for protective lighting of airports will depend upon the local situation and the areas to be protected. A careful analysis of security lighting requirements should be made on the basis of needs for good visibility and based on the following criteria: employee recognition and badge identification, vehicle inspection, detection of intruders, deterrent to illegal entry, etc. Protective lighting is generally inexpensive to maintain and when properly employed, may provide guard force personnel with added protection from surprise by the determined intruder. Good protective lighting is achieved by adequate, even light upon bordering areas, glaring lights oriented towards avenue of approach of the potential intruder, and relatively little light on the guard personnel. Lighting units for perimeter fences should be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area on both the inside and the outside of the fence. Generally, the light band should illuminate the fence perimeter barrier and extend as deeply as possible into the approach area. Limiting factors on the orientation of lights and the depth of the light band may be as follows: airport operations and air safety requirements, residences, waterways, roadways, railroads, etc. Types of protective lighting systems and light sources include the following:

(1) Lighting Systems.

(a) Continuous Lighting. This is the most common protective lighting system. It consists of a series of fixed lights arranged to flood a given area with overlapping cores on a continuous basis during the hours of darkness. There are two methods of employment of this system:

1 Glare projection lighting where the glare of lights directed across surrounding territory will not be annoying or interfere with adjacent operations;

2 Controlled lighting is the restriction of the width of the lighted strip to meet a particular need. This method often illuminates or silhouettes the guards.

(b) Standby Lighting. Lights in this system are either automatically or manually turned on when an interruption of power occurs or when suspicious activity is detected.

(c) Movable Lighting. This type lighting consists of manually operated movable flood lights.

(d) Emergency Lighting. This system may duplicate anyone of the aforementioned systems. Its use is limited to periods of power failure or other emergencies and is dependent upon an alternate power source.

(2) Light Sources.

(a) Incandescent Lamps. These are common glass lights. Special purpose bulbs are manufactured with interior coatings designed to reflect the light, with built-in lens to direct or diffuse the light or equipped with a shade or fixture designed to accomplish similar results.

(b) Gaseous Discharge Lamps. These are mercury vapor and sodium vapor lamps. When cold these lights require from two to five minutes to illuminate and when hot they require a slightly longer period to relight after a power interruption.

g. Locks and Key Control. One of the basic safeguards used to protect personnel and property is the locking mechanism. Regardless of its quality or cost, however, a lock is nothing more than a delaying device and not a positive bar to entry. Many ingenious methods have been developed to open them surreptitiously. Some locks require considerable time and expert manipulation for covert opening but all will succomb to force and the proper tools. Further, many locking devices can be bypassed either because of poor construction of the lock, poor building construction, or improper installation.

(1) Key Control. Of primary importance in maintaining the integrity of a locking system is the establishment of effective key control. Such a system includes control of keys, key codes, key cutting and combination equipment, and key issuance and retrieval. Rigid controls should be established to insure that:

(a) Key cutting codes and equipment, if a system requiring such equipment is in effect, are protected against loss or misuse.

(b) Keys are issued to personnel on the basis of operational needs and not as a convenience.

(c) Keys are retrieved when personnel leave the airport by transfer, dismissal, resignation or death.

(d) Lost keys are reported promptly to the Security element.

(e) Unissued keys are properly safeguarded.

(2) Combination Locks. Combination padlocks having a fixed combination or other types of padlocks which have a changeable combination have inherent security weaknesses and can be damaged by weather.

(3) Cipher Locks. A variety of cipher (push button) locks are available. Inherent security weaknesses in the design of these locks, however, limit their use to controlling access in manned areas and should not be considered for use as security locks or at unmanned locations. Both electrical and mechanical cipher locks are available. Each can be used with electric release latches and doors utilizing this type of lock should be equipped with automatic door closers. The electrical cipher lock should also be equipped with a keyed bypass lock to allow access in the event of power failure.

(4) The key type padlock of brass construction with pin tumblers, and a hardened shackle are generally the most satisfactory for outside use.

(5) Locks are an integral part of barriers and their security. In addition to their physiological deterrence, their physical strength and resistance to all but the most determined thief, provides security in itself. Even then, the loss in time, and usual added noise will give increased probability of apprehension. It is essential that the manager of a facility and his security officer know each employee who has access to each lock. Key control is as important as the use of locks.

8. CRITICAL AREAS (OTHER THAN AIR OPERATIONAL AREAS). There are certain areas on airports other than air operations areas which should be given protection in the interest of aviation safety. These should also be considered in the development of an airport security program. Adequate safeguards which prevent or deter unauthorized access which could jeopardize aviation safety should be provided for baggage concourses, cargo storage areas, fuel systems, emergency fire and crash/rescue equipment sites, utilities buildings, water storage and supply areas, emergency generator locations, communications facilities and other areas.

9. LAW ENFORCEMENT AND THE AIRPORT. The nation's airports are vital to the economic, social and cultural health of the community. They are more than mere cogs in the transportation system. They require the same degree of knowledgeable and capable law enforcement personnel as any other public or private sector of the community. The community should be urged to have its appropriate law enforcement organization staffed and equipped to respond to the needs of the airport including those of the air carriers and other tenants. It is highly desirable to have regularly assigned law enforcement personnel at the airport in order to assure familiarity with the basic physical security concepts, security equipment, personnel and vehicular control procedures.

10. SECURITY EDUCATION. Personnel having responsibilities or interest in air operations or other critical areas also have security responsibilities. They should know what these are and understand what is expected of them. They should also have a good general knowledge of the airport security program and the purpose for it. The success of any program is dependent upon the performance of the participants. Well informed personnel are inevitably the best performers. Airport operators are encouraged to provide meaningful and regular security training for their personnel.

11. SECURITY COMMITTEES. Security committees, comprised of responsible individuals, is most desirable. These committees should be representative of all segments of the airport community to operate effectively. Meetings should be held regularly for the purpose of giving coordinated direction to the overall airport security program.

12. LIAISON. It is imperative that airport operators establish and maintain liaison with appropriate law enforcement agencies, both local and federal. These organizations can respond more promptly and better serve the airport operator when they are acquainted with airport facilities and requirements.

    FAA, Air Transportation Security Field Offices exist for the purpose of evaluating, coordinating, and assisting in the security activities of the aviation community. They also coordinate the activities of local, state, and federal government agencies as they relate to the prevention of aircraft hijackings, aircraft sabotage and other crimes affecting air transportation security. Additional information, guidance and assistance pertaining to airport security may be obtained from these offices.

13. AIRPORT SECURITY SURVEY. The purpose of an Airport Security Survey is to insure that a systematic in-depth inspection of the security posture of an airport is made in order to provide an accurate up-to-date evaluation of security requirements. It is recommended that a security survey be accomplished as a first step towards developing an Airport Security Program.

When conducting a security survey certain steps or considerations should be taken to insure that all security methods or hazards are inspected and recorded. In the case of the airport security survey you are trying to determine whether existing security measures will prevent or deter unauthorized access by persons or objects which would jeopardize aviation safety.

The areas where aircraft are located should be positively identified. Each protective measure that contributes to the security of the air operations area starting with those measures within the area and moving outward to the most distant protective measure reasonably associated with the air operations area should be examined and evaluated for effectiveness.

Placing yourself in the shoes of an intruder, work your way back to the air operations area. Examine each protective measure and identify any hazards to security, and consider ways to circumvent each measure. This process will identify effective security measures and indicate needs for new or different measures.

The airport operator should be involved in the accomplishment of a security survey, since all phases of operations and activity of the airport usually have to be considered. Airport operator also has the overall responsibility for assuring the development and implementation of an adequate security program. This program should be concerned with the prevention of aircraft piracy, sabotage, theft, vandalism, and other acts which could adversely affect aviation safety.

a. Airport Security Survey Checklist. A survey checklist is needed in conducting physical security surveys. It saves time, manpower and money and lessens the possibility of overlooking material factors. There is a list of questions enclosed with this circular which may be helpful in conducting security surveys.

APPENDIX 1. AIRPORT SECURITY SURVEY CHECKLIST

1. PERIMETER BARRIERS.

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

(1) Specify type and height of physical barrier.
(2) Describe condition of physical barriers.
(3) Is perimeter barrier considered to be a security safeguard?
(4) Is airport perimeter barrier set back 20 feet or more from airport property boundary?
(5) Is perimeter barrier under surveillance at all times?

b. If chain link fence is used as the perimeter barrier,

(1) Is it constructed of #11 gauge or heavier wire?
(2) Is mesh opening no larger than two inches square?
(3) Is selvage twisted and barbed at top and bottom?
(4) Is bottom of fence extended into the ground?

c. If masonry wall is used, is it at least seven feet high with a top guard of barbed wire or at least eight feet high with broken glass set on edge and cemented to top surface?

d. Do building walls, floors, or roofs form a part of the perimeter barrier?

(1) Are all openings properly secured?

NOTE: Openings, with an area of 96 square inches or greater, and located less than 18 feet above the level of the ground outside the perimeter barrier or less than 14 feet from controlled structures outside the perimeter barrier, should be provided with security equivalent to that of the perimeter.

e. If building forms a part of the perimeter barrier,

(1) Does it present a hazard at the point of juncture with the perimeter fence?
(2) Does it have any doors, windows, or other openings on perimeter side?

f. If a river, lake or other body of water forms any part of the perimeter boundary, are additional security measures provided?

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

h. Describe the physical characteristics of each perimeter entrance.

i. Are all entrance points in perimeter barriers guarded or secured?

j. Are all perimeter gates of such material and installation as to provide protection equivalent to the perimeter barriers of which they are a part?

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

l. Is the security officer responsible for security of keys to perimeter entrances?

m. Are keys to perimeter entrances issued to other than facility personnel such as contractor personnel?

n. Are all normally used pedestrian and vehicle gates and other perimeter entrances lighted so as to assure:

(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.

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

p. Are "No Trespassing" signs posted on or adjacent to perimeter barriers at such intervals that at least one sign is visible at any approach to the barrier for a minimum distance of 50 yards?

q. Are clear zones maintained on both sides of the perimeter barrier?

r. Are automobiles permitted to park against or close to perimeter barriers?

s. Are lumber, boxes, or other materials allowed to be stacked against,

or in close proximity to, perimeter barriers?

t. Do guards patrol perimeter areas?

u. Do guards observe and report insecure factors related to perimeter barriers?

v. Is an interior all-weather perimeter road provided for the use of guard patrol cars? If so, what is the condition?

w. Are perimeters protected by intrusion alarm devices?

2. PROTECTIVE LIGHTING.

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

b. Does protective lighting provide a means of continuing during the hours of darkness the same degree of protection available during the daylight hours?

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

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

e. Is perimeter lighting used so that guards remain in comparative darkness?

f. Are lights checked for proper operation prior to darkness?

g. Are repairs to lights and replacement of inoperative lamps effected immediately?

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

i. Is additional lighting provided at active gates and points of possible intrusion?

j. Are gate guard shacks provided with proper illumination?

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

l. Does the facility have a dependable source of power for its lighting system?

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

n. Is the protective lighting system independent of the general airport

lighting or power system?

o. Is the power supply for lights adequately protected?

p. Is there provision for standby or emergency lighting?

q. Is the standby or emergency equipment tested frequently?

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

s. Is wiring for protective lighting properly 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?

t. 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?

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

v. Are materials and equipment in shipping and storage areas properly arranged so as not to mask security lighting?

3. PROTECTIVE ALARMS.

a. If an alarm system is used in the facility, what detection device is used?

(1) Is it a local alarm system?
(2) Is it a central station system?
(a) Is it connected to facility guard headquarters?
(b) Is it connected directly to a headquarters outside the facility proper? Is it a private protection service? Police station? Fire station?

b. Is the system backed up by properly trained, alert guards?

c. Is the alarm system for active areas of structures turned off during operational hours?

d. Is the system tested prior to activating it from nonoperational periods?

e. Is the alarm system inspected regularly?

f. Is the system tamper-resistant? Weatherproof?

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

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

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

j. Are frequent tests conducted to determine the adequacy and promptness of response to alarm signals?

4. SECURITY COMMUNICATIONS.

a. Is there a security communications system?

b. What means of communications are used?

(1) Telephone.

(a) Is it a commercial switchboard system?
(b) Is it an independent switchboard?
(c) Is it restricted for guard use only?
(d) Are switchboards adequately guarded?
(e) Are call boxes conveniently located?
(f) Are open wires, terminal boxes, cables, etc., frequently inspected for damage, sabotage, and wire-tapping?

(2) Radio.

(a) Is an effective routine code being used? Duress code?
(b) Is proper authentication required?

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

d. Is the equipment in use sufficient for 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?

g. Is there more than one system of communications restricted to security use available for communicating with outside protective agencies?

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

5. PERSONNEL IDENTIFICATION AND CONTROL CHECK LIST.

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

b. Does the identification and control system include arrangements for the following:

(1) Protection of coded or printed components of badges and passes.
(2) Designation of the various areas requiring special control measures.
(3) Controlled issue of identification media.

c. Are there written procedures for the method of identification at time of entering and leaving controlled area, as applied to both employees and visitors?

(1) Details of where, when and how ID cards shall be carried.
(2) Procedures to be followed in case of loss or damage to identification media.
(3) Procedure for recovery and invalidation.

d. If a badge exchange system is used for any controlled area, does the system provide for:

(1) Comparison of badge, pass and personnel?
(2) Physical exchange of pass for badge at time of entrance and exit?
(3) Security of badges not in use?

e. Are personnel who are regularly required to enter areas of varying degrees of security interest provided with special identification?

f. Are personnel who require infrequent access to a critical area and who have not been issued regular security identification for such area treated as "visitors" thereto, and issued either

(1) a visitor's badge or pass?
(2) a special pass?

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

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

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

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

k. What are procedures relative to lost, damaged, and/or forgotten badges?

l. Are rosters of lost badges posted at guard control points?

m. 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?

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

o. What type of badges are issued to outside contractor employees working within the installation?

p. Are all phases of system under supervision and control of security officer?

q. Is there a visitor escort procedure established?

r. Do guards check on visitors' movements to assure that they do not enter areas for which they do not have the required authorization?

s. Are visitors required to conspicuously display identification on outer garments at all times while in controlled areas?

t. When visitors leave the installation, are they required to turn in their identification badges?

u. Is the departure time in each case recorded on the visitor's register?

v. Are visitors indicating an intention to return at a later time permitted to retain their identification badges.

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

x. Is there a central receptionist?

(1) If "yes," specify functions.

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

y. Are vendors, tradesmen, utility servicemen, special equipment servicemen, etc., issued a special or distinctive type of visitor badge?

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

aa. Is the airport security officer the responsible official for all aspects of visitor control?

6. VEHICLE IDENTIFICATION.

a. Is an effective procedure used for control 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.

b. Is there coordination between guard headquarters and the activities that handle cargo movements?

c. Is a regular security education program in effect?

7. VEHICLE CONTROL.

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

b. Have definite procedures been established for the registration of private cars?

c. Do the vehicle registration provisions apply also to motor vehicles owned or operated by: employees of any individual firm, corporation, or contractor engaged in activities on the airport and individuals, partnerships or other business concerns whose business activities require daily or frequent use of their vehicles on the airport?

d. Is annual registration provided for?

e. Are decalcomania or other registration tags affixed to all registered vehicles?

f. Do the controls for registration tags include:

(1) Prohibition against transfer of registration tags for use with a vehicle other than the one for which originally issued?
(2) Replacement of lost tags at the registrant's expense?
(3) Return of tags to the airport security officer when vehicle is no longer authorized entry into facility?
(4) Destruction of invalidated decalcomania?
(5) Is security section notified when employee leaves for over 30 days?

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

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

i. Is a definite system used to control the movement of commercial trucks and other goods conveyances into and out of the air operations area?

j. Are loading and unloading platforms located outside the air operations area and separated therefrom by controlled and guard supervised entrances?

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

l. If trucks are permitted direct access to the air operations area, are truck drivers and vehicle contents carefully examined?

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

n. Are truck registers maintained?

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

p. 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?

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

r. Are automobiles allowed to be parked within the air operations area?

s. Are parking lots provided?

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

u. Are interior parking areas fenced so that occupants of automobiles

must pass through a pedestrian gate when entering or leaving the working area?

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

w. What is extent of guard surveillance over interior parking area?

x. Are there restrictions against employees entering parking areas during duty hours?

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

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

aa. Are parking facilities adequate?

8. LOCK SECURITY.

a. Has a key control official been appointed, normally airport security officer?

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

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

d. Are keys issued only to authorized personnel?

e. Are keys issued to other than airport personnel?

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

g. Are keys not in use maintained indicating:

(1) Buildings and/or entrances for which keys are issued?
(2) Number and identification of keys issued?
(3) Location and number of master keys?
(4) Location and number of duplicate keys?
(5) Issue and turn in of keys?
(6) Location of locks and keys held in reserve?

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

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

k. Are losses or thefs of keys promptly investigated by the key control

personnel?

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

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

n. Are padlocks rotated within the installation at least semiannually?

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

9. GUARD FORCES.

a. Is a guard force provided?

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

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

d. Is use of guard forces reviewed periodically to ascertain effective and economical use?

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

f. Is a guard headquarters area provided?

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

h. Are guards familiar with communications equipment used?

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

j. Are guards armed while on duty, and if so, with what type of weapon?

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

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

m. Is each member of guard force required to complete a course of basic training?

n. Are the subjects included in the various training course adequate?

Does the training cover:

(1) Care and use of weapons?
(2) Common forms of pilferage, theft, and sabotage activity?
(3) Types of bombs and explosives?
(4) Orientation on the facility emphasis of controlled and vulnerable areas?
(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 arrest or apprehend?

o. Are activities of the guard force consonant with established policy?

p. Is supervision of the guard force adequate?

q. Are general and special orders properly posted?

r. Are guard orders reviewed periodically to insure applicability?

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

t. Do physical, functional, or other changes at the airport indicate the necessity for or feasibility of

(1) Establishing additional guard posts?
(2) Discontinuing any existing posts or patrols?

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

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