7. AC 150/5300-13, Section 6, paragraph 614

614. PHYSICAL SECURITY. Airport facilities require protection from acts of vandalism. To provide a measure of protection, unauthorized persons must be precluded from having access to NAVAIDs and ATC facilities. Perimeter fencing should be installed to preclude inadvertent entry of people or animals onto the airport. In addition to airport perimeter fencing, the following security measures are recommended:

a. Off-Airport Facilities. Navigational and ATC facilities located off an airport, and in a location that is accessible to animals or the public, shall have a security perimeter fence installed at the time of construction.

b. On-Airport Facilities. Navigational and ATC facilities located on the airport have at least the protection of the operational areas. Any protection device, e.g., a guard rail or security fence, which penetrates an FAR Part 77 surface is an obstruction to air navigation. As such, it is presumed to be a hazard to air navigation until an FAA study determines otherwise.

615. CABLE PROTECTION. Most NAVAID and ATC facilities discussed in this chapter are served by buried power and control cables. FAA cables are typically buried approximately 24 inches (.6 m) below ground. They should be installed in conduit or duct beneath runways and taxiways, and in duct and manhole systems under aprons and paved parking areas. Information regarding the location of FAA cables and ducts may be obtained from the Manager of the Airways Facilities Maintenance Office serving the NAVAID or ATC facility. Questions relative to protecting or relocating cables can be obtained from the FAA Regional Airways Facilities Division Office.

616. to 699. RESERVED

8. AC 150/5300-13, Section 8

803. SHOULDERS AND BLAST PADS. Unprotected soils adjacent to runways and taxiways are susceptible to erosion. A dense, well-rooted turf cover can prevent erosion and support the occasional passage of aircraft, maintenance equipment, or emergency equipment under dry conditions. Paved shoulders are recommended for runways, taxiways, and aprons which will accommodate Group III and higher aircraft. Turf, aggregate-turf, soil cement, lime or bituminous stabilized soil are recommended adjacent to paved surfaces provided for Group I and II aircraft.

a. Shoulder and Blast Pad Dimensions. Paved shoulders should run the full length of the runway(s) and taxiway(s). Blast pads at runway ends should extend across the full width of the runway plus the shoulders. Table 3-1, 3-2, and 3-3 specify the standard blast pad dimensions and runway shoulder widths. Table 4-1 specifies the standard taxiway shoulder widths. Increases to these standard dimensions are permissible for unusual local conditions.

b. Pavement Strength. Shoulder and blast pad pavement needs to support the occasional passage of the most demanding airplane as well as the heaviest existing or future emergency or maintenance vehicle for the design life of the full strength pavement. These pavements may be constructed of bituminous or Portland Cement concrete materials. Specifications for materials and constructions standards for these pavements should be based on state highway requirements.

(1) For Airplane Design Groups III and IV, the minimum bituminous concrete surface thickness, constructed on an aggregate base, is 2 inches (51 mm) for shoulders and 3 inches (76 mm) for blast pads. These thicknesses should be increased by 1 inch (25 mm) for Airplane Design Groups V and VI. Aggregate base and subbase thicknesses should be determined using state highway design standards.

(2) The thickness of shoulders and blast pads constructed of Portland Cement concrete should be based on state highway standards. The minimum thickness of these pavements, as recommended in AC 150/5320-6, is 5 inches (127 mm).

(3) Shoulders and blast pads may have stabilized subbase and base. The stabilized subbase and base thicknesses should be determined using the equivalency factors in AC 150/5320-6 for converting aggregate subbase and base to stabilized subbase and base.

c. Drainage. Surface drainage should be maintained or improved in the shoulder and blast pad areas. Where a paved shoulder or blast pad abuts the runway, the joint should be flush, however, the shoulder may retain a 5 percent transverse slope. A 1.5 inch (3.8 cm) step is the standard at the edge of paved shoulders and blast pads to enhance drainage and to prevent fine graded debris from accumulating on the pavement. Base and subbase courses shall be of sufficient depth to maintain the drainage properties of granular base or subbase courses under the runway, taxiway, or apron pavement. An alternative is to provide a subdrain system with sufficient manholes to permit observation and flushing of the system.

d. Marking and Lighting. AC 150/5340-1 provides guidance for marking shoulders and blast pads. New construction should provide for edge lights to be base mounted and for the installation of any cable under the shoulder or blast pad pavement to be in conduit. When adding shoulders or blast pads to existing runways or taxiways, the existing runway or taxiway edge lighting circuitry, if not suitable, should be updated/modified prior to shoulder or blast pad paving.

9. AC 150/5300-13, Table A16-1A, Appendix 16

## Table A16-1A. Precision Instrument Approach Requirements.

| | | |
|---|---|---|
| **Visibility Minimums**[1] | <3/4 statute mile | < 1-statute mile |
| **Height Above Touchdown (HAT)**[2] | 200 | |
| **TERPS Glidepath Qualification Surface (GQS)**[3] | Table A2-1, Row 7, Criteria, and Appendix 2, par. 5a Clear | |
| **TERPS precision "W" surfaces** [4] | Clear | See Note 5 |
| **TERPS Paragraph 251** | 34:1 Clear | 20:1 Clear |
| **Precision Obstacle Free Zone (POFZ) 200 x 800**[6] | Required | Not Required |
| **Airport Layout Plan**[7] | Required | |
| **Minimum Runway Length** | 4,200 ft (1,280 m) (Paved) | |
| **Runway Markings (See AC 150/5340-1)** | Precision | Nonprecision |
| **Holding Position Signs & Markings (See AC 150/5340-1 and AC 150/5340-18)** | Precision | Nonprecision |
| **Runway Edge Lights**[8] | HIRL / MIRL | |
| **Parallel Taxiway** [9] | Required | |
| **Approach Lights**[10] | MALSR, SSALR, or ALSF | Recommended |
| **Runway Design Standards; e.g., Obstacle Free Zone (OFZ)** [11] | < 3/4-statute mile approach visibility minimums | ≥ 3/4-statute mile approach visibility minimums |
| **Threshold Siting Criteria To Be Met** [12] | Table A2-1, Row 9, Criteria | Table A2-1, Row 8, Criteria |
| **Survey Required for Lowest Minima** | Vertically Guided Airport Airspace Analysis Survey | |

1. Visibility minimums are subject to application of FAA Order 8260.3 (TERPS) and associated orders or this table, whichever are higher.
2. The HAT indicated is for planning purposes only. Actual obtainable HAT is determined by TERPS.
3. The GQS is applicable to approach procedures providing vertical path guidance. It limits the magnitude of penetration of the obstruction clearance surfaces overlying the final approach course. The intent is to provide a descent path from DA to landing free of obstructions that could destabilize the established glidepath angle. The GQS is centered on a course from the DA point to the runway threshold. Its width is equal to the precision "W" surface at DA, and tapers uniformly to a width 100 feet from the runway edges. If the GQS is penetrated, vertical guidance instrument approach procedures (ILS/MLS/WAAS/LAAS/Baro-VNAV) are not authorized
4. The "W" surface is applicable to precision approach procedures. It is a sloping obstruction clearance surface (OCS) overlying the final approach course centerline. The surface slope varies with glidepath angle. The "W" surface must be clear to achieve lowest precision minimums. Surface slope varies with glide path angle, 102/angle; e.g., for optimum 3° glide path 34:1 surface must be clear.
5. If the W surface is penetrated, HAT and visibility will be increased as required by TERPS.
6. This is a new airport surface (see paragraph 306).
7. An ALP is only required for airports in the NPIAS; it is recommended for all others.
8. Runway edge lighting is required for night minimums. High intensity lights are required for RVR-based minimums.
9. A parallel taxiway must lead to the threshold and, with airplanes on centerline, keep the airplanes outside the OFZ.
10. To achieve lower visibility minimums based on credit for lighting, a TERPS specified approach light system is required.
11. Indicates what chart should be followed in the related chapters of this document.
12. Circling procedures to a secondary runway from the primary approach will not be authorized when the secondary runway does not meet threshold siting (reference Appendix 2), OFZ (reference paragraph 306) criteria, and TERPS Order paragraph 251 criteria.

10. DOT/FAA/AR-04/10, Section 4

## 4. CONCLUSIONS.

Increasing the size of the markers from 96 square inches to 200 square inches would provide only a slight improvement over the standard marker for most aircraft types, and even less of an increase in effectiveness for aircraft having the less advantageous wing taxi lamp placement.

For aircraft that have the taxi lamps located immediately in line with the pilot's eye, the standard 96-square-inch markers are effective and adequate. The majority of smaller aircraft, the principal users of unlighted airports, do have this central taxi lamp placement. For those aircraft having wing-mounted taxi lamps, markers of any size provide marginal guidance at best, and the pilots must primarily rely on painted surface markings. As an aircraft moves closer to the marker, the aircraft taxi lamp passes the main marker and the reduction in marker effectiveness is even more pronounced. The brightness of the standard 96-square-inch marker is decreased to approximately 40 to 50 percent when the taxi lamp is located to the side by as little as 5 feet. Locating the lamp even further away from the pilot's eye, 15 feet right of center, as in a Learjet 25 (not evaluated) wing tip tank location, decreased the returned light to only 10 to 30 percent.

In general, the acquisition ranges were found to be the following.

- 96 square inches of blue type III grade retro-reflective sheeting for cylindrical markers was seen at a distance of 500 feet away.

- 200 square inches of blue type IX grade retro-reflective sheeting for cylindrical markers was seen at a distance of 700 feet away.

- 96 square inches of white type III grade retro-reflective sheeting for cylindrical markers was seen at a distance of 400 feet away.

- 200 square inches of white type IX grade retro-reflective sheeting for cylindrical markers was seen at a distance of 500 feet away.

The range of the blue taxiway markers is from 500 to 700 feet, whereas the range for the white runway markers is 400 to 500 feet. It would appear that the blue taxiway markers, having a retro-reflectivity high enough to be seen at a minimum distance of 300 feet, provided adequate taxi guidance. To be effective at much higher rollout speeds, the white runway markers will need to have acquisition ranges of 800 to 1000 feet, considerably greater than the ranges provided by the white markers evaluated in this test.

11. Order 6940.1

# ORDER

**DEPARTMENT OF TRANSPORTATION**
**FEDERAL AVIATION ADMINISTRATION**

6940.1

1/13/70

SUBJ: ACCESS ROADS TO FAA OWNED AND OPERATED FACILITIES

1. PURPOSE. This Order sets forth the requirement for establishing access roads to FAA owned and operated facilities, both on or off airports, and specific pavement requirements for these roads (existing or new) when they join runways and taxiways on airports.

2. CANCELLATIONS. None.

3. REQUIREMENT. Access roads with turn around areas shall be provided to all FAA facilities or installations where a road is considered to be the best means of ingress and egress. Determination of need shall be based on frequency of use, travel time, and comparative costs.

   Where these access roads are on airports and intersect or terminate at paved runways and/or taxiways, the initial 300-feet adjacent to the runway or taxiway shall be paved. It is desirable to keep to the minimum access roads which would be within the runway primary surface as defined in FAR Part 77. At no time shall an access road be constructed parallel to a runway closer than 200-feet edge to edge and 100-feet edge to edge when parallel to a taxiway. Final siting and layout of these access roads on airports shall be coordinated with the Chief, Airports Branch of the local FAA area office.

4. IMPLEMENTATION

   A. Construction.

      (1) The practicability of construction of an access road shall be determined by the regional director.

      (2) All roads shall be of the most economical type that will provide satisfactory and safe transportation of personnel, equipment, and material in the types of weather and climatic conditions normally encountered at the location. They shall be constructed in accordance with Specification FAA-C-95, "Construction of Driveway," modified to meet local requirements. Where paving is required, the pavement shall be asphalt or portland cement concrete in accordance with AC-150/5370-1A, Standard Specifications for Construction of Airports. In the areas of high snowfall, turn around areas shall be of sufficient size to accommodate supply support vehicles and snow removal equipment.

30762

**Distribution:** WAT/FS/LG/RD/BU-2; WAS/SM-3; RAT/FS-2; RAS/AF-3; MAT/AF/AS/FS-2; N-2

~~AOR-400~~
ATC Facilities

B. Funding.

(1) Funding for the initial installation of access roads or relocation, replacement, modification, or improvement of existing access roads shall be in accordance with Order 2500.8, "Operations vs F&E Funding." Funds to accomplish initial installation or relocation, replacement, or modification shall be requested through the normal budgetary process.

(2) On airports where facilities must be relocated, replaced, or modified, because of improvements or changes to the airport, access roads are considered as part of these facilities and funding for their construction shall be in accordance with FAA Order 6030.1.

(3) FAA should enter into an agreement with the responsible party for reimbursement of the cost of relocation or replacement of access roads to facilities located off airports, which is caused by highway relocations, installation of power lines, etc.

(4) Funds for maintaining access roads to these facilities shall be included in the operations budget. Where access roads or facilities are jointly used, a maintenance agreement should be negotiated with the joint user on a reimbursable basis.

C. Maintenance.

Access roads shall be maintained in accordance with FAA Handbook AF P 6940.7, "Maintenance of Roads."

Joe D. Conerly
for John A. Weber, Director
Systems Research and
Development Service

12. TSA Guidelines, Part III, Section A, June 2006

# Recommended Security Guidelines for Airport Planning, Design and Construction

Revised June 15, 2006

Transportation Security Administration

# PART III

# RECOMMENDED GUIDELINES

## Section A - Airport Layout and Boundaries

The first step in the integration of security into airport planning, design or major renovation is the analysis and determination of the airport's general security requirements, layout and boundaries. These decisions are critical to the efficient, safe and secure operation of an airport. While existing airports may not have great leeway in redesigning the general layout, adjustments to the location of access roads or types of boundaries for security areas may be beneficial and integrated into adjacent construction projects. Periodic review of an airport's boundary system and locations is recommended to assure that the airport's needs are met, particularly since aviation security requirements and surrounding environments may frequently change.

### 1. General Airport Layout

The general layout of an airport consists of three (3) areas generally referred to in the industry as Airside, Landside, and Terminal. While the terminal area generally lies on the boundary of the airside and landside (as may other buildings), due to the nature of its use and the special requirements that apply to airport terminals, it is best treated for security purposes as a distinct area.

Each major area of the airport (airside, landside, terminal) has its own special requirements. Airside/landside requirements and operational parameters should be carefully considered when planning and designing a new airport or facility. The requirements, barrier and boundary measures that delineate airside from landside, may have major effects on the facility's efficiency, employee and public accessibility, and overall aesthetics.

Maintaining the integrity of airside/landside boundaries plays a critical role in reducing unauthorized access to, attacks on, or the introduction of dangerous devices aboard, passenger aircraft. Effective airside security relies heavily on the integrated application of physical barriers, identification and access control systems, surveillance or detection equipment, the implementation of security procedures, and efficient use of resources.

a. *Airside*

The airside of an airport is the movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is controlled. Typically, the airside is beyond the security screening stations and restricting perimeters (fencing, walls or other boundaries) and includes runways, taxiways, aprons, aircraft parking and staging areas and most facilities which service and maintain aircraft. For operational, geographic, safety, or security reasons, other facilities such as tenant and cargo facilities may be located within the airside as well.

As the airside generally includes security areas to which certain requirements apply under 49 CFR 1542; e.g., the Aircraft Operations Area (AOA), Security Identification Display Area (SIDA) and Secured Areas, the airside, by nature, must be nonpublic. Further information on these security requirements is contained in *Security Areas* on page 15.

The choice as to where this airside perimeter fencing or barrier may be located is often subject to the surrounding environment and access roads and may be one of the most critical decisions in designing or renovating an airport. In addition to the factors discussed in *Facilities, Areas and Geographical Placement* on page 41, the following factors should be considered when determining airside boundaries and orientation:

1) Dangerous or hazardous areas that could affect the safety or security of a parked or moving aircraft;

2) Concealed/overgrown areas that could hide persons or objects that might endanger aircraft or critical airport systems;

3) Adjacent facilities having their own security concerns and provisions, e.g., correctional, military or other facilities that could affect or be affected by the proximity of airside operations;

4) Natural features, large metal structures/buildings or electronics facilities that might affect ground or aircraft communications or navigational systems; (Reduced or limited communications can endanger not only aircraft and airport personnel safety, but also limit security response capabilities and information availability during emergency as well as routine situations.)

5) Adjacent schools, hotels, parks or community facilities that might affect or be affected by the proximity of aircraft and the related safety and security concerns. (While safety concerns exist, the increased possibility of airside penetrations and/or vandalism is a security concern.)

For an airport to obtain the certification required for operations, the airside must be able to maintain required operational clear areas, have adequate emergency response routes and response times, and have in place required safety measures.

b. *Landside*

Excluding terminals, which are treated separately below, the landside of an airport is that area of an airport and buildings to which both traveling passengers and the non-traveling public have unrestricted access. Typically, the landside facilities include patron and other public parking areas, public access roadways, rental car facilities, taxi and ground transportation staging areas, and any on-airport hotel facilities.

Since the landside includes all non-airside areas (other than the terminal(s)), its location is determined by the airside and perimeter boundary. Within landside, factors affecting the location of facilities are discussed in *Facilities, Areas and Geographical Placement* on page 41

Since the landside is not directly affected by the operation of aircraft, it generally has less stringent security requirements than the airside. However, some clear area and communication requirements may still affect landside design and layout, such as an airside fence/boundary, aircraft approach glide slopes, communications and navigational equipment locations and non-interference areas, and heightened security in the terminal area. Further information on these requirements is contained in *Security Areas* on page 15.

The landside in general must meet the local jurisdictional standards for public safety and security, which may result in special safety requirements that will interface with the airport's overall security and fire safety system.

c. Terminal

An airport terminal is a building or buildings designed to accommodate the enplaning and deplaning activities of aircraft operator passengers. Larger airports or those with general aviation areas often have more than one terminal. For purposes of this document, the term "terminal" typically refers to that main building or group of buildings where the boarding of public, scheduled commercial aircraft occurs or from which persons who have passed through a security screening process will proceed to boarding facilities located elsewhere on the airside.

When considering passenger and baggage screening security provisions, it is important for planners and designers to distinguish the commercial terminal from the general aviation terminal where charter and private passenger activity typically occur. However, it is also important to note that security requirements may affect charter and private aviation as well as scheduled commercial aviation. Planners and designers are encouraged to discuss security considerations with the FSD when developing charter or private aviation facilities as well as when developing facilities intended for use by scheduled commercial air carriers or aircraft operators. .

The terminal is typically the area of the airport with the most security, safety, and operational requirements. Many of these requirements are closely linked to the location of *security areas* within, and in close proximity to, the terminal. Since the terminal usually straddles the boundary between airside and landside, certain portions must meet the requirements of both of these areas.

When designing a new facility, the terminal should be centrally located on the airport site when possible. This not only provides for efficient aircraft access to most runways and facilities, but can benefit terminal security as well. A centralized terminal buffers the terminal from outside-airport threats and security risks due to distance. A fundamental concept in security planning, "distance," provides the flexibility for the airport operator to put in place systems, measures or procedures to detect, delay, and respond (DDR) to

unauthorized penetration. Providing additional "standoff" distance from a potential Large Vehicle Improvised Explosive Device (LVIED) is highly beneficial when addressing blast protection measures. A centralized terminal can also minimize the communications interference that might be caused by adjacent, non-airport facilities.

**Section III-A-1 - Airport Layout and Boundaries Checklist:**

- ☐ **Analysis of General Security Requirements**
- ☐ **Security & Safety Considerations**
  - Separate dangerous or hazardous areas
  - Minimize concealed/overgrown areas
  - Effects on/by adjacent facilities
  - Natural features that might allow access
  - Prevent communications interference due to natural features, buildings & equipment
  - Public safety & security concerns
  - Criminal Activity

**Airside**
- Nonpublic
- Maintain airside/landside boundaries
- Maintain security clear areas and zones
- Adequate emergency response routes
- Required safety measures & clearances

- ☐ **Landside**
  - Public safety & security
  - Maintain airside/landside boundaries
  - Maintain security clear zones
  - Deter criminal activity
- ☐ **Terminal**
  - Maintain public/nonpublic boundaries
  - Maintain security area boundaries
  - Meet security regulations
  - Personnel security & safety
  - Public security & safety

2. *Security Areas* (Refer also to *Figure II-C-1* on page 9)

The Airport Security Program (ASP) required under 49 CFR 1542.101 contains specific descriptions of the following areas in which security measures are specified in 49 CFR 1540.

a. Air Operations Area (AOA)

An AOA is a portion of an airport, specified in the ASP, in which security measures specified in 49 CFR 1542 are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas, for use by aircraft regulated under 49 CFR 1544 and 49 CFR 1546, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the secured area.

The airport operator is required to control and prevent access to the AOA; control movement within the AOA; and control unauthorized penetrations of the AOA. TSA regulations do not specify how to accomplish this, but rather, leaves the solution to the local authorities, subject to TSA approval.

In most cases, it is advantageous to align the AOA boundary with other boundaries or with physical barriers. Typically, the AOA is a major portion of the area within the fence or other barrier that defines the airside/landside boundary of the airport. Exceptions to this may occur when electronic barriers or natural barriers such as rivers are being used to delineate boundaries. The AOA is required to have a distinct, securable boundary line. Refer to *Boundaries* on page 22 for more information.

When allocating AOA space, and since the AOA requires less specific security measures than SIDAs or secured areas, consider whether to locate construction staging areas, in-flight kitchens, commissaries, and other facilities outside those critical areas within the AOA. This will facilitate implementation and may reduce the cost of access control and identification system measures for such areas. Locating most non-terminal areas outside of the SIDA may also reduce the amount of man-hours needed for identification media issuance and revalidation, background checks, and security training. Further discussion on *Facilities, Areas and Geographical Placement* is included on page 41.

b. Security Identification Display Area (SIDA)

A SIDA is a portion of an airport, specified in the ASP, in which security measures specified in 49 CFR 1542 are carried out. This area includes the secured area and may include other areas of the airport. Generally, the SIDA is an area requiring display of an authorized identification media.

The airport operator has the responsibility to secure SIDAs and prevent or respond immediately to access by unauthorized persons and vehicles. SIDAs may lie within AOAs; a secured area is by definition always a SIDA, in that all SIDA requirements within 49 CFR 1542.205 must be met within a secured area.

In general, SIDA layouts should be held to the smallest manageable size to provide the level of protection sought for the area or facility. The SIDA is the area that requires the greatest continuous procedural attention from employees. The number of SIDA access points should be limited to the minimum necessary for operational practicality.

c. Secured Area

A Secured Area is a portion of an airport, specified in the ASP, in which certain security measures specified in 49 CFR 1542 are carried out. This area is where aircraft operators and foreign air carriers, that have a security program under 49 CFR 1544 or 1546, enplane, deplane passengers and sort and load baggage, and any adjacent areas that are not separated by adequate security measures.

Each secured area must independently meet all the requirements placed upon it by the ASP, including control of access, challenge procedures, law enforcement officer (LEO) response, display of ID, etc., particularly where the various secured areas may not enjoy common boundaries or access points. A secured area is by definition always a SIDA, in that all SIDA requirements within 49 CFR 1542.205 must be met within a secured area.

Although the secured area generally includes portions of the landside and terminal, it is desirable to locate secured areas contiguously or as close together as possible to maximize access by response personnel, utilize common areas of closed circuit television (CCTV) surveillance coverage, and minimize requirements for redundant boundaries and electronic access controls. Where there are several unconnected secured areas - baggage makeup areas, movement areas, safety areas, etc. - each may require separate but integrated electronic controls.

d. Sterile Area

A Sterile Area is a portion of an airport, specified in the airport security program that provides passengers access to boarding aircraft and to which access generally is controlled by TSA, or by an aircraft operator under 49 CFR 1544 or a foreign air carrier under 49 CFR 1546, through the screening of persons and property.

TSA, the aircraft operator, or designated foreign air carrier must use adequate facilities and procedures to screen persons and property prior to entry into the Sterile Area to prevent or deter the carriage aboard aircraft of any explosive, incendiary, or deadly or dangerous weapon on or about each individual's person or accessible property. In addition, the aircraft operator must prevent or deter the carriage of any explosive or incendiary in any checked baggage brought into the sterile area.

Sterile areas require physical, financial and manpower resources dedicated to providing screening. These should be held to an operational minimum so that appropriate surveillance and control resources can be concentrated where necessary, rather than scattered among less security-related areas. Sterile areas may include various revenue-generating facilities, particularly concessions, which may be impacted by periods of heightened threat. Designers and planners should allow flexibility within sterile areas such that added security measures during times of heightened alert will have the least possible negative impact.

e. Exclusive Area

An Exclusive Area is any portion of a secured area, AOA, or SIDA, including individual access points, for which an aircraft operator or foreign air carrier that has a security program under 49 CFR 1544 or 49 CFR 1546 has assumed responsibility under 49 CFR 1542.111.

Within the Exclusive Area, the responsible signatory aircraft operator or designated foreign air carrier must perform security control requirements described in the exclusive area agreement. The aircraft operator, not the airport, may control access and movement within the Exclusive Area.

Specific requirements and conditions must appear in the exclusive area agreement, which is approved by TSA. Such conditions include a delineation of very specific areas for which the aircraft operator assumes

security responsibilities. Like SIDAs and Sterile Areas, Exclusive Areas should be held to an operational minimum so that appropriate surveillance and control resources can be concentrated where necessary, rather than scattered among less security-related areas.

f. Airport Tenant Security Program (ATSP) Area

An ATSP Area is an area specified in an agreement between the airport operator and an airport tenant that specifies the measures by which the tenant will perform specified security functions, authorized by the TSA, under 49 CFR 1542.113.

Subject to a tenant-area-specific security program approved by TSA, the airport tenant has responsibility for specific security systems, measures or procedures.

Where tenants other than air carriers elect to undertake under their own security programs 49 CFR 1542, such areas should be limited to the tenants' immediate boundaries and sphere of influence, and should accommodate security requirements for contiguous boundaries with other tenants and/or the airport and airlines.

**Section III-A-2- Security Areas Checklist:**

- ☐ **AOA**
  - Align AOA boundary with fences or natural boundaries
- ☐ **SIDA**
  - Part of AOA
  - Smallest manageable contiguous size(s)
- ☐ **Secured Area**
  - Consider general aviation, cargo, maintenance, and other facilities in a manner consistent with latest TSA regulation and policy guidance.
- ☐ **Sterile Area**
  - Minimize size to help surveillance and control
- ☐ **Exclusive Area**
  - Minimize areas to be monitored/controlled
- ☐ **ATSP Areas**
  - Minimize areas to be monitored/controlled

**3. Assessment of Vulnerable Areas**

a. Basic concepts of security risk management dictate that the security system provide the appropriate level of security to all of the assets to be protected, in light of the perceived threat to those assets. Therefore, at the facility planning stage it is prudent to consider all of the assets (or targets of a terrorist or criminal attack), considering their relative "value" (or consequence of loss) and economical impact. There are many possible high value assets at an airport to consider, such as: aircraft (with or without passengers aboard); air traffic support facilities (tower, radar, weather, communications); terminal building(s), groups of members of the public or employees; fuel storage; critical infrastructure (power, water, communications) and railway, roadway or vehicle access way and surrounding waterways/intermodal transportation facilities.

b. One of the fundamental concepts for airport security is the establishment of a boundary between the public areas and the areas controlled for security purposes (such as the AOA, Secured Areas, SIDA, ATSP Areas and Exclusive Areas). Since barriers and controls are required to differentiate these areas and to limit access to them, this may lead to the assumption that anyone or anything found in the area is authorized. This suggests a common vulnerability; once inside the controlled area, an intruder may move about without encountering additional controls. For example, if an intruder breaches the fence line (considered to be easily and quickly achieved), he may find no further physical barriers to control access to aircraft, the baggage makeup area (BMA), maintenance facilities, and other areas. Security measures often employed to mitigate this situation include challenge procedures augmented by ramp patrols, electronic monitoring (such as by CCTV), personnel surveillance, ground radar or intrusion detection sensors, and others, all of which have planning and design implications.

c. Other means of achieving unauthorized access exist, such as through reverse use or other misuse of emergency exits (for example, from public side to the secured area) or unauthorized use of a controlled access portal opened by an authorized user, a practice often called "piggybacking." New construction designs should minimize the number of emergency exits that lead to the secured area from public areas.

Some fire codes allow the use of delayed egress hardware on emergency exit doors. Where authorized for use by fire or building code officials, delayed egress hardware should be considered for use as a deterrent to discourage unauthorized, non-emergency use of emergency exit doors. Where necessary, these doors should be supported by comprehensive surveillance (such as CCTV) on both sides of the door for alarm assessment. Ideally the airside surveillance would include an intruder tracking capability to allow for directing the response force. Attentive planning and incorporation of appropriate surveillance or control devices can significantly improve the identification and control of piggybacking, as well as the deployment and efficient use of manpower resources to respond to anomalies. Contact the airport security coordinator and local FSD for current sensor evaluation (pilot program) reports that may be applicable at a particular airport.

d. Another area of concern is unauthorized entry or breach in the sterile area. Any open boundary between the public area and the sterile area is a candidate for such a breach. Typically, the breach will occur either through the passenger security screening checkpoint or via the exit lane (bypassing the security checkpoint). From the planning and design standpoint, the most significant considerations for implementing a physical breach control system are: 1) source and location of breach identification alarm generator; 2) location of physical barriers which respond to the breach alarm; and 3) sufficient separation distance between 1 & 2 to allow safe and sure closure prior to intruder's further penetration which could result in terminal evacuation. Other concerns such as fire and safety codes must also be considered.

e. All public access facilities, within which large congregations of people are customary, suffer from a fundamental vulnerability to terrorist bombing or armed attack. Considering blast mitigation at the planning and design stage can reduce this vulnerability significantly. For the threat of large vehicle bombs, the primary blast mitigating consideration is separation distance. This consideration runs counter to the passenger convenience consideration of minimized transit distances. [Refer to charts in *Appendix C*]. Innovative designs that satisfy both passenger convenience and separation distance for blast mitigation should be sought, including potential facility design to minimize large congregations of people close to points of vehicle access or drop-off, or to redirect or otherwise mitigate blast effects.

f. The threat of an armed attack on the terminal as well as the threat of an abandoned article containing an explosive device raises attention to another form of vulnerability. As long as there is a "public side" within the terminal, where congregations are expected, there are limited means by which a security system can prevent an attack. To assure that LVIEDs, IEDs, or terrorists with weapons do not enter the terminal requires moving the point of screening "to the front door." Here again, architects and designers may seek innovative designs that can accommodate all of the passenger convenience issues, as well as accommodating screening of all people and items before entering the terminal (creating a "sterile terminal"), to significantly reduce this vulnerability. Many other issues that may not be readily apparent require that a "front door" option be carefully considered in close coordination with aircraft operators, the airport authority, and the local FSD.

g. A potential vulnerability also exists at any facility using an access media/identification system that grants access privileges to employees and others. These "insiders" have legitimate needs to access the portions of the airport controlled for security purposes and are granted access to those areas, and in some cases to the workings of the security system itself. However, threats from insiders, acting alone or in collusion with outsiders, pose a criminal and terrorist threat to airports. The need to inspect individuals, their identification media, and their possessions as they cross the security boundary using their access privileges, may increase in the future. The need to identify and control individuals under escort within the controlled portions of the airport may also increase in the future, affecting the design of access gates and the procedures used to authorize access to the airside. At the planning and design stage, one goal should be to minimize the number of access points that employees use to gain access to their work site in the secure area. Infrastructure provisions for screening equipment at these locations would enable future inspection capability with significantly less impact. The same locations may also be considered as sites for inspection of deliveries of commercial goods. Although challenging in the absence of specific security requirements, designers and planners should consider throughput in the event security requirements are mandated for employee access portals.

h. There are numerous areas in and around an airport, its terminal building complex, support facilities, utility tunnels, storm sewers, construction entrances, public roadways, parking lots, maintenance areas, cargo and

general aviation facilities, commercial and industrial buildings, etc., which, while not necessarily recognized as a target of terrorist activity, might still be in the path of such an attack, or at the very least might be subject of common crime such as theft or vandalism, and thus might require varying levels of security protection. These may or may not fall under the jurisdiction or responsibility of the airport, but it is important to look at the entire airport environment, make those determinations, and bring every affected entity into the early planning discussions, if for no other reason than to establish early on where the lines of responsibility lie. The airport must also keep careful records of these determinations, and consider putting those agreements and lines of demarcation in writing, possibly as conditions of the lease, or into exclusive area or ATSP agreements.

i. Utility Infrastructure

1) Utility sources, equipment and supply potential should be protected and/or monitored to the extent warranted by a threat and vulnerability assessment. Contact the airport security coordinator and local FSD for any current studies relating to utility infrastructure security. The design of these systems should also reflect their importance for mission-critical operations of airports, with due consideration given to redundancy, backup systems, alternative sources and the required levels of service, response times during emergency situations, and associated airport and non-airport organizational responsibilities.

2) In this context, 'utilities' encompasses electrical power including both external services and on-airport generation and distribution systems; lighting; water and drainage systems; fuel farms including pipeline distribution and pumping stations; telecommunications (voice, video, data) including external wired and wireless services as well as on-airport networks and trunked radio systems used for public safety functions; and facility heating, ventilation and Cooling (HVAC).

3) Electrical power is critical to an airport's operation. No major airport should be without alternatives to its primary electrical power supply, such as linkage to a second substation or, where feasible, a second regional grid, generated secondary power, and/or battery back-up or an Uninterrupted Power Supply (UPS) system with appropriate switching capability. Individual battery back-up or UPS units to support access control systems during power outages are also highly desirable. Furthermore, the security design must provide distributed essential power for priority provisions (i.e., lighting, communications, etc.). Consideration should also be given to providing essential power to support defined secondary (limited use) requirements that may be needed during outages.

4) HVAC systems have important functions during extreme weather conditions because they control and maintain ambient temperatures for thousands of passengers and employees. HVAC equipment provides fresh air or heat circulation, and an attractive target or vector for attack. The security design should consider providing a capability to monitor publicly accessible air intakes (e.g., use of video cameras), the capability to isolate sections of the building, and to extract and vent sections of the building by using a positive air pressure. *See Appendix G, Airport Chem-Bio Protection and Response.* For more on design to prevent or mitigate chem-bio events.

5) Tunnels and drainage provisions provide apertures into the building that may be exploited by an adversary. Airport design should consider the security of the routes by which utilities enter and exit the terminal building.

6) Fuel supplies may support vehicle and/or aircraft operations that require protecting the pipelines, fuel farms, or other facilities that are operationally sensitive and vulnerable to attack.

7) Water sources may merit protection, keeping in mind the function of the water. Whether water's source is external or internal, the designer should assess the level of risk for all aspects of the system. The designer may consider protecting the water supply from interruption or the introduction of a contaminant. An alternative source of water may be appropriate, particularly for fire-fighting and other emergency purposes.

8) Telecommunications services and the networks on which they run provide essential services for airport operations. Service entrance points for carrier services should be protected against both accidental and deliberate damage. Telecommunications rooms and operations centers should be designated as

"critical assets" and secured by ACAMS and CCTV systems in the same manner as other critical airport facilities. When network cabling traverses public areas, metal conduit should be used to protect the cabling.

9) In emergencies, having reliable, robust, and capable wireless communications for management, operations, and public safety functions will be essential. Public safety departments will often have their own trunked radio systems, which should also support airport operations and other departments. Dependence on carrier cellular services should be minimized as these networks can be saturated by traffic during emergencies. A standards-based wireless extension of the airport local area network (LAN) can be valuable in emergencies provided that operating frequencies and access point coverage have been properly designed and coordinated with all users including tenants.

10) Seismic Requirements

Seismic requirements, while not innately a security issue, are relevant to security guidelines in that the continuity of operations of an airport is paramount to airport security.

This section provides information referencing various state and federal legislation addressing seismic safety. While much seismic engineering and mitigation guidance exists in the form of state and local codes, directives and ordinances, these requirements focus only on acts that are currently in effect, not those being proposed for future planning and design needs.

The existence of these laws does not necessarily indicate that they fully meet their intent, or that they necessarily accomplish their objectives. Some are considered more or less effective than others, and even some weaker ones may be enforced to a greater extent than others. Architects, engineers and contractors should refer to further resources for information or expert opinion about the appropriateness and effectiveness of any specific seismic requirement as it affects their airport design. It is also important to note that the burden of conformance may rest solely on the Architect, Engineer and Contractor and to remember that the guidelines and regulations supporting the implementation of individual acts often contain the most important detail.

In recent years enforcement of the earthquake protection requirements in the Model Codes for nonstructural building components has also become commonplace. Model Codes provide for nonstructural, infrastructure elements of the building design, such as electrical enclosures, control consoles, conduits, cable trays, etc. Architects, Engineers and Contractors are relied upon to know, understand, design and install earthquake protection in accordance with the requirements of these Codes.

It is important to note that all of the Seismic Laws and the Executive Orders apply to virtually all new construction that is federally owned, leased or regulated or other new construction that receives federal financial assistance through loans, loan guarantees, grants or federal mortgage insurance. Additionally, several states require seismic mitigation in the design of all projects.

When designing a project, it is important to meet the federal, state and local code and standard elements applicable to the project location. Although the following list is not intended to be comprehensive and complete, as an aid to the designer, the TSA recommends that the following sources of information be checked to determine the requirements to be applied.

a) Public Laws 95-124 and 101-614 "The Earthquake Hazards Reduction Act of 1977 as Amended"
b) Executive Order 12699 of January 5, 1990 "Seismic Safety of Federal and Federally Assisted or Regulated New Building Construction"
c) Executive Order 12941 of December 1, 1994 "Seismic Safety of Existing Federally Owned or Leased Buildings"
d) ICBO (International Conference of Building Officials) "Uniform Building Code (UBC)," 1994, and amendments to include the 1994 NFPA-13 Standard for Building Fire Sprinkler Systems
e) BOCA (Building Officials Code Authority) "National Building Code"
f) SBCCI (Southern Building Code Congress International) "Standard Building Code"

g) Section 13080 of the Corps of Engineers Guide Specifications with Fire sprinkler Sections 15330, 15331, and 15332 revised in March 1995 to unequivocally require seismic bracing on the small diameter piping.

h) Various State Building Codes, e.g., California, Washington, Alaska, Missouri, New York, etc., which may require mitigation elements in addition to the national standards.

**Section III-A-3 - Vulnerable Areas Checklist:**

- ☐ **Vulnerability Assessment (see *Appendix A*)**
- ☐ **Consider all assets, targets, and their relative value/loss consequence**
  - Aircraft
  - Communications
  - Support Facilities
  - Terminal
  - Public and Employees
  - Fuel Areas
  - Utilities
  - Roadways and Access Way
  - Storage Areas
- ☐ **Establish a security boundary between public and secured areas**
  - Barriers
  - Patrols
  - Surveillance/CCTV
  - Sensors
- ☐ **Minimize means of unauthorized access**
  - Access Controls
  - Emergency Exits
  - Delays
  - Piggybacking
  - Surveillance/CCTV
- ☐ **Plan for breach control measures and procedures**
  - Physical Barriers
  - Separation Distance
- ☐ **Reduce bombing/armed attack vulnerability**
  - Blast Mitigation
  - Separation Distance
  - Minimization of Large Congregations
  - Placement of Screening Checkpoint
- ☐ **Minimize vulnerability from employees**
  - Minimize numbers of employee access points
  - Capability for Employee Screening
- ☐ **Consider vulnerability of adjacent areas and paths of travel**

### 4. Chemical and Biological Agents

When considering overall layout, it is prudent to take some precautions to prevent attacks by non-conventional means, such as the use of chemical and biological agents, to attack civil aviation. The possibilities for such attacks include the use of chemical or biological agents to attack persons in an aircraft in flight, as well as in public areas of airports, (see *Terminal* on page 58) or persons in areas controlled for security purposes.

Some measures that should be considered to help mitigate a potential chemical/biological attack include:

- Locate mailrooms and airport loading docks at the perimeter of the terminal or at a remote location with "screening" devices in place that can detect explosives and chemical/biological contaminants.
- If the mailroom and loading docks are in or near the terminal, consider having a dedicated ventilation system for those rooms and dedicate an emergency shut-off device for the ventilation system.
- Take measures to seal off these areas from the rest of the terminal to minimize the potential for contaminants to migrate to other areas of the terminal. Maintain a slight negative pressure in these rooms to help prevent the spread of the contaminants to other areas.
- Locate air intakes to HVAC systems so they are not accessible to the public. Preferably, locate air intake as high as practical on a wall or on the roof; if vents are ground level, they should be protected if possible with screens or grates, and turned away from public exposure.
- Coordinate the smoke control system and emergency power with the chemical/biological alarms and ventilation system.
- Consider installing special air filtration in critical ventilation systems that captures chemical/biological agents.

Additionally, at the direction of the Department of Homeland Security (DHS) Science and Technology Directorate through the PROACT (Protective and Responsive Options for Airport Counter-Terrorism) program, the Sandia National Laboratories issued "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism," co-authored with the Lawrence Berkeley National laboratories. These guidelines are available for review from the TSA Federal Security Director at your airport or directly from Sandia National Laboratories upon request. An extract of the Sandia National Laboratories document is available in *Appendix G* of this document.

**Section III-A-4 - Chemical & Biological Agent Checklist:**

- ☐ **Sources of guidance may include TSA, Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Center for Disease Control (CDC) and Office for Domestic Preparedness Support.**
- ☐ **The *Bibliography* lists several relevant chem.-bio documents.**
- ☐ **Report Card for *airport Chem-Bio Protection and Response***

**5. Boundaries and Access Points**

To delineate and adequately protect the AOA, SIDA, and other security areas from unauthorized access, it is important to consider boundary measures such as fencing, walls, or other physical barriers, electronic boundaries (e.g. sensor lines, alarms), and natural barriers in the planning and design process of an airport. Access points for personnel and vehicles through the boundary lines, such as gates, doors, guard stations, and electronically controlled or monitored portals must also be considered. In addition, there are other security measures which should be part of the design that enhance these boundaries and access points such as clear zones on both sides of fences, security lighting, locks, monitoring systems such as CCTV, and signage.

The choice of an appropriate security boundary design is not only affected by the cost of equipment, installation, and maintenance, but also by the more important aspects of effectiveness and functionality. Certainly the highest consideration in an effective boundary measure is its ability to prevent unauthorized penetration. Thus, any access points through a boundary line must not only be able to prevent access, but differentiate between an authorized and an unauthorized user. At an airport, access through boundary lines can be frequent, and must be quick to prevent unacceptable delays. In addition, if a boundary access point is not user-friendly, it may be abused, disregarded, or subverted and thus, pose a security risk and possible financial liability to the airport.

Regardless of boundary location or type, the number of access points should be minimized for both security and cost efficiency. Proper planning and design can often create fewer, more functional and maintainable access points that will benefit the airport in the long run.

Various boundary/barrier and access point types as well as security measures which can enhance them are described below:

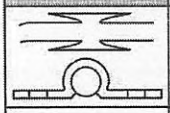
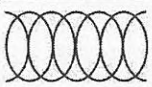
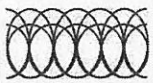
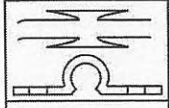
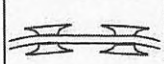
a. Physical Barriers

Physical barriers can be used to deter and delay the access of unauthorized persons into nonpublic areas of airports. These are usually permanent barriers and designed to be an obvious visual barrier as well as a physical one. They also serve to meet safety requirements in many cases. Where possible, security fencing or other physical barriers should be aligned with security area boundaries.

1) Fencing

Fencing is available in several designs that are difficult to climb or cut as well as those which are provided with motion, tension or other electronic sensing means. For fences with sensors, either mounted on the fencing or covering areas behind fencing, there are other elements to the security system for monitoring of the sensors and response to intrusion alarms. *Table III-A-1* below shows some of the available types of fence fabrics.

**Table III-A-1 - Fence Types and Fabric**

| | PRODUCT | APPLICATION | SIZES | WT / ROLL | MATERIAL | ATTACHMENT SPACING LENGTH | BREAK LOAD |
|---|---|---|---|---|---|---|---|
|  | RAZOR RIBBON - Single Coil with Core Wire | Medium Security Fence Topping | 18″<br>24″<br>30″ | 13 lbs.<br>17 lbs.<br>21 lbs. | AISI 430 Stainless Steel, .098 dia. high Tensile Wire | 6″ - 16.67′<br>9″ - 25′<br>18″ - 50′ | 2800 lbs. |
|  | RAZOR RIBBON MAZE - Single Coil with Wire, Concertina Style | Ground Barrier Max. Security Fence Topping | 24″<br>30″<br>36″ | 15 lbs.<br>19 lbs.<br>23 lbs. | AISI 430 Stainless Steel, .098 dia. high Tensile Wire | 12″ - 15′<br>16″ - 20′ | 2800 lbs. |
|  | RAZOR RIBBON MAZE - Concertina Style, Double Coil | Ground Barrier Max. Security Fence Topping | 24″ inside<br>30″ outside | 34 lbs. | AISI 430 Stainless Steel, .098 dia. high Tensile Wire | 12″ - 15′<br>16″ - 20′ | 2800 lbs. |
| | MIL-B-52775 B Type II - Austenitic Double Coil | Ground Barrier Max. Security Fence Topping | 24″ inside<br>30″ outside | 35 lbs. | AISI 301 / 304 Stainless Steel .047 dia. Stainless Wire Rope | 24″ - 66′ | 2250 lbs. |
| | MIL-B-52775 B Type IV - Austenitic Double Coil | Ground Barrier Max. Security Fence Topping | 24″ inside<br>30″ outside | 35 lbs. | AISI 316 Stainless Steel .047 dia. Stainless Wire Rope | 24″ - 66′ | 2250 lbs. |
|  | RAZOR RIBBON - Single Coil | Min. Security Fence Topping. Commercial Use | 18″<br>24″ | 9 lbs.<br>12 lbs. | AISI 430 Stainless Steel | 6″ - 16.67′<br>9″ - 25′<br>18″ - 50′ | 1260 lbs. |
|  | BAYONET BARB - Concertina | Ground Barrier | 27 1/2″<br>37 1/2″ | 23 lbs.<br>34 lbs. | ASTM A 526 Zinc Galvanized .098 dia. high Tensile Wire | 20″ - 50′ | 1300 lbs. |

Chain link fencing is a common type of fencing and is often the most cost-effective solution when deterrence, as opposed to the prevention of forced entry, is the primary security objective. Chain link fences are typically constructed with 7 feet of fabric plus one or more coils of stranded barbed wire on top, which may be angled outward at a 45 degree incline from the airside. Fences configured in this manner are shown in *Figure III-A-1* below.

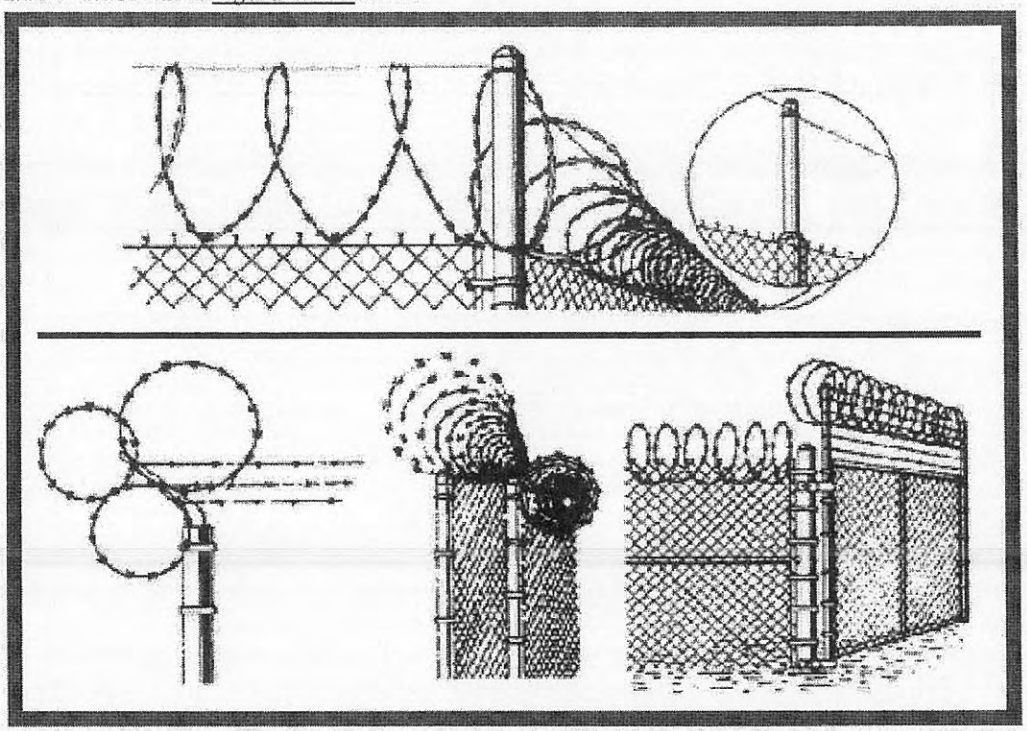


**Figure III-A-1 - Chain Link Fence Barbed Wire Configurations**

Chain link fencing is normally the most suitable and economic physical barrier for securing the airside, although this may vary somewhat with airport-specific conditions and topography. It is also readily available through a large variety of sources and is easily and inexpensively maintained. This type of fence provides clear visibility for security patrols, and is available in varieties that can be installed in almost any environment. Barbed wire, razor wire and other available toppings increase intrusion difficulty. For locations with aesthetic concerns, there are also a large variety of decorative yet functional styles available as well as opaque styles that limit public visibility of service, storage or other non-aesthetic areas. On boundaries coinciding with property lines, locate the fence line should be located inside the airport property line to prevent encroachment on adjacent property by the barbed wire angled topping or its outriggers.

Another common type of fencing is constructed of vertical bars which have curved spiked tops as shown in *Figure III-A-2* below. Depending on the diameter and materials used for the bars, this design can provide additional protection against forced entry.

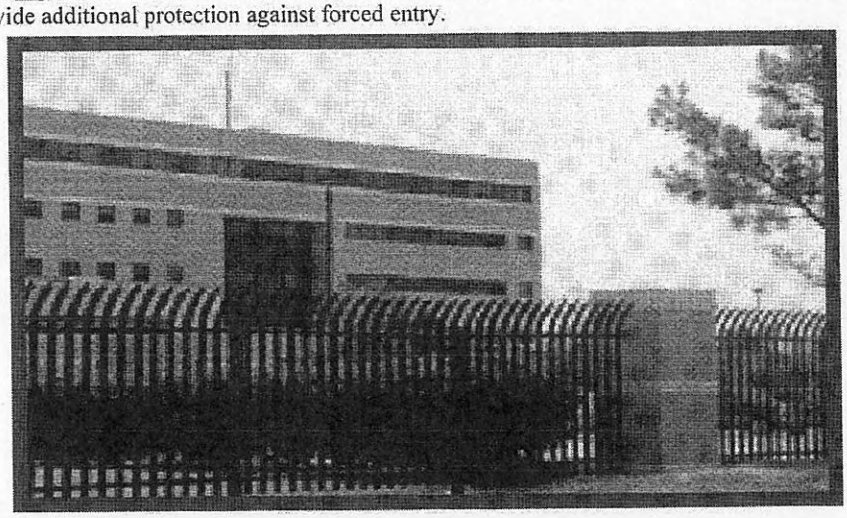


**Figure III-A-2 - Vertical Bar Fence**

There are several means of constructing fences to provide a higher level of protection against forced entry. Chain link fences, for example, can be reinforced with posts and rails, as shown in *Figure III-A-3* below, with rails being either solid material or stranded-steel cable encased in hollow pipe. The posts and rails can also be designed to blend into the fence. This type of reinforced fencing has been has successfully tested to the U.S. Department of State's K8 Anti-Ram rating, stopping a 15,000 pound truck traveling at 40 mph within 3 feet of the fence line.

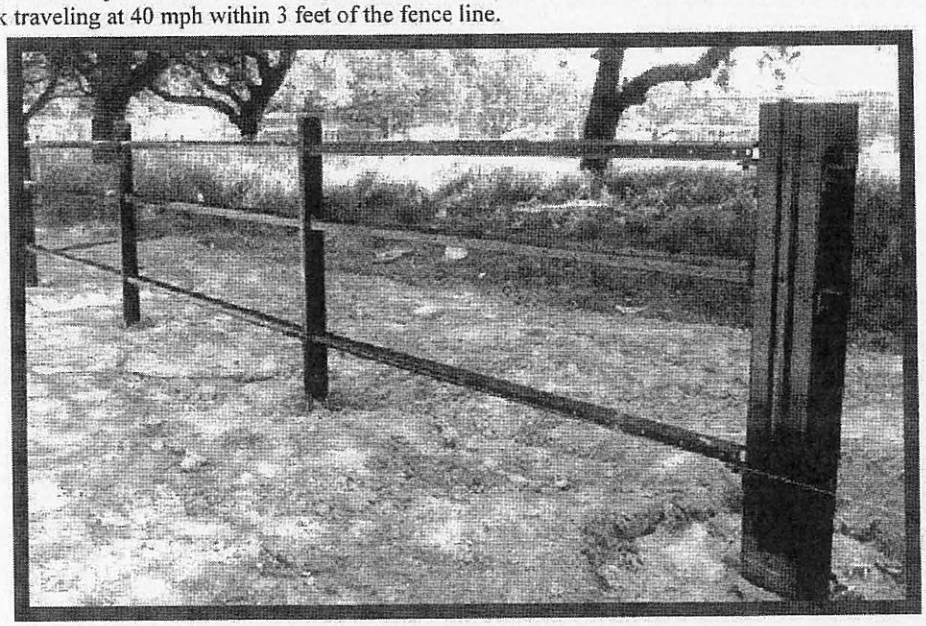


**Figure III-A-3 - Fence Post and Rail Reinforcement**

When utilizing fencing as a security boundary, care must be taken to ensure that the provision of fencing does not conflict with the operational requirements of the airport. Access points must permit passage of authorized vehicles and persons with relative ease. While the number of access points should be kept to a minimum, adequate access points must be planned for routine operations, maintenance operations, and emergency operations. For further information on fencing access points see *Gates* on page 29 or *Guard Stations* on page 31.

To assist in surveillance and security patrol inspection, keep fences as straight and uncomplicated as possible. This will minimize installation and maintenance costs.

Wind is often an issue when designing chain link fencing to be instrumented with intrusion detection sensors, including wind-induced fence motion caused by proximity of fencing to runways. A taut fence fabric is often required under such circumstances.

Effectiveness of fencing in critical areas can be improved by anchoring or burying the bottom edge of the fence fabric to prevent it from being pulled out or up to facilitate unauthorized entry. Use of concrete mow strips below the fence line and/or burying the bottom of the fence fabric can also deter tunneling underneath the fence by persons and animals. Mowing strips may also reduce security and maintenance man-hours and costs.

For safety or operational reasons (e.g. presence of navigational systems) some sections of perimeter fencing may not be able to meet standard security specifications. Special surveillance or detection measures may need to be applied to improve the safeguarding of these areas.

More specific information on fencing materials and installation, including the use of barbed wire outriggers, is available in FAA Advisory Circular 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities; and Advisory Circular 150/5370-10, Standards for Specifying Construction of Airports, among others.

In summary, fences are the most basic first line of deterrence and defense. There is excellent guidance available from the Chain Link Manufacturers Institute, including detailed technical and procurement guidelines and specifications such as the Security Fencing Recommendations..

2) Buildings

Buildings and other fixed structures may be used as a part of the physical barrier and be incorporated into a fence line if access control or other measures to restrict unauthorized passage through the buildings or structures are taken at all points of access. Whether those points are located on the airside or landside boundaries, or perhaps through the middle of such buildings, may be dependent upon the nature of the business being conducted inside, and the level of continuous access required by personnel.

3) Walls

Walls are one of the most common types of physical barriers. Various types of walls are used for interior as well as exterior security boundary separation. In addition, walls play an important part as visual barriers and deterrents.

a) Interior Walls

When interior walls are to be used as security barriers, consideration should be made to the type, construction material used, and their height. When possible, security walls should be full height, reaching not just suspended ceilings, but complete floor to ceiling or slab.

Interior walls may be used as part of the security boundary, with appropriate attention paid to maintaining the integrity of the boundary and the level of access control to a degree at least equal to that of the rest of the boundary.

b) Exterior Walls

While typically not as economical as chain link fencing, the use of exterior walls as physical barriers and security boundaries is frequently necessary. Walls provide less visibility of storage or secured areas and can be matched to the surrounding architecture and buildings. In addition, some varieties of exterior walls are less climbable and thus more secure than security fencing or other barriers that offer hand-holds.

Walls of solid materials should not have hand or foot holds that can be used for climbing. The tops of walls should be narrow to prevent perching, and should have barbed wire or other deterrent materials. Blast walls are not necessarily good security fences, although appropriate design can aid in incorporating features of both, spreading the cost over more than one budget.

As in the case of interior walls, exterior building walls may also be used as part of the security boundary as long as the integrity of the secured area is maintained to at least the level maintained elsewhere along the boundary.

b. Electronic Boundaries

In the case of boundaries which are monitored by electronic sensors, motion detectors, infrared or microwave sensors, etc., it is clear that these are intended to serve essentially the same security functions as other detectors, but are simply employing other technologies, usually with somewhat higher maintenance costs. Typically they will be used in conjunction with other technologies such as alarms, CCTV, or other reporting and assessment methods. Nonetheless, there are appropriate places for using such applications, especially where normal conduit and cabling might be impractical, or where excessive trenching might be required. In addition, new technologies involving existing FAA ground radar surveillance can be incorporated for use in a security mode. See also Radio Technical Commission for Aeronautics (RTCA) Document DO-221, "Guidance and Recommended Requirements for Airport Surface Movement Sensors."

1) New Electronic Boundary Technologies

This document is focused on planning and design during the initial planning for current projects, even though new facilities such as terminals may sometimes be 4 or 5 years from the drawing board to processing the first aircraft and its passengers. When planning that terminal, and all other related facilities requiring a security perspective, one must also take account of continuing developments throughout the airport industry and the technologies that contribute to its secure well-being. While it may not be possible, or even prudent, to adopt first-generation beta-version technologies (although there may also be some corresponding advantages in such an approach), it is virtually certain that technology developments in many areas will afford new security capabilities and new requirements in the easily foreseeable future.

Among these is a rather broad concept called "data fusion", in which a wide array of sensors, surveillance techniques, data analysis and communications capabilities and procedures are brought together to enhance the ability of airport security to monitor and respond to a wide range of alarms, including the use of automated system analyses and alerts, thereby expanding an operator's "vision" and capability several fold.

Whether this is a necessary, immediate, or even desirable course of action for your airport, nevertheless as new technology becomes tested and available, it may not only be useful but also very cost-effective to consider such expansion early-on when designing infrastructure such as cabling to perimeter locations, power sources, lighting, communications, and more, so as to avoid the need for such costly things as re-trenching, replacing limited panels, relocating camera positions, etc.

One such technology being tested in a major Category X environment is the adaptation of the existing FAA ASDE ground surveillance radar signal to also monitor non-aircraft movement on the AOA as well as along external boundaries of an airport. This concept is illustrated in *Figure III-A-4* and *Figure III-A-5* below.

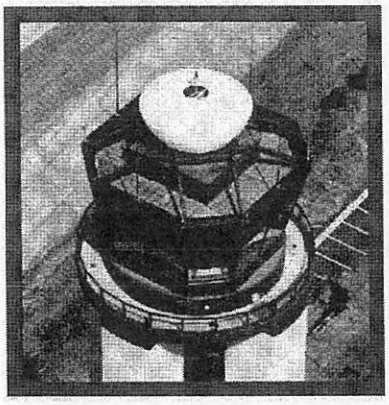


**Figure III-A-4 - ASDE Radar**

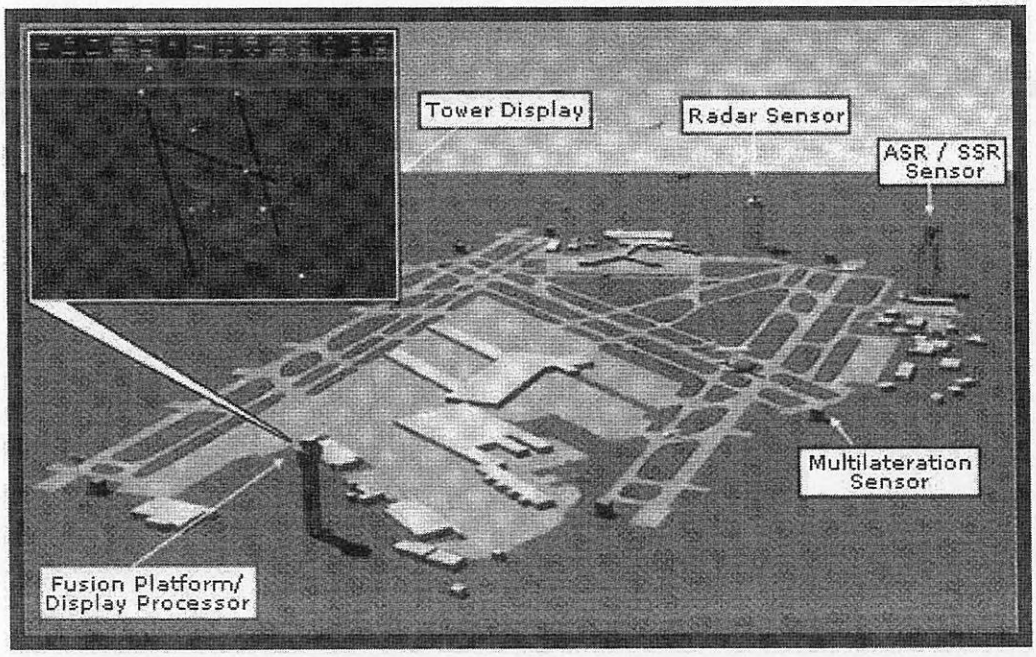



**Figure III-A-5 - ASDE Radar & Its Adaptation for Surface Security and Intrusion Detection**

Tests by TSA's Transportation Security Laboratory are designed to demonstrate that modified ASDE radar could differentiate between "approved" and "unauthorized" targets, including persons and ground vehicles as well as marine craft approaching a waterside perimeter. The radar is intended to determine the origin and track the paths of movement of these targets. With further development, the system is expected to classify an object, to predict its likely next movements or directions, and to assist the

operator in providing an appropriate level of response. Some of these functions can also be automated and applied to pre-programmed zones of priority to enhance security decision-making.

c. Natural Barriers

The use of natural barriers may be necessary or advantageous at an airport in areas that cannot structurally support physical barriers or fencing, or where the use of fencing or physical barriers would cause conflict with aircraft navigation, communications, or runway clear areas beneath approach paths. With TSA approval, natural barriers may be incorporated into the security boundary of an airport in lieu of standard physical barriers or in conjunction with and as a complement to additional security measures or procedures.

Natural barriers may include bodies of water, expanses of trees, swampland, dense foliage areas, cliffs, and other such areas.

Earthen material may also be used to create a visual barrier between any public road and the AOA. This can be accomplished through various methods such as trenching or the stockpiling of earthed materials. Trenching may be done below the grade of any adjacent airfield surface such as the perimeter road and at a slope that would prevent an individual from achieving a visual reference of the airfield. The stockpiling of material can also be used to create a visual barrier, but must not impact any protected surfaces or create an impact to the safe and efficient operation of aircraft or any airport operation. It is in the interest of the airport operator to have an above grade barrier on the airport property for ease of maintenance and control. A fence may be constructed atop the barrier

Using "time and distance" from critical facilities to be protected is another optional natural barrier. This concept suggests that if an unauthorized entry were to occur at a particular location, the amount of time and distance, combined with a high level of visibility would significantly reduce the likelihood of the intruder reaching the critical area without detection and/or intervention. "Time and distance" may be considered as an enhancement to standard physical barriers/boundaries when barriers or boundaries are relatively removed from the critical areas they are protecting.

Another common security design principle is known as "DDR: Detect, Delay, Respond", in which protection of a relatively remote perimeter or facility may require only moderate security measures if it is sufficiently removed from the primary security-related areas to allow the airport to detect an intrusion, and delay its progress until an appropriate security response can be implemented.

d. Access Points

Typically there are access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are typically doors; guard points or electronic means or controls may be also used. In all cases, the access point type and design may be the determining factor in the effectiveness of the security boundary and control in that area. So, in all cases, the number of access points should be minimized and their use and conditions closely monitored.

1) Gates

While the number of access points should be kept to a minimum, adequate pedestrian and vehicle access points must be planned for routine operations, maintenance operations, and emergency operations.

a) Routine Operations

Routine operational gates at an airport are typically those used by operations personnel, police patrols and response teams, catering, fuel and belly cargo vehicles and tugs, scheduled delivery vehicles, and ground service equipment and maintenance vehicles.

Most airport gates used for routine operations are typically high-throughput and should be designed for high-activity and long-life. These gates will take the most wear and tear, and should be designed to minimize delays to users, particularly where piggybacking may be a concern.

SIDA, secured area, AOA, and other security boundary gates that are high-throughput are the most likely candidates for automation and electronic access control. See *Electronic Access Points* on page 31 for further information

b) Maintenance Operations

Maintenance operations gates at an airport are typically those used by the airport, tenant and FAA personnel to perform regular and periodic maintenance to remote grounds or equipment. Typical maintenance tasks include mowing, utility service, navigational and communications equipment maintenance.

These gates, unless high-throughput or jointly used for routine operations, are typically non-automated, non-electronic.

c) Emergency Operations

Emergency operations gates are gates used by on-airport and mutual aid emergency response vehicles responding to emergency situations, especially those involving an aircraft, but may also be used for regular operations

Airport emergency operations gate controls may be controlled from an emergency operations center; or from the ARFF response vehicles themselves.

A capability for emergency response vehicles to crash through frangible mounts at emergency operations gates should be considered during the gate design, as should alarms on those gates. Consider special paint markings to identify the frangible fence or gate sections to approaching response vehicles.

Gates should be constructed and installed to the same or greater standard of security as any adjacent fencing to maintain the integrity of the area.

All gates should be equipped to be securely closed and locked, where enhanced security conditions require it. Swing gate hinges should be of the non-liftoff type or provided with additional welding to prevent the gates from being removed.

Security provided by gates can be improved if they are designed and installed with no more than 4'-6" of ground clearance beneath the gate. Where cantilever (slide) and/or rolling gates are used, consideration should be made during planning and design to curb heights, wheel paths, potential obstructions, local weather/wind phenomena, and drainage issues throughout the full path of the gate and in its adjacent areas. Proper drainage grading, planned gaps in curbs, installation of concrete channels or mow strips below the gate path, and use of bollards to prevent obstructions within the gate path and protect gate equipment are all design considerations which may prolong the efficient operation of a slide gate.

If "tailgating" entry is a concern at un-staffed vehicle access points, the first response is usually procedural rather than design, since it is the responsibility of the person authorized to use the gate to be certain tailgating does not occur. However, if a fence design solution is desired, an automated two-gate system (also known as a "vehicle entrapment gate") is one method that could help prevent "tailgate" entry. Such gates are separated one vehicle length apart and are sequenced so that the second gate does not open until the first has fully closed. Time-delayed closures are a viable alternative; sensor arrays have also been used to successfully monitor vehicle movement and assist in detection of "tailgate" entries. "Tailgating" and "reverse tailgating" (where a vehicle enters a gate opened by an exiting vehicle) at automated gates may also be reduced by use of a security equipment layout that provides space for waiting vehicles to stop, which obstructs, or at least deters other vehicles from passing through. CCTV may deter breaches at those facilities, and may provide an improved response when breaches occur. Additionally, CCTV may provide a visual record that can be used to document breaches that become the subject of investigations.

More specific information on gate materials and installation is available in FAA Advisory Circular 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities, and Advisory Circular 150/5370-10, Standards for Specifying Construction of Airports, among others.

2) Doors

To prevent unauthorized access to the airside, doors leading from unsecured areas of the terminal to the airside, and which are under visual control of authorized personnel, should be limited to the operational minimum. Nevertheless, where they are necessary, electronic devices or closely controlled lock and key procedures may best control these doors. It may, however, be preferable to include the

use of electronic control devices, such as CCTV or cardreader/pinpads, to minimize labor costs and to be able to track personnel using specific doors to the AOA.

Unsupervised emergency exit doors providing egress from the terminal to the airside should be avoided if possible. If essential, these doors should be equipped with audio and visual alarms. Consider mounting a police-blue lens (to differentiate security from fire alarms), preferably located on both sides of the door, which can be monitored from a supervised location such as an airport security control center. Consider the possibility of CCTV cameras on both sides of certain high risk or high traffic doors. The use of frangible devices or covers over emergency exit activation bars deters misuse. Some codes allow for special locking arrangements for emergency exits that provide delays of up to 45 seconds, depending on local fire and life safety codes, as long as reasonable life safety is assured. Building codes establish specific performance requirements for doors with delay egress hardware. Each airport must work with local fire and building code officials to determine the best systems allowable to accommodate both emergency and security needs. See also *Emergency Exits* on page 70 for information regarding NFPA fire codes on emergency exits.

Passenger gates, aircraft loading walkways and other devices used for aircraft loading must be capable of being locked or otherwise secured to prevent unauthorized access to the airside and parked aircraft.

3) Guard Stations

Manned guard stations to control access into a security area may be appropriate at some locations. The purpose of such guard stations is to provide a point of entry at which personal identification can be established and persons and vehicles can be permitted to enter according to local security program requirements which vehicles require search.

a) Devices such as turnstiles, tire shredders, roll gates, pop-up barriers, or a remotely operated drop arm barrier gate may be used at guard stations to impede passage through the guard station until access authority is verified.

b) Use of a sheltered checkpoint station is recommended for gates secured by security personnel. The shelter can be designed to permit maximum visibility over the immediate area of the gate and to provide easy access for the guard to carry out the duties of inspecting vehicles and their contents.

c) Sufficient space should be provided to direct a person or vehicle to one side for further inspection without blocking access for those following. Space should also be provided to allow vehicles refused entry to turn and exit. Vehicle lanes and inspection stations should be provided in sufficient quantity to meet the expected traffic volumes, average inspection and processing times, and size of the largest vehicle entering the checkpoint. Stations may employ vehicle manifest pre-clearance checkpoints and special expedited clearance lanes for recognized deliveries, by agreement between the airport and the TSA. Dependable and instant communications from these stations to a central location must be installed, maintained, and frequently tested.

d) It is essential to provide communications between any sheltered security checkpoint station and the airport security services office, as well as to provide a duress alarm by which emergency assistance may be summoned.

e) In some applications, a vehicle access point may be remotely controlled by use of a card reader or similar credential verification device, in conjunction with CCTV monitoring taking place at the Security/Communications Center.

4) Electronic Access Points

a) Automatic Gates

In cases where gates are automated and induction loops are used on the airside of gates for free vehicle exit, ensure the loop is located so as to minimize the possibility of objects being thrown or pushed from the public side to activate the loop. Additional access control measures, such as microwave, infrared or other vehicle sensors or CCTV monitoring may be desirable in addition to loops where space is limited or additional security is desired.

Consider means of protecting access control devices (such as card readers or other monitors) serving exterior vehicle gates to reduce possible physical damage from passing vehicles. Properly placed

curbing, bollards, and highway railing are useful for this purpose. Consider also protection of equipment from weather elements, including protection from extreme heat or cold inside equipment enclosures, which can affect the operation of electronic and mechanical components. Heaters and/or fans are available as standard options for most access control devices, housings and operators.

b) Doors with Access Controls

There are numerous technologies available for controlling access through doors (magnetic stripe, Weigand, proximity, Smart card, etc.) and there are numerous ways of implementing their use at any kind of doorway – wooden doors, glass, metal, single or double doors, roll-up doors, or indeed at electronic barriers where there is no physical door at all. The designer should take into account any existing systems the airport might wish to retain and integrate with new systems, and whether newer advances in technology might suggest a complete or partial replacement of the old systems to provide better security and security management. An extensive discussion of this issue is found in the RTCA document DO-230A, "Standards for Airport Security Access Control Systems." Recent technological advances may provide additional solutions including biometrics.

c) Sensor Line Gates

Sensor line gates and/or electronic gates function as typical access controlled gates, except that a sensor line (microwave, infrared, etc.) is used instead of a mechanical barrier. Depending on the electronic sensor technology used (see *Electronic Boundaries* on page 27 for further information), sensor line gates may be comparable in cost to mechanical ones.

The use of sensor line gates is typically the most feasible as a second, interior boundary where delays due to the mechanical operation of a physical gate are not practical, where space is limited, or where additional vehicle monitoring is desired. Sensor line gates are most often used to control vehicle access into a secured area or in cargo or maintenance areas where time is critical.

d) Automated Portals

Automated access portals are designed for high-throughput, performing access control and/or providing sensing technology in a high-speed, multi-user fashion, yet also providing a positive means of access denial of unauthorized persons. They typically provide an unobstructed pathway with the capability of preventing access if multiple or unauthorized persons attempt to enter. Where these are employed, the delay induced by door opening/closing is eliminated. These portals are designed to replace high-throughput doors where piggybacking is a concern or to add additional explosives, drug, or weapon sensing technology to high-throughput areas.

There are also portals and sensing technologies under development that are sensitive to the direction of the intruder's movement, and automatically provide photographs of security violators, and/or detain unauthorized individuals. As technology advances, the capability and affordability of automatic portals will increase and should be evaluated for high-throughput and/or special-use access point locations.

5) Vehicle Inspection Stations, Blast Protection, and Road Barriers

Manned vehicle inspection stations and vehicle crash barriers in roadways may be necessary to control access in and around the airport terminal and other airport facilities. Additional, non-permanent measures may also be necessary during elevated threat levels or high-risk areas. This aspect of airport design should begin with the results of the vulnerability assessment undertaken during the planning phase.

The purpose of vehicle inspection stations is to provide a location outside of the "blast envelope" in which to inspect vehicles that are approaching the airport terminal on the access roadway. Vehicle inspection stations may also be necessary at vehicle parking locations that are located within the blast envelope. Consideration should be given to including the following features at vehicle inspection stations.

a) Turnstiles, roll gates, or vehicular crash barriers should be provided that will stop or impede "gate crashing."

b) A sheltered checkpoint station is recommended. The shelter should be designed to permit maximum visibility over the immediate area of the station and to provide easy access for the guard to carry out the duties of inspecting vehicles and their contents.

c) Sufficient space should be considered to direct a person or vehicle to one side for further inspection without blocking access for those following. Dependable and instant communications from these stations to the Security Operations Center (SOC) or other appropriate central location should be installed, maintained, and frequently tested. Sufficient space should be provided for emergency vehicles and other pre-authorized vehicles to by pass the vehicle inspection stations to access the terminal.

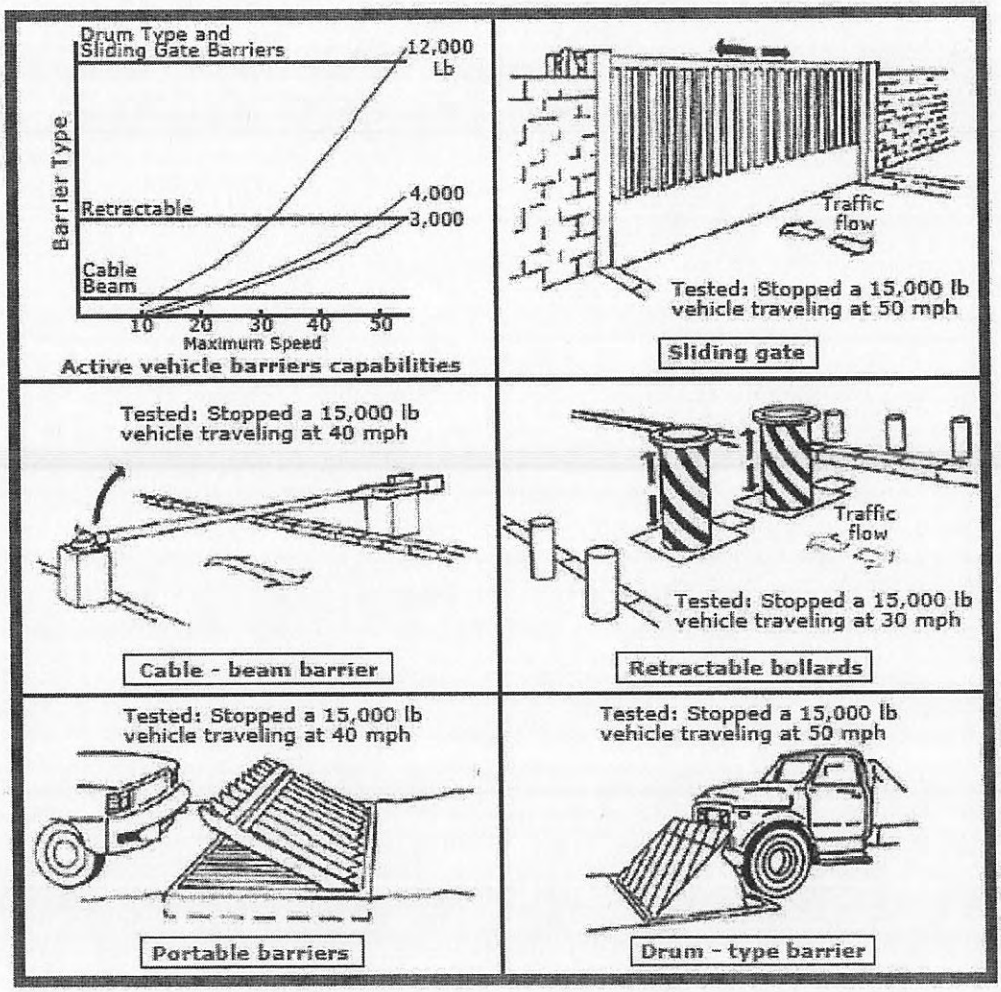
d) A duress alarm system should be provided.

e) Provide ample vehicle queuing distance and vehicle inspection portals to avoid long traffic backups and delays.

Airports are faced with the possibility of attack by explosive-laden vehicles. Fortunately, there is a considerable body of knowledge on blast effects and protective measures available at U.S. government laboratories and agencies. In addition, the U.S. Department of State (DoS) has developed standards for vehicle crash barriers which airport designers can apply with confidence in the level of protection afforded.

*Figure III-A-6* below illustrates the types of barriers that might be employed for various airport security applications, depending on the severity of the threat and the level of protection required. Barriers should also be designed to work with other measures, such as physical setbacks of buildings and natural barriers such as berms, on developing a blast protection solution.

**Figure III-A-6 - Types of Road Barriers**



Blast effects and protective measures have been extensively studied and tested. *Table III-A-2* below and *Table III-A-3* on page 36 show the lethal blast radii for various types of threats and the types of blast-protection measures that barriers might be considered to protect against each type of threat.

**Table III-A-2 - Lethal Radius of Various Explosive Packages**

| Type of Expolsive | Expolsive Capacity in TNT Equivalents | Lethal Air Blast Range |
|---|---|---|
| Pipe Bomb | 5 lbs. (2.3 kg) | |
| Briefcase, Backpack, or Suitcase Bomb | 50 lbs. (23 kg) | |
| Compact Sedan (in trunk) | 500 lbs. (227 kg) | 100 ft. (30 m) |
| Full Size Sedan (in trunk) | 1,000 lbs. (454 kg) | 125 ft. (38 m) |
| Passenger or Cargo Van | 4,000 lbs. (1,814 kg) | 200 ft. (61 m) |
| Small Box Van (14th ft box) | 10,000 lbs. (4,536 kg) | 300 ft. (91 m) |
| Box Van or Water/Fuel Truck | 30,000 lbs. (13,608 kg) | 450 ft. (137 m) |
| Semi-trailer | 60,000 lbs. (27,216 kg) | 600 ft. (183 m) |

Source: Transportation Security Working Group, "Terrorist Bomb threat Standoff (Card)," Government Printing Office (1999).

**Table III-A-3 - Comparative Effectiveness of Barrier Types**

| | | Vehicle | | Protection Level (0-10) |
|---|---|---|---|---|
| | | Weight | Speed | 10 |
| Passive Barrier Test Results | Concrete Filled Steel Bollards | 4,500 | 30 | 1 |
| | Jersey Barrier | 4,000 | 50 | 2.6 |
| | Straight Retaining Wall | 15,000 | 30 | 3.6 |
| | Sloped Back Retaining Wall | 15,000 | 40 | 6.4 |
| | Concrete Planter Retaining Wall | 15,000 | 50 | 10 |
| Active Barrier Test Results | Cable - Beam Barrier | 10,000 | 15 | .6 |
| | Rectractable Bollards | 15,000 | 30 | 3.6 |
| | Portable Barriers | 15,000 | 40 | 6.4 |
| | Drum Type Barriers | 15,000 | 50 | 10 |
| | Sliding Gate | 15,000 | 50 | 10 |

Source: Military FM 5-114

DoS performance requirements for vehicle crash barriers are based the kinetic energy represented by the mass of a vehicle and its impact velocity. These "K" ratings are:

**K4** 15,000 lb vehicle impacting at 30 mph
**K8** 15,000 lb vehicle impacting at 40 mph
**K12** 15,000 lb vehicle impacting at 50 mph

To be certified with a Department of State "K" rating, a barrier must demonstrate the ability to stop a 15,000 vehicle and the bed of the vehicle must not penetrate the barrier by more than 36 inches. Additional information on DoS security measures can be obtained from the Bureau of Diplomatic Security, Physical Security Programs, Physical Security Division (DS/PSP/PSD).

DoS certified barriers can be configured as pop-up wedge type barriers, as illustrated in *Figure III-A-7* below, or as vertical bollards or any other configuration which meets the above performance requirements.

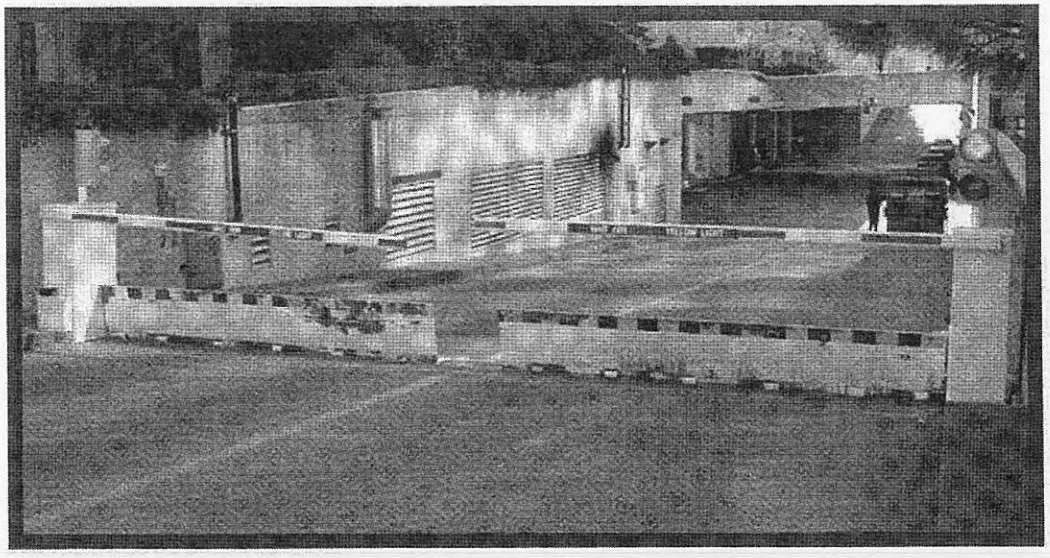


**Figure III-A-7 - Example of Pop-Up Wedge Vehicle Crash Barrier**

e. Other Security Measures

1) Fence Clear Zones

a) Security effectiveness of perimeter fencing is materially improved by the provision of clear zones on both sides of the fence, particularly in the vicinity of the terminal and any other critical facilities. Such clearance areas facilitate surveillance and maintenance of fencing and deny cover to vandals, trespassers and contraband.

b) Within clear zones there should be no climbable objects, trees, or utility poles abutting the fence line nor areas for stackable crates, pallets, storage containers, or other materials. Likewise, the parking of vehicles along the fence should also be prevented. In addition, landscaping within the clear zone should be minimized or eliminated to reduce potential hidden locations for persons, objects, fence damage, and vandalism.

c) There have been cases in which individuals have gained access to passenger aircraft by scaling or crashing through perimeter fencing. To deter or delay attacks, sufficient distance should be maintained between the perimeter fencing and aircraft parking areas.

2) Security Lighting

Lighting of the area on both sides of gates and selected areas of fencing is highly recommended. Lighting beneficial for security inspection, and to assure that fence/gate signage is readable and card readers, keypads, phones, intercoms, and/or other devices at the gate are visible and usable. Similarly, sufficient lighting is required for any area in which a CCTV camera is intended to monitor activity. Reduced lighting or sensor activated lighting may be considered in areas which have minimal traffic throughput in the off-peak hours.

3) Locks

Advanced electronic key technologies should be considered as well as the time-honored deadbolt lock, built-in door handle lock, or padlock and metallic key to secure a portal, particularly those that are

low-risk, low throughput, or significantly distant from the main areas of concern or from the central control station. Note that securing perimeter access portals through the use of locks necessarily involves procedural elements such as a key management system and the difficulties of recording usage at numerous locations and reissuing all keys when some are lost or stolen. An important consideration in choosing lock systems is total life-cycle cost.

4) CCTV Coverage
   a) While gates, like all other access points, should be kept to a minimum and, where physically and economically feasible, should be considered for treatment with access control and CCTV monitoring, it is recognized that certain low-traffic gates, maintenance access points and gates well removed from the principal areas of security concern may be candidates for greater reliance on time-and-distance considerations.
   b) Further information on CCTV Systems and coverage is contained in *Surveillance and Video Detection Systems* on page 162.

5) Signage
   a) TSA requires signage on certain security boundaries and access points. Specific requirements are found in the ASP pursuant to 1542.201 (secured area) and 1542.203 (AOA). Signs should be located such that when standing at one sign, the observer should be able to see the next sign in both directions.
   b) The use of signage, even in some non-required locations, provides a deterrent by calling attention to the boundary and stating the consequences of violating.
   c) Many locations with access control or surveillance equipment such as CCTV may warrant signage for either directional or legal purposes (e.g. "Alarm will sound if opened", "Authorized personnel only", "Notice: All activities in this area are being recorded via CCTV", etc.)
   d) While signage for security purposes should be designed to draw attention, it should be coordinated with the airport for policy, style and consistency. Based on local environment, the use of multi-lingual security signage should also be considered.
   e) Refer to the *Terminal Section* on page 58 for additional signage information.

## Section III-A-5 - Boundaries & Access Points Checklist:

- ☐ **Boundary Choice Factors**
  - Equipment Cost
  - Installation Cost
  - Maintenance Cost
  - Effectiveness
  - Functionality
- ☐ **Physical Barriers**
  - Align with security area boundaries
  - Fencing
    - Select fencing type based on threat and vulnerability assessments, aesthetic considerations, and cost
    - Typically 7' chain link fabric + 1' barbed wire
    - Fence designs are available which are difficult to climb or cut
    - Select barrier types based on threat and vulnerability assessments, aesthetic considerations, and cost
      - Permanent barriers
      - Movable barriers
      - Bollards
      - Vehicle crash barriers
    - Motion, tension or other electronic sensing means available
    - Allow access points for vehicles and persons
    - In critical areas, anchor or bury the fence bottom
    - Keep lines straight and noncomplex
    - FAA References include:
      - Advisory Circular 150/5360-13
      - Advisory Circular 150/5370-10
      - 49 CFR 1542.201 & 1542.203
  - Buildings
    - May be used as a physical barrier
    - May be incorporated into a fence line
    - Assess security access points
  - Interior Walls
    - Security walls should be full height, floor-to-solid ceiling or to slab
  - Exterior Walls
    - Aesthetic designs available
    - Minimize hand & foot holds that can be used for climbing
    - Consider topping walls with barbed wire or other deterrent materials
- ☐ **Electronic Boundaries**
  - Electronic sensors
  - Motion detectors
  - Infrared sensors
  - Stand-alone or used with other barriers
- ☐ **Natural Barriers**
  - Bodies of water
  - Expanses of trees
  - Swampland
  - Dense foliage
  - Cliffs
  - Other areas difficult to traverse
  - Natural barriers may provide "time and distance" protection
- ☐ **Access Points**
  - Minimize the number of access points
  - Gates
    - Plan for routine, maintenance, and emergency operations:
      - Patrols
      - Emergency Response Teams
      - Service Vehicles and Tugs
      - Delivery Vehicles

        - Maintenance Vehicles
    - Design for high activity/long gate life
    - Gate hinges should be non-liftoff or have welding to prevent removal
    - Automate/Monitor gates as necessary
    - Reduce ground clearance beneath, typically to no more than 4-6 inches
    - Two-gate systems can help prevent "tailgate" entry (sally ports)
    - FAA References include:
        - Advisory Circular 150/5300-13
        - Advisory Circular 150/5360-9
        - Advisory Circular 150/5360-13
        - Advisory Circular 150/5370-10
- Doors
    - Avoid unsupervised emergency exit doors to the AOA
    - Automate/Monitor doors as necessary
    - Coordinate hardware with building and fire codes
- Guard Stations
    - Manned access control and search capability
    - Size number of inspection lanes against predicted traffic volumes and inspection processing rates
    - Vehicle lane widths and heights should be matched to largest vehicle accessing the airport
    - Provide sheltered checkpoint station
    - Provide adequate secondary inspection space
    - Dependable communications required
- Electronic Access Points
    - Automatic Gates
        - Locate induction loop to minimize objects from the public-side activating loop
        - Consider bollards to reduce equipment damage by vehicles
        - Protect of electronic equipment from weather and temperature
    - Doors with Access Controls
        - Numerous technologies available
        - See RTCA DO-230A, "Standards for Airport Security Access Control Systems"
    - Sensor Line Gates
        - Function as access-controlled gates
        - Reduced delay time for access
        - Higher risk due to lack of barrier
    - Automated Portals
        - Designed for high-throughput
        - Can include screening technologies
        - Direction sensitive capabilities
        - Can detain violators
- Other Security Measures
    - Fencing Clear Zones
        - Both sides of fence
        - No obstructions
        - Minimal landscape
        - No climbable objects
    - Security Lighting
        - Both sides of gates and fencing is highly recommended
    - Locks
        - Various key technologies available
        - Consider total life cycle costs, not just initial capital cost
    - CCTV Coverage
        - CCTV can be used to enhance detection and/or response
    - Signage
        - Specific requirements are in ASP
        - TSA/FAA-required signage per Advisory Circular 150/5360-12C
        - Deterrent signage
        - Instructional and/or legal signage
        - Coordinate with airport signage policy

**6. Facilities, Areas and Geographical Placement**

When determining the security requirements of all airport facilities, examine the interaction and relationships among the various areas, the types of activity within each area, the flow of public and employee traffic to and through each area, the flow and type of delivery and maintenance traffic, potential needs for and frequency of security escorts, and the manner in which each such area is addressed in the airport's ASP. A facility's placement in relation to the airside/landside boundary, commercial passenger terminal, and regulated security areas will heavily affect what security and access control requirements exist and who has responsibility for security.

a. Aircraft Maintenance Facilities

Aircraft maintenance facilities may be completely landside, completely airside or part of the airside/landside boundary line. As these facilities contain aircraft ramp and/or hangar areas as well as involve public access and supply delivery, their property and/or buildings are typically parts of the airside/landside boundary line and as such require coordination with the airport operator for access control.

Security considerations for aircraft maintenance facility layout and placement include:

- Compliance with 49 CFR 1542
- Prevention of unauthorized access to the aircraft
- Prevention of unauthorized access to and tampering with aircraft parts and equipment
- Non-reliance on large hangar doors/opening as a security boundary/demarcation line
- Location of loading/delivery docks landside

b. Aircraft Movement Areas

By definition, aircraft movement areas (runways, taxiways, aircraft ramps) are completely airside, are required to be within the AOA or secured area, and require security measures per 49 CFR 1542 as well as adherence to appropriate Federal Aviation Regulations (FARs).

Detailed information is contained in *Aircraft Movement Areas* on page 47 under the *Airside* section.

c. Aircraft Rescue and Fire Fighting (ARFF) Facilities

ARFF stations and their equipment are a requirement of 14 CFR 139, Subpart D, Certification and Operations: Land Airports Serving Certain Air Carriers, which is administered by FAA. These facilities are clearly critical to an airport's operations. Typically, even in a multi-station scenario, the primary ARFF station may be located straddling the airside and landside boundary. This positioning may be necessary for a variety of reasons, but public access to the ARFF station may be needed, as well as for mutual aid responders and for ease of landside access to the ARFF station for the fire fighters themselves. However, public access in a multi-station scenario should be limited to the primary ARFF station, not the substation(s).

Positioning of each ARFF station must consider emergency response times and routes. Thus, stations are located for minimum response times to 14 CFR 139 required locations. ARFF vehicles may need landside access for response to landside incidents.

ARFF stations generally include a training classroom that is often used for training airport tenant employees and related activities. If possible, portions of the ARFF station should be accessible without requiring persons to pass though access controls. However, other portions of the ARFF station must be controlled to prevent unauthorized access to the airside.

Similarly, the administrative office area of an ARFF station may be open to public access, enabling persons having business with ARFF officers to access these areas without access control.

In all cases listed for this section, coordinate ARFF facilities with airport staff to determine design direction and resulting operations.

d. Security Operations Center (SOC)/Airport Emergency Command Post (CP)

The title for locations where an airport operates from during normal security operations, as well as during an emergency, event or incident varies by individual airport. Typical titles for facilities where normal security dispatch and operations occur include Security Operations Center (SOC) and Airport Operations Center (AOC). Typical titles for facilities where airport emergency operations occur include Airport Emergency Command Post (CP) and Airport Emergency Operations Center (EOC). For purposes of this document, the standardized terminology SOC and CP shall be used.

When addressing SOC and CP facilities, it should be noted that demand for their use may be for a single or potentially, multiple events happening concurrently. It may also be necessary to address redundant systems, or at least redundancy of primary components installed in a SOC and/or CP, for location in other areas of the airport is it within a terminal or an alternate facility. In addition, links to other government emergency facilities may enhance the operation of an airport's CP.

There are no hard and fast rules for these locations though most are in or attached to the main terminal. In all cases they should be located within a secure area. The designer must be certain to discuss alternative proposed locations with all departments who will use the SOC and/or CP. Indeed, secondary or satellite locations may be valuable for those instances when the primary SOC or CP is out of service. While ease of access to the airside is one primary consideration, there are numerous other concerns such as sufficient operating space for police and other support personnel, central location for access to or dispatch to any point on the airport, technical considerations such as cable routing for all necessary equipment, or support services such as restroom or break room amenities. Considerations for public accessibility should also be considered for SOC facilities based on procedures for such public-related systems and services such as paging, lost and found, or first aid.

For a full discussion on these areas and their contents, see *Security Operations Center* on page 78 and *Airport Emergency Command Post* on page 79 under the *Terminal* section.

e. Airport Personnel Offices

Most personnel and administrative offices typically have landside and/or public access during business hours. During non-business hours they are usually secured, and may be included in the airport's overall access control system, particularly if located within the terminal complex. In addition, some personnel offices, such as airfield maintenance or operations, may be completely airside.

Most airport personnel offices are located in or near the terminal, and are secured (nonpublic) at least part of the time. See *Airport Personnel Offices* on page 76 under the *Terminal Nonpublic Areas* section.

f. Belly Cargo Facility

Belly cargo is carried on passenger aircraft rather than all-cargo or freighter aircraft. Belly cargo facilities share many of the same security requirements as standard cargo areas, and in many airports may be part of one joint cargo facility or area. However, some airports maintain a completely separate area for belly cargo that will be traveling in passenger aircraft rather than cargo planes. One of the primary differences between most dedicated belly cargo facilities and other cargo facilities is that the belly cargo facility may not need to be attached to or adjacent to an aircraft ramp. Since most belly cargo is handled via tugs, a belly cargo facility can be located either adjacent to the terminal where its aircraft operator aircraft are, or at any point along a service roadway which connects to the terminal. A standard cargo facility on the other hand may need to handle aircraft cargo directly where the plane actually pulls up to a fixed or movable loading bridge.

The added flexibility in the location of a belly cargo facility, as well as the fact that it can be separate from the general cargo facility, enables a belly cargo facility to be designed with potentially higher or stricter security levels. Since belly cargo usually involves smaller quantities of public air cargo and U.S. mail, belly cargo facilities can be designed which have the potential for 100% Explosives Detection System (EDS) screening of cargo, and have more flexibility than direct "cargo to plane" operations in that the facility can be either landside or airside and still be isolated from critical passenger aircraft areas. Refer to the *Security Screening* section on page 87 for further information.

A facility for shared cargo screening, including belly cargo and regular cargo, should be considered.

g. All-Cargo Area

A general all-cargo area includes all the ground space and facilities provided for cargo handling. It also includes airport ramps, cargo buildings and warehouses, parking lots and roads associated therewith.

Refer to the *Security Screening* section on page 87 for further information.

h. FAA Airport Traffic Control Tower (ATCT) and Offices

The FAA ATCT and its administrative offices may be located within or adjacent to a terminal complex or in an airside or landside area. ATCT location is dependent upon runway configuration and line of site criteria. ATCT security needs should be addressed by the airport planner and designer such that an interface takes place with FAA security requirements for FAA ATCT design criteria. When the ATCT is in a remote airport location, it may require significant levels of protection as one of an airport's most critical operational facilities. Coordination with the FAA, TSA and the airport is necessary in order to address all ATCT security impacts or requirements to airport operations.

i. Fuel Facilities

Fuel farms are often placed in a remote location of the airport, often with underground hydrant systems feeding fuel to the ramp areas and require attention. Security fences should surround the fuel tanks, and should be access-controlled whenever possible to monitor all movements, including authorized traffic. Where distance precludes hard wiring to the main system, there are wireless technologies as well as freestanding electronic locking mechanisms available. Closed circuit television monitoring, alarms and sensing should be considered in and around fuel farms and storage tanks to alert law enforcement/security personnel of potential intruders or tampering.

j. General Aviation (GA) and Fixed Base Operator (FBO) Areas

GA and FBO areas at commercial passenger airports are airport tenant areas typically consisting of aircraft parking areas, aircraft storage and maintenance hangars, and/or tenant terminal facilities. GA/FBO areas will typically be part of the airside/landside boundary; with aircraft parking areas/ramps located completely airside.

For information on security at non-commercial general aviation airports, see TSA Information Publication (IP) A-001, "Security Guidelines for General Aviation Airports", issued in May 2004. The TSA document is available on the Internet at

*http://www.tsa.gov/interweb/assetlibrary/security_guidelines_for_general_aviation_airports_may_2004_a-001.pdf*

This material should be considered a living document which will be updated and modified as new security enhancements are developed and as input from the industry is received.

Further information is in *General Aviation (GA) Parking Area* on page 47 under the *Airside* section.

k. Ground Service Equipment Maintenance (GSEM) Facility

Many airports today maintain specialized areas for storage and maintenance of ground service equipment (baggage tugs, push-back vehicles, refueling trucks). These areas are often referred to as Ground Service Equipment Maintenance (GSEM) facilities and may also be used to service and maintain other airport and maintenance vehicles. As with other maintenance facilities, these areas may be landside or airside depending upon their needs, and the amount and frequency of landside/airside travel.

As with other service and maintenance areas, particular attention should be paid to material and vehicle parking/storage areas and assuring they do not compromise airside fencing clear zones or security.

l. Ground Transportation Staging Area (GTSA)

A GTSA is a designated area where taxis, limos, buses and other ground transportation vehicles are staged prior to the terminal. By nature, these areas are always landside as it involves public and private off-airport transportation services.

Refer to the *Ground Transportation Staging Area (GTSA)* section on page 52 under *Landside* Facilities.

m. Hotels and On-Airport Accommodations

By nature, hotels and on-airport accommodations are always landside as they are public facilities.

Refer to the *Hotel and On-Airport Accommodations* above under *Landside* Facilities.

n. Industrial/Technology Parks

Industrial/technology Parks may be landside, airside or both. Many airports have land available or in use as industrial/technology parks. Evaluate this land use for security impacts to the airport's operations.

o. In-Flight Catering Facility

On-airport facilities for in-flight catering service may be located landside, airside, or may be a boundary facility with portions of both. Due to the nature of the facility, as well as its typical placement near the passenger terminal, security needs and choices may require substantial amounts of coordination, both architecturally and procedurally. Determination of the security risk involving catering operations should be evaluated in advance of design or construction of these facilities.

p. Intermodal Transportation Area

While *intermodal* transportation areas vary greatly in function and location, they are typically always completely landside facilities. The function of an intermodal transportation area is to transfer passengers or cargo from one mode of transportation to another (i.e., train to plane, bus to plane).

Detailed information is contained in Intermodal Transportation Areas under Landside Facilities.

q. Isolated Security Aircraft Parking Position

The Isolated Security Aircraft Parking Position is a location within the airside used for parking an aircraft when isolation is required due to security or other concerns. This location is subject to special security requirements as identified in the airport's ASP.

Detailed information is contained in *Isolated Security Aircraft Parking Position* on page 48 within the *Airside* section.

r. Military Facilities

Some airports may have adjacent or on-airport military facilities such as Reserve, National Guard or active duty units. Since each of these situations is unique, and since these facilities may be partially airside, or adjacent; detailed coordination between the airport, FAA, TSA, and the military facility must occur for both design and procedure. Typical areas of coordination include access control, identification systems and background check requirements, areas of access, security patrol boundaries, blast protection, security response responsibilities, and joint and/or shared security system data and equipment. Proper coordination should also occur to assure that the security and safety of such military facilities are not compromised by the placement of airport CCTV and access control equipment. See Unified Facilities Criteria UFC 4-010-01 for Department of Defense (DOD) Minimum Anti-Terrorism Standards for buildings used by the military.

s. Navigational & Communications Equipment

Since the placement of navigational and communications equipment is typically driven by functionality, not security, most airports typically have equipment both airside and landside. Where equipment cannot be included within the airside, it should be at a minimum fenced for both safety and security. In addition, electronic monitoring and/or controlling of access to critical equipment may be desirable.

t. Passenger Aircraft Loading/Unloading Parking Areas

Passenger aircraft loading/unloading parking areas are required to be airside and are typically at or near the passenger terminal, are required to be within the secured area, and require security measures per 49 CFR 1542.

Detailed information is contained in Passenger Aircraft Loading/Unloading Parking Areas within Airside.

u. Passenger Aircraft Overnight Parking Areas

Passenger aircraft overnight parking areas are required to be airside and are typically adjacent to the passenger terminal, but may also normally be on a designated ramp located remotely from the terminal. These areas are required to be within the AOA or secured area, and require security measures per 49 CFR 1542.

Detailed information is contained in Passenger Aircraft Overnight Parking Areas within Airside.

v. Rental Car and Vehicle Storage Facilities

Rental car facilities and vehicle storage are usually landside.

See the *Rental Car Storage Areas* section on page 52 under *Landside* Facilities.

w. State/Government Aircraft Facilities

Some airports include areas for non-military government aircraft support facilities. For the most part, these facilities should be given the same considerations as GA/Fixed Base Operator (FBO) areas. However, because of their nature, non-military government aircraft support facilities are typically isolated from other GA/FBO areas and require stricter, and more extensive, security measures. In many cases these areas will have their own, independent security/access control/CCTV system, as well as their own monitoring and security personnel.

x. Terminal Patron Parking Areas

Terminal patron parking areas are public areas and are required to be completely landside. Parking areas are typically at or near the passenger terminal, but may also be located remotely. Security requirements for patron parking areas varies greatly dependent upon the area's proximity to the passenger terminal, security areas and perimeter fencing, and methods used to control entry to the parking areas.

Detailed information is contained in Terminal Patron Parking Areas within Landside.

y. Utilities and Related Equipment

Design and location of utilities and related equipment and service areas should be coordinated with security and fencing design to minimize security risks and vandalism potential. While it is beneficial from a safety and vandalism standpoint to locate utility equipment airside when possible, maintenance contracts, and service personnel identification media issuance and access may require utilities to be landside. Special emphasis should be given to aboveground electrical substations.

Where underground service ducts, storm drains, sewers, tunnels, air ducts, trash chutes, drainage structures, and other openings provide access to the airside or other restricted area, security treatments such as bars, grates, padlock, or other effective means may be required to meet practical maximum opening size requirements. For structures or openings that involve water flow, consider in the security treatment design the direction of flow, type, and size of potential debris, and frequency and method of maintenance access required for debris removal, as well as the potential for flood and/or erosion during heavy flow/debris periods.

## Section III-A-6 - Facilities, Areas and Geographical Placement Checklist

- ☐ **Facility Placement Considerations:**
  - Interaction and relationships among areas
  - Types of activity within each area
  - Flow of public/employees to/through areas
  - Flow and type of delivery traffic
  - Flow and type of maintenance traffic
  - Need for and frequency of security escorts
  - How each area is addressed in the ASP
- ☐ **Each Airport is Unique**
- ☐ **Facilities:**
  - Aircraft Maintenance Facilities
    - Airside, Landside or Both
    - Security the responsibility of the facility
  - Aircraft Movement Areas
    - Airside
    - Requires controlled access
  - Passenger Aircraft Overnight Parking Area
    - Airside
    - Requires controlled access
  - ARFF Facilities
    - Either Airside or Both
    - Consider response routes and times
    - Facility may require public access
  - SOC/CP
    - Secure location
    - Consider alternate/back-up locations
    - Ease of airside access
    - Sufficient operating space for personnel
    - Central location for dispatching
    - See Terminal Nonpublic Areas Checklist
  - Airport Personnel Offices
    - Airside, Landside or Both
    - Consider security needs
    - See Terminal Nonpublic Areas Checklist
  - Belly Cargo Facility
    - Airside, Landside or Both
    - Flexible Placement
    - Terminal Access (via roads) required
    - Consider cargo screening needs
  - Cargo Area
    - Typically Airside or Both
    - Screening and inspection needs
    - Secure cargo-holding area
    - Postal facility inclusion possible
    - Doors must be lockable and controlled
    - Consider fence protection measures
  - FAA ATCT and Offices
    - Landside or Airside
    - May require airport security controls
  - Fuel Area
    - Landside or Airside
    - Typically remote from terminal
    - Safety and security fencing required
    - Consider access controls to area
  - GA Areas
    - Typically Airside on Both
    - Boundaries based on function
  - GSEM Facility
    - Landside or Airside
    - Consider airside travel frequency
    - Maintain fencing clear zones
  - GTSA
    - Landside
    - Public Safety and Security Concerns
  - Hotels and On-Airport Accommodations
    - Landside
    - Public Safety and Security Concerns
  - Industrial/Technology Parks
    - Landside, Airside or Both
  - In-Flight Catering Facility
    - Landside, Airside or Both
    - Typically adjacent to terminal
  - Intermodal Transportation Area
    - Typically Landside
  - Military Facilities
    - Substantial coordination required
  - Navigation and Communications Equipment
    - Airside and Landside
    - Driven by functionality
    - Control access to critical equipment
  - Rental Car Facilities
    - Landside
    - Public Safety and Security Concerns
  - State/Government Aircraft Facilities
    - Both airside and landside
    - Security typically independent
    - Coordinate security requirements
  - Utilities and Related Equipment
    - Locate airside when possible
    - Control access
    - Secure access points and equipment

13. MAC Agency Directive AD-001a, November 14, 2001

# *The Commonwealth of Massachusetts*
## AERONAUTICS COMMISSION
## AGENCY DIRECTIVE

Date: 11/14/2001

**TITLE:** AIRPORT SECURITY — MAC AD – 001a

**PURPOSE.** The purpose of this DIRECTIVE is to establish minimum airport security standards for public-use airports located in the Commonwealth of Massachusetts. This DIRECTIVE also provides guidance to airport sponsors for implementing the security standards recommended herein.

**APPLICABILITY.** This DIRECTIVE applies to all public-use airports located in the Commonwealth of Massachusetts. However it is not intended to replace or supercede airport security standards required by the FAA under FAR Part 107 or airline security standards required by FAR Part 108. Therefore, any part of this DIRECTIVE found to be inconsistent with, or contrary to, the security standards required by the FAA shall be deemed inapplicable.

**CANCELLATION.** This DIRECTIVE hereby cancels and replaces the emergency DIRECTIVE, dated October 2, 2001 titled "*Implementation of Airport Security Measures*" that was issued by the Commission under emergency conditions in response to the September 11th terrorist attacks.

**BACKGROUND.** On September 11, 2001, the United States of America experienced a series of terrorist attacks that involved the mid-air highjacking and subsequent destruction of four commercial passenger jets, their occupants, and nearly 5,000 people on the ground. Most horrific of all was the intentional use of the airplanes as weapons.

All four planes involved in the attacks originated from major air carrier airports subject to FAA security regulations. In the immediate wake of the terrorist attacks, government regulators and airport professionals alike assessed the vulnerability of airport security across the country. Sensitive to the fact that aircraft were used as weapons, the Massachusetts Aeronautics Commission issued the initial DIRECTIVE on October 2, 2001.

**DEFINITIONS.** The following terms used in this document shall be defined as follows:

*AOA* shall mean Aircraft Operating Area
*Commission* shall mean the Massachusetts Aeronautics Commission
*DIRECTIVE* shall mean this AGENCY DIRECTIVE
*FAA* shall mean the Federal Aviation Administration
*FAR* shall mean Federal Aviation Regulation
*FBO* shall mean Fixed Base Operator
*FDA* shall mean the federal Food and Drug Administration
*GA* shall mean General Aviation, referring to a type of airport or operational characteristic
*Restricted area* shall mean any area designated on the airport security plan as requiring ID card access
*Sponsor* shall mean the legal owner and/or operator of a public-use airport
*Tenant* shall mean any person or legal entity to receive written permission to establish a leasehold at the airport

---

### 1. AIRPORT CLASSIFICATION

The public-use airports in Massachusetts range in size from small rural GA facilities with only a few based aircraft operating under visual flight rule conditions to large commercial service airports accommodating jet aircraft operating in all-weather flight conditions. It is generally accepted that small airports which can only accommodate single-engine aircraft pose much less of a security risk than large airports offering scheduled airline passenger service using jet aircraft. Recognizing the difficulty of developing one standard to suit all airports, the following airport categories are defined to accommodate the varied level of (security) risk posed by each facility.

**Class 1** – Airports with scheduled airline passenger service
**Class 2** – Municipally owned airports without scheduled airline passenger service
**Class 3** – Privately owned airports

The above-noted airport classifications will be referenced throughout this DIRECTIVE, and minimum security standards will be developed, and shall be enforced, for each classification.

## 2. SECURITY STANDARDS

Regardless of the size or operational characteristics of a particular facility, the Commission hereby directs that all public-use airport sponsors in Massachusetts adopt reasonable security standards to (a) monitor and protect airport users and airport property including buildings, facilities and equipment, (b) control the movement of persons and ground vehicles on airport property, especially in the AOA, (c) prevent unauthorized access of persons and ground vehicles into unauthorized areas on airport property, especially into the AOA, (d) detect and prevent unauthorized deadly or dangerous weapons or devices from being transferred into the AOA or onto aircraft, and (e) prevent the theft and subsequent illegal operation of aircraft.

**The following guidance applies to Class 1, 2 and 3 Airports except as noted below:**

a. **Monitoring & Protecting Airport Users and Property.** Airport sponsors shall take reasonable measures to monitor and protect airport users, visitors and guests, and airport property including buildings, facilities and equipment. Depending on the class of airport, reasonable measures may include the following:

   i) Installation of security fencing to protect against inadvertent or unauthorized access to the AOA.
   ii) Closing vehicular and pedestrian gates leading into the AOA and locking them when not in use.
   iii) Installing access control devices on gates to manage and control the movement of people into the AOA.
   iv) Periodically changing access codes and locks to vehicular and pedestrian gates leading into the AOA.
   v) Installing locks on fuel cabinets, fill hatches and pumps, and power shutoff switches on fueling facilities.
   vi) Installing locks on airfield electrical vaults and other electrical systems, including (non-FAA) NAVAIDS.
   vii) Installing barriers to protect fueling facilities, HazMat storage areas and other areas of concern.
   viii) Installing sufficient outside lighting fixtures to illuminate buildings, walkways, aircraft ramps and aprons.
   ix) Monitoring airport property by performing regular inspections, and by means of video surveillance if warranted.
   x) Requesting periodic inspections / patrols of the airport by local law enforcement officers.
   xi) If warranted, employment of local law enforcement officers on a regular or part time basis.
   xii) Developing an airport security plan and updating the plan periodically.
   xiii) Requiring tenants to develop their own security plan and to comply with the sponsor's airport security plan.

   **EXCEPTIONS:** None.

b. **Controlling Movement on the Airport.** Airport sponsors shall take reasonable steps to control the movement of persons, aircraft and ground vehicles on airport property by installing airport user signs, aircraft guidance signs, airfield lights and markers, and pavement markings, as appropriate. Airport sponsors shall:

   i) Manage and operate their airport facility in a safe and efficient manner pursuant to all laws, rules, regulations, directives, orders and advisories of applicable federal, state and local authorities. To this end, sponsors are expected to utilize an adequate number of people to control and direct the movement of people, aircraft and ground vehicles on airport property including airside and landside. This may be accomplished by any combination of qualified airport staff, lease or contract employees, or volunteer staff.
   ii) Install signs to direct the movement of people and inform patrons of pertinent information regarding the safe and efficient use and operation of the facility. This may include, but is not limited to, parking and directional signs, informational signs, do-not-enter signs, warning signs, etc. Whatever the sign type, it should communicate the proper message to the appropriate party at the right time and place.
   iii) Install airfield guidance signs and airfield lights and markers, as appropriate, to direct and control the movement of aircraft and ground vehicles within the AOA. The installation and operation of airfield guidance signs and airfield lights and markers should be accomplished pursuant to applicable FAA standards.
   iv) Install pavement markings to direct and control the movement of aircraft and ground vehicles on airport property. The installation of pavement markings in the AOA and elsewhere on the airfield should be accomplished pursuant to applicable FAA standards. Pavement markings used to control ground vehicles that operate on airport property but off the airfield should meet applicable Highway Dept. standards.

   **EXCEPTIONS:** As noted below.

   iii) Aircraft guidance signs and airfield lights/markers should be installed at Class 3 Airports as funding permits. Aircraft guidance signs and airfield lights/markers are not required for Class 3 Airports that possess a MAC issued Airport Operating Certificate with the following limitation(s): *Day VFR Only*.

c. **Preventing Unauthorized Access.** Airport sponsors shall take necessary steps to prevent unauthorized access of persons and ground vehicles into unauthorized areas on airport property. This includes, among other things, preventing unauthorized access into the AOA, moving between areas within the AOA, and separating / segregating

persons and ground vehicles from aircraft, fueling facilities, and other areas of concern within the AOA. Airport sponsors shall:

i) Install security fencing, and access gates where appropriate, to enclose the AOA and to protect other sensitive areas on airport property including all fuel farms and HazMat storage areas. Whenever possible, the sponsor should enclose fuel farms with sufficient fencing to include parking spaces for all fuel trucks. Until such time as the entire AOA is enclosed, priority should be given to areas where easy public access to the AOA is of most concern, spanning open areas with fence and using terrain, existing vegetative cover and environmental conditions as natural barriers. Fencing specifications should meet the following standard: eight foot chain-link-fence, black vinyl-coated, with one foot of barbed wire on top, installed per manufacturer's recommendations. Barbed wire is not recommended for fencing located in the immediate vicinity of the airport terminal building. The location and height of fencing should not violate applicable airspace standards or negate airport master plan improvements. Security fencing should receive high priority in an airport's Capital Improvement Plan.

ii) Discourage unnecessary pedestrian and vehicular access to, and movement within, the AOA. For example, aircraft owners should park their cars outside the AOA and walk to their planes.

iii) Restrict pedestrian and vehicular access into the AOA to as few locations as possible, balancing the need for access by emergency, safety and maintenance personnel inside and outside the AOA.

iv) Install access control devices (e.g. card readers, mechanical pin latch mechanisms, etc.) on fence gates leading into the AOA, where appropriate.

v) Install video surveillance & detection equipment. The Commission recommends installing video cameras to monitor access gates leading into the AOA, where appropriate. Class 1 airports should also consider installing video cameras to monitor areas in the terminal building, where appropriate.

vi) Install heavy-duty barriers to protect fuel farm areas and other areas of special concern from inadvertent or deliberate damage by ground vehicles or aircraft. Concrete bollards are the preferred method for protecting above ground fueling facilities. Any combination of jersey barriers, concrete blocks, large boulders, telephone poles and heavy duty chains may also suffice for protecting or blocking access to other areas of concern.

vii) Require the use of identification (ID) badges for allowing access to anyone wishing to enter the AOA and for controlling the movement of persons within the AOA. Sponsors shall also implement procedures for challenging persons who are not displaying the proper identification. Any person authorized to enter the AOA or move within the AOA shall display a standard ID badge with sufficient information to clearly identify the individual and ascertain the level of security authorization. Anyone without the proper identification must be escorted at all times while in restricted areas of the AOA by another person with the proper ID badge.

Applications for ID badges should be submitted to the Commission by December 31, 2001. With approval from the Commission, sponsors may develop their own distinct ID badge format. Upon request, the Commission will supply each airport sponsor with a sufficient number of ID badges for use at their facility, at no cost to the sponsor.

**EXCEPTIONS:** As noted below.

i) Other types of fencing may be substituted for standard security fencing recommended by the Commission. Examples of this include the use of wooden or plastic fencing within the critical area of a NAVAID facility, or the use of wildlife fencing required by environmental regulators to allow for the migration of small mammals.

Class 3 airports are exempt from the standard specification for eight-foot chain-link-fence with barbed wire due to the length of the runway, size of the aircraft and type of operation at these facilities. Instead, the Commission recommends that Class 3 airports install four foot fencing, either: black vinyl-coated chain-link-fence, wooden fencing (post & rail, split rail, etc.) or some other type of low-profile fencing that is functional (i.e. prevents unauthorized vehicular access into the AOA) but not too obtrusive.

iv) Class 3 airports are exempt from this requirement. Class 2 airports should comply as funding permits.

v) Class 2 and 3 airports are exempt from this requirement, however Class 2 airports are encouraged to comply.

vii) Operators of transient aircraft and their guests are not expected, and thus not required, to possess the standard ID badge. Nevertheless, the requirement for escorting unidentified individuals while in the AOA still applies.

Notwithstanding the requirement to possess and display the proper ID Badge to enter and move about within the AOA, the sponsor may authorize unescorted access to the following individuals: an employee of federal and state government agencies including the FAA and the Commission who, by job function, are required to work inside the AOA.

d. **Detecting and Preventing Weapons into the AOA.** The FAA imposes federal screening requirements on certain airlines under FAR Part 108 titled "Airplane Operator Security". More specifically, FAR Part 108 applies to the operations of holders of FAA air carrier operating certificates or operating certificates engaging in scheduled passenger operations or public charter passenger operations. Notwithstanding FAA security requirements on airports under FAR Part 107 or airlines under FAR Part 108, the Commission recommends that Class 1 airports take reasonable measures to detect and prevent the transfer of unauthorized deadly or dangerous weapons or devices into the AOA or onto aircraft carrying ticketed passengers for all regularly scheduled airline flights. Accordingly, the Commission recommends that Class 1 airports voluntarily screen all passengers, all checked baggage and all carry-on baggage for every person intending to board a regularly scheduled airline flight.

**In lieu of any federal screening requirements for Class 1 Airports that are not subject to FAR Part 107, the Commission offers the following guidance for consideration:**

i) Electronic metal detection equipment and cabinet X-ray machines should be installed for detecting unauthorized guns, knives and other deadly or dangerous weapons being carried by any person prior to entering the AOA in advance of boarding a departing aircraft of a regularly scheduled airline flight. Only equipment approved by the FDA for this intended use should be installed. The sponsor should assure that such equipment meets or exceeds the current standards for installation, operation and performance established by the FDA. The equipment should be subject to regular testing in order to maintain operational and performance standards set by the FDA. All records of installation and testing should be made available for inspection by the Commission, the FAA and the FDA.

ii) The sponsor should develop a program for initial and recurrent training of staff responsible for the safe, efficient and proper use and operation of the screening equipment.

iii) Appropriate signage should be conspicuously located to notify the general public of screening operations.

iv) A local law enforcement officer should be stationed at all screening check points to monitor and assist airport security personnel during the screening process.

v) All baggage, whether carried on board by crewmembers or passengers or destined for storage as cargo, should be screened by electronic means for detecting unauthorized guns, knives and other deadly or dangerous weapons prior to entering sterile passenger holding areas or the AOA.

vi) All crewmembers and passengers of a departing (scheduled airline) aircraft should be subject to metal detection screening, questioning, and to bodily search if necessary, for reasonable cause or suspicion of attempting to transfer an unauthorized deadly or dangerous weapon into the AOA or onto the aircraft.

vii) All unauthorized guns, knives and other deadly or dangerous weapons found on a person or in baggage should be confiscated by the local law enforcement officer stationed at the screening checkpoint. Airport security personnel shall complete a detailed log of information about the confiscation including the location, date and time of the event, the person's name, address and phone number, and a detailed description of the confiscated weapon. A copy of the event log shall be supplied to any of the following representatives upon written request: the Commission, the FAA or any federal, state or local law enforcement official.

viii) Any person refusing to consent to the sponsor's screening program should be refused permission to enter the AOA and to board any departing aircraft. If such an event occurs, airport security personnel should complete a detailed log of the event. If warranted, local police should be called for assistance.

ix) Boarding procedures should be established for segregating screened passengers from those who have not been screened so as to keep screened passengers isolated in a sterile environment while waiting to board, and during boarding, a departing aircraft.

x) Airport sponsors should implement other security screening procedures and systems that they believe are necessary for detecting unauthorized deadly or dangerous weapons being carried by any person prior to entering the AOA through airline passenger screening check points in advance of boarding a departing aircraft.

**EXCEPTIONS:** As noted below.

i-x) Class 2 and 3 airports are exempt (by definition) from this requirement.

vii) Law enforcement officers, government officials and other individuals possessing legal authorization to carry guns or other weapons are exempt from confiscation but shall notify airport security personnel in advance of passing through screening procedures.

e. **Preventing Theft and Illegal Operation of Aircraft.** Airport sponsors shall require that all based aircraft owners take reasonable measures of preventing the theft and illegal operation of their aircraft. Consider the following:

i) Aircraft owners should install anti-theft devices on their aircraft when not in use.

ii) Aircraft owners should install devices to lock aircraft flight control surfaces when not in use.

iii) Aircraft owners should remove the keys to their aircraft, if applicable, and lock all doors when not in use.

iv) Aircraft owners should consider lockable devices to secure their aircraft.
v) Doors on aircraft storage hangars should be kept locked at all times when not in use.
vi) Aircraft owners and pilots should report suspicious activity to airport management or other authorities.
vii) Airport sponsors and tenants should install sufficient lighting equipment to illuminate aircraft ramps and aprons.

**EXCEPTIONS:** None.

## 3. AIRPORT SECURITY PLANS

The Commission hereby directs that all public-use airport sponsors in Massachusetts create an *Airport Security Plan* incorporating the applicable security standards noted in Section 2 above. However, creating and implementing such a plan will take a team effort, requiring a lot of coordination and cooperation of local, state and federal authorities as well as private end users. Therefore the Commission also directs that sponsors assemble an *Airport Security Team* to advise the sponsor in developing its *Airport Security Plan*.

a. **Airport Security Team**. Sponsors shall assemble an Airport Security Team (AST). The AST should be made up of representatives from the airport, airport tenants and users including based aircraft owners, local public safety officials (police, fire, etc.), local emergency management personnel, and representation of other appropriate parties. The purpose of the AST is to advise the sponsor regarding issues to consider in planning for security improvements. Good communication and cooperation between all parties is essential for balancing the desire for public access and utility against the need for public safety and security. The AST shall:

i) List and clearly define the different types of airport users. The list may include airlines, FBOs, maintenance facilities, fueling operators, flight schools, based aircraft owners, restaurants, etc. Based aircraft owners can be considered as a user group.
ii) Document the hours of operation for each user listed above. Aircraft owners can be considered as one group.
iii) Discuss the access requirements for each specific user, with particular emphasis on those that require access to the AOA. Access to the AOA by employees, visitors and guests, and mail & package delivery requirements should be discussed in detail.
iv) Discuss the security requirements for each user. Aircraft owners can be considered as a group.
v) Discuss emergency response issues.
vi) Advise the sponsor on all security requirements recommended for inclusion on the Airport Security Plan.

b. **Airport Security Plan**. Based on input from the Airport Security Team, Sponsors shall create an Airport Security Plan that incorporates the applicable security standards and guidance provided in this DIRECTIVE. This requirement is not intended to replace any such requirement promulgated by the FAA or other federal authority. In fact, FAA mandated security plans may be substituted for this state requirement, however these airports are still encouraged to create an Airport Security Team to advise airport management on airport security issues.

The airport sponsor shall develop a written Airport Security Plan pursuant to the following guidance:

i) Reference the list of airport users developed by the AST. Review it for accuracy, update as necessary, and incorporate the list into the plan. The list should include every based aircraft owner. Briefly describe the type of operation for each user. Special consideration should be given to agricultural spraying operations, aerial demonstrations, blimp operations, banner towers and site-seeing operations.
ii) Document the normal hours of operation for each user listed above.
iii) Document the location and access requirements for each specific user, with particular emphasis on those that require access to the AOA. Incorporating a scaled airport map may be helpful. Aircraft owners can be located by apron or hangar in lieu of showing each one individually.
iv) Document the security requirements for each user. Aircraft owners can be considered as a group.
v) Document the likely AOA access points for each user.
vi) Incorporate the security standards and applicable guidance from Section 2.
vii) Incorporate procedures for reporting suspicious activity from Section 4.
viii) Incorporate emergency response considerations recommended by the AST and from Section 5.
ix) Periodically review the plan, consulting with the AST, and update as necessary.

Given the sensitive nature of this issue, the Commission advises against distribution, disclosure and availability of any sensitive information that could compromise airport security. The sponsor should consider seeking legal advice regarding applicable public disclosure laws.

## 4. REPORTING SUSPICIOUS ACTIVITY

Airport sponsors shall implement procedures for reporting unusual or suspicious activity to the proper authorities:

a. Develop a list of unusual or suspicious activity that warrants particular attention, such as:

   i) Aircraft with unusual or unauthorized modifications.
   ii) Persons loitering for extended periods of time in the vicinity of parked aircraft or elsewhere in the AOA.
   iii) Pilots who appear to be under the control of other persons.
   iv) Persons wishing to obtain aircraft without presenting proper credentials or persons who present apparently valid credentials but do not have a corresponding level of aviation knowledge.
   v) Witnessing deadly or dangerous weapons or explosives being loaded onto an aircraft.
   vi) Anything that doesn't look right such as events or circumstances that does not fit the pattern of normal lawful activity at the airport.

b. Include the following 24 hour phone numbers on their contact list:

   i) Airport Manager..... (###) ###-####
   ii) Local Police Department.....(###) ###-####
   iii) Massachusetts State Police Headquarters.....(508) 820-2121
   iv) Massachusetts Aeronautics Commission.....(508) 301-2118
   v) Federal Bureau of Investigation (FBI), Boston Field Office.....(617) 742-5533
   vi) FAA, Regional Command Center.....(781) 238-7001

c. Develop a process to facilitate determining whom to call.

d. Add any other appropriate contact numbers to the list.

e. Circulate these reporting procedures to all tenants and others who have a regular presence on the airport.

f. Encourage all tenants and based aircraft owners to comply with the sponsor's reporting procedures.

## 5. EMERGENCY RESPONSE PROCEDURES

Airport sponsors shall develop and implement emergency procedures to respond to regional disasters, acts of terrorism, and other situations deemed to be an emergency by state or federal authorities. Airport sponsors shall:

a. Develop a list of reasonably potential emergency situations that could involve the airport either directly or indirectly.

b. Address ways to adequately respond to each emergency situation noted above, including the development of a "communication tree" for prioritizing the proper authorities to contact in emergency situations.

c. Designate a primary (airport) respondent and two alternates to respond to emergency situations at the airport.

d. Maintain a list of contact data for all designated respondents and other potential persons likely to be involved in emergency situations including their names, various phone numbers (home, work, cell, pager, etc.), fax numbers and email addresses.

e. Share the information noted above with the Commission, FAA, MEMA (Massachusetts Emergency Management Agency), and other local, state and federal authorities as necessary.

f. Periodically review the procedures noted above and update as necessary.

## 6. STATE FUNDING OF AIRPORT SECURITY IMPROVEMENTS

The Commission considers airport security to be a high priority objective. Eligibility for state funding assistance will be subject to an approved *Airport Security Plan* consistent with the guidance contained herein.

Robert J. Mullen

Executive Director, *Massachusetts Aeronautics Commission*

14. AC 150/5320-6D, Chapter 3, Paragraph 302a

# CHAPTER 3. PAVEMENT DESIGN

## SECTION 1. DESIGN CONSIDERATIONS

**300. SCOPE.** This chapter covers pavement design for airports serving aircraft with gross weights of 30,000 pounds (13 000 kg) or more. Chapter 5 is devoted to the design of pavements serving lighter aircraft with gross weights under 30,000 pounds (13 000 kg).

**301. DESIGN PHILOSOPHY.** The FAA policy of treating the design of aircraft landing gear and the design and evaluation of airport pavements as three separate entities is described in the Foreword to this advisory circular. The design of airport pavements is a complex engineering problem which involves a large number of interacting variables. The design curves presented in this chapter are based on the CBR method of design for flexible pavements and a jointed edge stress analysis for rigid pavements. Other design procedures such as those based on layered elastic analysis and those developed by The Asphalt Institute and the Portland Cement Association may be utilized to determine pavement thicknesses when approved by the FAA. These procedures will yield slightly different design thicknesses due to different basic assumptions. All pavement designs should be summarized on FAA Form 5100-1, Airport Pavement Design, which is considered to be part of the Engineer's Report. An Engineer's Report should be prepared for FAA review and approval along with initial plans and specifications. Because of thickness variations, the evaluation of existing pavements should be performed using the same method as was employed in the design. Procedures to be used in evaluating pavements are described in detail in Chapter 6 of this advisory circular. Details on the development of the FAA method of design are as follows:

a. **Flexible Pavements.** The flexible pavement design curves presented in this chapter are based on the California Bearing Ratio (CBR) method of design. The CBR design method is basically empirical; however, a great deal of research has been done with the method and reliable correlations have been developed. Gear configurations are related using theoretical concepts as well as empirically developed data. The design curves provide the required total thickness of flexible pavement (surface, base, and subbase) needed to support a given weight of aircraft over a particular subgrade. The curves also show the required surface thickness. Minimum base course thicknesses are given in a separate table. A more detailed discussion of CBR design is presented in Appendix 2.

b. **Rigid Pavements.** The rigid pavement design curves in this chapter are based on the Westergaard analysis of edge loaded slabs. The edge loading analysis has been modified to simulate a jointed edge condition. Pavement stresses are higher at the jointed edge than at the slab interior. Experience shows practically all load induced cracks develop at jointed edges and migrate toward the slab interior. Design curves are furnished for areas where traffic will predominantly follow parallel or perpendicular to joints and for areas where traffic is likely to cross joints at an acute angle. The thickness of pavement determined from the curves is for slab thickness only. Subbase thicknesses are determined separately. A more detailed discussion of the basis for rigid pavement design is presented in Appendix 2.

**302. BACKGROUND.** An airfield pavement and the operating aircraft represent an interactive system which must be addressed in the pavement design process. Design considerations associated with both the aircraft and the pavement must be recognized in order to produce a satisfactory design. Careful construction control and some degree of maintenance will be required to produce a pavement which will achieve the intended design life. Pavements are designed to provide a finite life and fatigue limits are anticipated. Poor construction and lack of preventative maintenance will usually shorten the service life of even the best designed pavement.

a. **Variables.** The determination of pavement thickness requirements is a complex engineering problem. Pavements are subject to a wide variety of loadings and climatic effects. The design process involves a large number of interacting variables which are often difficult to quantify. Although a great deal of research work has been completed and more is underway, it has been impossible to arrive at a direct mathematical solution of thickness requirements. For this reason the determination of pavement thickness must be based on the theoretical analysis of load distribution through pavements and soils, the analysis of experimental pavement data, and a study of the performance of pavements under actual service conditions. Pavement thickness curves presented in this chapter have been developed through correlation of the data obtained from these sources. Pavements designed in accordance with these standards are intended to provide a structural life of 20 years that is free of major maintenance if no major changes in forecast traffic are encountered. It is

likely that rehabilitation of surface grades and renewal of skid resistant properties will be needed before 20 years due to destructive climatic effects and deteriorating effects of normal usage.

b. **Structural Design.** The structural design of airport pavements consists of determining both the overall pavement thickness and the thickness of the component parts of the pavement. There are a number of factors which influence the thickness of pavement required to provide satisfactory service. These include the magnitude and character of the aircraft loads to be supported, the volume of traffic, the concentration of traffic in certain areas, and the quality of the subgrade soil and materials comprising the pavement structure.

**303. AIRCRAFT CONSIDERATIONS.**

a. **Load.** The pavement design method is based on the gross weight of the aircraft. For design purposes the pavement should be designed for the maximum anticipated takeoff weight of the aircraft. The design procedure assumes 95 percent of the gross weight is carried by the main landing gears and 5 percent is carried by the nose gear. AC 150/5300-13, Airport Design, lists the weight of nearly all civil aircraft. Use of the maximum anticipated takeoff weight is recommended to provide some degree of conservatism in the design and is justified by the fact that changes in operational use can often occur and recognition of the fact that forecast traffic is approximate at best. By ignoring arriving traffic some of the conservatism is offset.

b. **Landing Gear Type and Geometry.** The gear type and configuration dictate how the aircraft weight is distributed to the pavement and determine pavement response to aircraft loadings. It would have been impractical to develop design curves for each type of aircraft. However, since the thickness of both rigid and flexible pavements is dependent upon the gear dimensions and the type of gear, separate design curves would be necessary unless some valid assumptions could be made to reduce the number of variables. Examination of gear configuration, tire contact areas, and tire pressure in common use indicated that these follow a definite trend related to aircraft gross weight. Reasonable assumptions could therefore be made and design curves constructed from the assumed data. These assumed data are as follows:

(1) **Single Gear Aircraft.** No special assumptions needed.

(2) **Dual Gear Aircraft.** A study of the spacing between dual wheels for these aircraft indicated that a dimension of 20 inches (0.5 1 m) between the centerline of the tires appeared reasonable for the lighter aircraft and a dimension of 34 inches (0.86 m) between the centerline of the tires appeared reasonable for the heavier aircraft.

(3) **Dual Tandem Gear Aircraft.** The study indicated a dual wheel spacing of 20 inches (0.51 m) and a tandem spacing of 45 inches (1.14 m) for lighter aircraft, and a dual wheel spacing of 30 inches (0.76 m) and a tandem spacing of 55 inches (1.40 m) for the heavier aircraft are appropriate design values.

(4) **Wide Body Aircraft.** Wide body aircraft; i.e., B-747, DC-10, and L-101 1 represent a radical departure from the geometry assumed for dual tandem aircraft described in paragraph (c) above. Due to the large differences in gross weights and gear geometries, separate design curves have been prepared for the wide body aircraft.

c. **Tire Pressure.** Tire pressure varies between 75 and 200 PSI (516 to 1 380 kPa) depending on gear configuration and gross weight. It should be noted that tire pressure asserts less influence on pavement stresses as gross weight increases, and the assumed maximum of 200 PSI (1 380 kPa) may be safely exceeded if other parameters are not exceeded and a high stability surface course is used.

d. **Traffic Volume.** Forecasts of annual departures by aircraft type are needed for pavement design. Information on aircraft operations is available from Airport Master Plans, Terminal Area Forecasts, the National Plan of Integrated Airport Systems, Airport Activity Statistics and FAA Air Traffic Activity. These publications should be consulted in the development of forecasts of annual departures by aircraft type.

**304. DETERMINATION OF DESIGN AIRCRAFT.** The forecast of annual departures by aircraft type will result in a list of a number of different aircraft. The design aircraft should be selected on the basis of the one requiring the

15. 49CFR Part 1542.103(14) and Part 1544

(4) Includes an index organized in the same subject area sequence as § 1542.103; and

(5) Has been approved by TSA.

(b) The airport operator must maintain one current and complete copy of its security program and provide a copy to TSA upon request.

(c) Each airport operator must—

(1) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know; and

(2) Refer all requests for SSI by other persons to TSA.

**§ 1542.103 Content.**

(a) *Complete program.* Except as otherwise approved by TSA, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(1) or § 1546.101(a) of this chapter, must include in its security program the following:

(1) The name, means of contact, duties, and training requirements of the ASC required under § 1542.3.

(2) [Reserved]

(3) A description of the secured areas, including—

(i) A description and map detailing boundaries and pertinent features;

(ii) Each activity or entity on, or adjacent to, a secured area that affects security;

(iii) Measures used to perform the access control functions required under § 1542.201(b)(1);

(iv) Procedures to control movement within the secured area, including identification media required under § 1542.201(b)(3); and

(v) A description of the notification signs required under § 1542.201(b)(6).

(4) A description of the AOA, including—

(i) A description and map detailing boundaries, and pertinent features;

(ii) Each activity or entity on, or adjacent to, an AOA that affects security;

(iii) Measures used to perform the access control functions required under § 1542.203(b)(1);

(iv) Measures to control movement within the AOA, including identification media as appropriate; and

(v) A description of the notification signs required under § 1542.203(b)(4).

(5) A description of the SIDA's, including—

(i) A description and map detailing boundaries and pertinent features; and

(ii) Each activity or entity on, or adjacent to, a SIDA.

(6) A description of the sterile areas, including—

(i) A diagram with dimensions detailing boundaries and pertinent features;

(ii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and

(iii) Measures used to control access as specified in § 1542.207.

(7) Procedures used to comply with § 1542.209 regarding fingerprint-based criminal history records checks.

(8) A description of the personnel identification systems as described in § 1542.211.

(9) Escort procedures in accordance with § 1542.211(e).

(10) Challenge procedures in accordance with § 1542.211(d).

(11) Training programs required under §§ 1542.213 and 1542.217(c)(2), if applicable.

(12) A description of law enforcement support used to comply with § 1542.215(a).

(13) A system for maintaining the records described in § 1542.221.

(14) The procedures and a description of facilities and equipment used to support TSA inspection of individuals and property, and aircraft operator or foreign air carrier screening functions of parts 1544 and 1546 of this chapter.

(15) A contingency plan required under § 1542.301.

(16) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(17) Procedures for posting of public advisories as specified in § 1542.305.

(18) Incident management procedures used to comply with § 1542.307.

(19) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions.

(20) Each exclusive area agreement as specified in § 1542.111.

(21) Each airport tenant security program as specified in § 1542.113.

(b) *Supporting program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(2) or (f), or § 1546.101(b) or (c) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC, as required under § 1542.3.

(2) A description of the law enforcement support used to comply with § 1542.215(a).

(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 1542.221.

(5) The contingency plan required under § 1542.301.

(6) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(7) Procedures for public advisories as specified in § 1542.305.

(8) Incident management procedures used to comply with § 1542.307.

(c) *Partial program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(b) or § 1546.101(d) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC as required under § 1542.3.

(2) A description of the law enforcement support used to comply with § 1542.215(b).

(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 1542.221.

(5) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(6) Procedures for public advisories as specified in § 1542.305.

(7) Incident management procedures used to comply with § 1542.307.

(d) *Use of appendices.* The airport operator may comply with paragraphs (a), (b), and (c) of this section by including in its security program, as an appendix, any document that contains the information required by paragraphs (a), (b), and (c) of this section. The appendix must be referenced in the corresponding section(s) of the security program.

**§ 1542.105 Approval and amendments.**

(a) *Initial approval of security program.* Unless otherwise authorized by the designated official, each airport operator required to have a security program under this part must submit its initial proposed security program to the designated official for approval at least 90 days before the date any aircraft operator or foreign air carrier required to have a security program under part 1544 or part 1546 of this chapter is expected to begin operations. Such requests will be processed as follows:

(1) The designated official, within 30 days after receiving the proposed security program, will either approve the program or give the airport operator written notice to modify the program to comply with the applicable requirements of this part.

(2) The airport operator may either submit a modified security program to the designated official for approval, or petition the Administrator to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.

(3) The designated official, upon receipt of a petition for reconsideration, either amends or withdraws the notice, or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the notice to modify, or by affirming the notice to modify.

(b) *Amendment requested by an airport operator.* Except as provided in

(2) Refer all requests for SSI by other persons to TSA.

**§ 1542.103 Content.**

(a) *Complete program.* Except as otherwise approved by TSA, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(1) or § 1546.101(a) of this chapter, must include in its security program the following:

(1) The name, means of contact, duties, and training requirements of the ASC required under § 1542.3.

(2) [Reserved]

(3) A description of the secured areas, including—

(i) A description and map detailing boundaries and pertinent features;

(ii) Each activity or entity on, or adjacent to, a secured area that affects security;

(iii) Measures used to perform the access control functions required under § 1542.201(b)(1);

(iv) Procedures to control movement within the secured area, including identification media required under § 1542.201(b)(3); and

(v) A description of the notification signs required under § 1542.201(b)(6).

(4) A description of the AOA, including—

(i) A description and map detailing boundaries, and pertinent features;

(ii) Each activity or entity on, or adjacent to, an AOA that affects security;

(iii) Measures used to perform the access control functions required under § 1542.203(b)(1);

(iv) Measures to control movement within the AOA, including identification media as appropriate; and

(v) A description of the notification signs required under § 1542.203(b)(4).

(5) A description of the SIDA's, including—

(i) A description and map detailing boundaries and pertinent features; and

(ii) Each activity or entity on, or adjacent to, a SIDA.

(6) A description of the sterile areas, including—

(i) A diagram with dimensions detailing boundaries and pertinent features;

(ii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and

(iii) Measures used to control access as specified in § 1542.207.

(7) Procedures used to comply with § 1542.209 regarding fingerprint-based criminal history records checks.

(8) A description of the personnel identification systems as described in § 1542.211.

(9) Escort procedures in accordance with § 1542.211(e).

(10) Challenge procedures in accordance with § 1542.211(d).

(11) Training programs required under §§ 1542.213 and 1542.217(c)(2), if applicable.

(12) A description of law enforcement support used to comply with § 1542.215(a).

(13) A system for maintaining the records described in § 1542.221.

(14) The procedures and a description of facilities and equipment used to support TSA inspection of individuals and property, and aircraft operator or foreign air carrier screening functions of parts 1544 and 1546 of this chapter.

(15) A contingency plan required under § 1542.301.

(16) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(17) Procedures for posting of public advisories as specified in § 1542.305.

(18) Incident management procedures used to comply with § 1542.307.

(19) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions.

(20) Each exclusive area agreement as specified in § 1542.111.

(21) Each airport tenant security program as specified in § 1542.113.

(b) *Supporting program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(2) or (f), or § 1546.101(b) or (c) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC, as required under § 1542.3.

(2) A description of the law enforcement support used to comply with § 1542.215(a).

(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 1542.221.

(5) The contingency plan required under § 1542.301.

(6) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(7) Procedures for public advisories as specified in § 1542.305.

(8) Incident management procedures used to comply with § 1542.307.

(c) *Partial program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(h) or § 1546.101(d) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC as required under § 1542.3.

(2) A description of the law enforcement support used to comply with § 1542.215(b).

(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 1542.221.

(5) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(6) Procedures for public advisories as specified in § 1542.305.

(7) Incident management procedures used to comply with § 1542.307.

(d) *Use of appendices.* The airport operator may comply with paragraphs (a), (b), and (c) of this section by including in its security program, as an appendix, any document that contains the information required by paragraphs (a), (b), and (c) of this section. The appendix must be referenced in the corresponding section(s) of the security program.

**§ 1542.105 Approval and amendments.**

(a) *Initial approval of security program.* Unless otherwise authorized by the designated official, each airport operator required to have a security program under this part must submit its initial proposed security program to the designated official for approval at least 90 days before the date any aircraft operator or foreign air carrier required to have a security program under part 1544 or part 1546 of this chapter is expected to begin operations. Such requests will be processed as follows:

(1) The designated official, within 30 days after receiving the proposed security program, will either approve the program or give the airport operator written notice to modify the program to comply with the applicable requirements of this part.

(2) The airport operator may either submit a modified security program to the designated official for approval, or petition the Under Secretary to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.

(3) Ensure that all parties involved know their responsibilities and that all information contained in the plan is current.

(b) TSA may approve alternative implementation measures, reviews, and exercises to the contingency plan which will provide an overall level of security equal to the contingency plan under paragraph (a) of this section.

**§ 1542.303 Security Directives and Information Circulars.**

(a) TSA may issue an Information Circular to notify airport operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(b) Each airport operator must comply with each Security Directive issued to the airport operator within the time prescribed in the Security Directive.

(c) Each airport operator that receives a Security Directive must—

(1) Within the time prescribed in the Security Directive, verbally acknowledge receipt of the Security Directive to TSA.

(2) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(d) In the event that the airport operator is unable to implement the measures in the Security Directive, the airport operator must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval. The airport operator must submit the proposed alternative measures within the time prescribed in the Security Directive. The airport operator must implement any alternative measures approved by TSA.

(e) Each airport operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.

(f) Each airport operator that receives a Security Directive or an Information Circular and each person who receives information from a Security Directive or an Information Circular must:

(1) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need-to-know.

(2) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those who have an operational need to know without the prior written consent of TSA.

**§ 1542.305 Public advisories.**

When advised by TSA, each airport operator must prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures. This information must be posted in the manner specified in the security program and for such a period of time determined by the Secretary of Transportation.

**§ 1542.307 Incident management.**

(a) Each airport operator must establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

(b) Immediately upon direct or referred receipt of a threat of any of the incidents described in paragraph (a) of this section, each airport operator must—

(1) Evaluate the threat in accordance with its security program;

(2) Initiate appropriate action as specified in the Airport Emergency Plan under 14 CFR 139.325; and

(3) Immediately notify TSA of acts, or suspected acts, of unlawful interference to civil aviation operations, including specific bomb threats to aircraft and airport facilities.

(c) Airport operators required to have a security program under § 1542.103(c) but not subject to 14 CFR part 139, must develop emergency response procedures to incidents of threats identified in paragraph (a) of this section.

(d) To ensure that all parties know their responsibilities and that all procedures are current, at least once every 12 calendar months each airport operator must review the procedures required in paragraphs (a) and (b) of this section with all persons having responsibilities for such procedures.

6. Add new part 1544 to Chapter XII, Subchapter C.

## PART 1544—AIRCRAFT OPERATOR SECURITY: AIR CARRIERS AND COMMERCIAL OPERATORS

**Subpart A—General**

Sec.
1544.1 Applicability of this part.
1544.3 TSA inspection authority.

**Subpart B—Security Program**

1544.101 Adoption and implementation.
1544.103 Form, content, and availability.
1544.105 Approval and amendments.

**Subpart C—Operations**

1544.201 Acceptance and screening of individuals and accessible property.
1544.203 Acceptance and screening of checked baggage.
1544.205 Acceptance and screening of cargo.
1544.207 Screening of individuals and property.
1544.209 Use of metal detection devices.
1544.211 Use of X-ray systems.
1544.213 Use of explosives detection systems.
1544.215 Security coordinators.
1544.217 Law enforcement personnel.
1544.219 Carriage of accessible weapons.
1544.221 Carriage of prisoners under the control of armed law enforcement officers.
1544.223 Transportation of Federal Air Marshals.
1544.225 Security of aircraft and facilities.
1544.227 Exclusive area agreement.
1544.229 Fingerprint-based criminal history records checks (CHRC): Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions.
1544.231 Airport-approved and exclusive area personnel identification systems.
1544.233 Security coordinators and crewmembers, training.
1544.235 Training and knowledge for individuals with security-related duties.

**Subpart D—Threat and Threat Response**

1544.301 Contingency plan.
1544.303 Bomb or air piracy threats.
1544.305 Security Directives and Information Circulars.

**Subpart E—Screener Qualifications When the Aircraft Operator Performs Screening**

1544.401 Applicability of this subpart.
1544.403 Current screeners.
1544.405 New screeners: Qualifications of screening personnel.
1544.407 New screeners: Training, testing, and knowledge of individuals who perform screening functions.
1544.409 New screeners: Integrity of screener tests.
1544.411 New screeners: Continuing qualifications for screening personnel.

**Authority:** 49 U.S.C. 114, 5103, 40119, 44901–44905, 44907, 44913–44914, 44916–44918, 44932, 44935–44936, 44942, 46105.

### Subpart A—General

**§ 1544.1 Applicability of this part.**

(a) This part prescribes aviation security rules governing the following:

(1) The operations of aircraft operators holding operating certificates under 14 CFR part 119 for scheduled passenger operations, public charter passenger operations, private charter passenger operations, and other aircraft operators

adopting and obtaining approval of an aircraft operator security program.

(2) Each law enforcement officer flying armed aboard an aircraft operated by an aircraft operator described in paragraph (a)(1) of this section.

(3) Each aircraft operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular issued by TSA.

(b) As used in this part, "aircraft operator" means an aircraft operator subject to this part as described in § 1544.101.

**§ 1544.3 TSA inspection authority.**

(a) Each aircraft operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with—

(1) This subchapter and any security program under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each aircraft operator must provide evidence of compliance with this part and its security program, including copies of records.

(c) TSA may enter and be present within secured areas, AOA's, and SIDA's without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

(d) At the request of TSA and the completion of SIDA training as required in a security program, each aircraft operator must promptly issue to TSA personnel access and identification media to provide TSA personnel with unescorted access to, and movement within, areas controlled by the aircraft operator under an exclusive area agreement.

## Subpart B—Security Program

**§ 1544.101 Adoption and implementation.**

(a) *Full program.* Each aircraft operator must carry out subparts C, D, and E of this part and must adopt and carry out a security program that meets the requirements of § 1544.103 for each of the following operations:

(1) A scheduled passenger or public charter passenger operation with an aircraft having a passenger seating configuration of 61 or more seats.

(2) A scheduled passenger or public charter passenger operation with an aircraft having a passenger seating configuration of 60 or fewer seats when passengers are enplaned from or deplaned into a sterile area.

(b) *Partial program—adoption.* Each aircraft operator must carry out the requirements specified in paragraph (c) of this section for each of the following operations:

(1) A scheduled passenger or public charter passenger operation with an aircraft having a passenger-seating configuration of 31 or more but 60 or fewer seats that does not enplane from or deplane into a sterile area.

(2) A scheduled passenger or public charter passenger operation with an aircraft having a passenger-seating configuration of 60 or fewer seats engaged in operations to, from, or outside the United States that does not enplane from or deplane into a sterile area.

(c) *Partial program—content.* For operations described in paragraph (b) of this section, the aircraft operator must carry out the following, and must adopt and carry out a security program that meets the applicable requirements of § 1544.103(c):

(1) The requirements of §§ 1544.215, 1544.217, 1544.219, 1544.235, 1544.301, 1544.303, and 1544.305.

(2) Such other provisions of subparts C, D, and E of this part as TSA has approved upon request.

(3) The remaining requirements of subparts C, D, and E of this part when TSA notifies the aircraft operator in writing that a security threat exists concerning that operation.

(d) [Reserved]

(e) [Reserved]

(f) *Private charter program.* Each aircraft operator must carry out §§ 1544.201, 1544.207, 1544.209, 1544.211, 1544.213, 1544.215, 1544.217, 1544.219, 1544.229, 1544.233, 1544.235, 1544.303, and 1544.305, and subpart E of this part and must adopt and carry out a security program that meets the applicable requirements of § 1544.103 for each private charter operation in which passengers are enplaned from or deplaned into a sterile area.

(g) *Limited program.* TSA may approve a security program after receiving a request by an aircraft operator, holding a certificate under 14 CFR part 119 other than one identified in paragraph (a), (b), or (c) of this section. The aircraft operator must—

(1) Carry out selected provisions of subparts C, D, and E of this part,

(2) Carry out § 1544.305, as specified in its security program, and

(3) Adopt and carry out a security program that meets the applicable requirements of § 1544.103(c).

**§ 1544.103 Form, content, and availability.**

(a) *General requirements.* Each security program must:

(1) Provide for the safety of persons and property traveling on flights provided by the aircraft operator against acts of criminal violence and air piracy, and the introduction of explosives, incendiaries, or weapons aboard an aircraft.

(2) Be in writing and signed by the aircraft operator or any person delegated authority in this matter.

(3) Be approved by TSA.

(b) *Availability.* Each aircraft operator having a security program must:

(1) Maintain an original copy of the security program at its corporate office.

(2) Have accessible a complete copy, or the pertinent portions of its security program, or appropriate implementing instructions, at each airport served. An electronic version of the program is adequate.

(3) Make a copy of the security program available for inspection upon request of TSA.

(4) Restrict the distribution, disclosure, and availability of information contained in the security program to persons with a need-to-know as described in part 1520 of this chapter.

(5) Refer requests for such information by other persons to TSA.

(c) *Content.* The security program must include, as specified for that aircraft operator in § 1544.101, the following:

(1) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.201 regarding the acceptance and screening of individuals and their accessible property.

(2) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.203 regarding the acceptance and screening of checked baggage.

(3) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.205 regarding the acceptance and screening of cargo.

(4) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.207 regarding the screening of individuals and property.

(5) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.209 regarding the use of metal detection devices.

(6) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.211 regarding the use of x-ray systems.

(7) The procedures and description of the facilities and equipment used to comply with the requirements of § 1544.213 regarding the use of explosives detection systems.

(8) The procedures used to comply with the requirements of § 1544.215 regarding the responsibilities of security coordinators. The names of the Aircraft Operator Security Coordinator (AOSC) and any alternate, and the means for contacting the AOSC(s) on a 24-hour basis, as provided in § 1544.215.

(9) The procedures used to comply with the requirements of § 1544.217 regarding the requirements for law enforcement personnel.

(10) The procedures used to comply with the requirements of § 1544.219 regarding carriage of accessible weapons.

(11) The procedures used to comply with the requirements of § 1544.221 regarding carriage of prisoners under the control of armed law enforcement officers.

(12) The procedures used to comply with the requirements of § 1544.223 regarding transportation of Federal Air Marshals.

(13) The procedures and description of the facilities and equipment used to perform the aircraft and facilities control function specified in § 1544.225.

(14) The specific locations where the air carrier has entered into an exclusive area agreement under § 1544.227.

(15) The procedures used to comply with the applicable requirements of § 1544.229 regarding fingerprint-based criminal history record checks.

(16) The procedures used to comply with the requirements of § 1544.231 regarding personnel identification systems.

(17) The procedures and syllabi used to accomplish the training required under § 1544.233.

(18) The procedures and syllabi used to accomplish the training required under § 1544.235.

(19) An aviation security contingency plan as specified under § 1544.301.

(20) The procedures used to comply with the requirements of § 1544.303 regarding bomb and air piracy threats.

**§ 1544.105 Approval and amendments.**

(a) *Initial approval of security program.* Unless otherwise authorized by TSA, each aircraft operator required to have a security program under this part must submit its proposed security program to the designated official for approval at least 90 days before the intended date of passenger operations. The proposed security program must meet the requirements applicable to its operation as described in § 1544.101. Such requests will be processed as follows:

(1) The designated official, within 30 days after receiving the proposed aircraft operator security program, will either approve the program or give the aircraft operator written notice to modify the program to comply with the applicable requirements of this part.

(2) The aircraft operator may either submit a modified security program to the designated official for approval, or petition the Under Secretary to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.

(3) The designated official, upon receipt of a petition for reconsideration, either amends or withdraws the notice, or transmits the petition, together with any pertinent information, to the Under Secretary for reconsideration. The Under Secretary disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the notice to modify, or by affirming the notice to modify.

(b) *Amendment requested by an aircraft operator.* An aircraft operator may submit a request to TSA to amend its security program as follows:

(1) The request for an amendment must be filed with the designated official at least 45 days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the designated official.

(2) Within 30 days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(3) An amendment to an aircraft operator security program may be approved if the designated official determines that safety and the public interest will allow it, and the proposed amendment provides the level of security required under this part.

(4) Within 30 days after receiving a denial, the aircraft operator may petition the Under Secretary to reconsider the denial. A petition for reconsideration must be filed with the designated official.

(5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to the Under Secretary for reconsideration. The Under Secretary disposes of the petition within 30 days of receipt by either directing the designated official to approve the amendment, or affirming the denial.

(6) Any aircraft operator may submit a group proposal for an amendment that is on behalf of it and other aircraft operators that co-sign the proposal.

(c) *Amendment by TSA.* If safety and the public interest require an amendment, TSA may amend a security program as follows:

(1) The designated official notifies the aircraft operator, in writing, of the proposed amendment, fixing a period of not less than 30 days within which the aircraft operator may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the aircraft operator of any amendment adopted or rescinds the notice. If the amendment is adopted, it becomes effective not less than 30 days after the aircraft operator receives the notice of amendment, unless the aircraft operator petitions the Under Secretary to reconsider no later than 15 days before the effective date of the amendment. The aircraft operator must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice or transmits the petition, together with any pertinent information, to the Under Secretary for reconsideration. The Under Secretary disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the amendment, or by affirming the amendment.

(d) *Emergency amendments.* If the designated official finds that there is an emergency requiring immediate action with respect to safety in air transportation or in air commerce that makes procedures in this section contrary to the public interest, the designated official may issue an amendment, without the prior notice and comment procedures in paragraph (c) of this section, effective without stay on the date the aircraft operator receives notice of it. In such a case, the designated official will incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The aircraft operator may file a petition for reconsideration under paragraph (c) of this section; however, this does not stay the effective date of the emergency amendment.

## Subpart C—Operations

### § 1544.201 Acceptance and screening of individuals and accessible property.

(a) *Preventing or deterring the carriage of any explosive, incendiary, or deadly or dangerous weapon.* Each aircraft operator must use the measures in its security program to prevent or deter the carriage of any weapon, explosive, or incendiary on or about each individual's person or accessible property before boarding an aircraft or entering a sterile area.

(b) *Screening of individuals and accessible property.* Except as provided in its security program, each aircraft operator must ensure that each individual entering a sterile area at each preboard screening checkpoint for which it is responsible, and all accessible property under that individual's control, are inspected for weapons, explosives, and incendiaries as provided in § 1544.207.

(c) *Refusal to transport.* Each aircraft operator must deny entry into a sterile area and must refuse to transport—

(1) Any individual who does not consent to a search or inspection of his or her person in accordance with the system prescribed in this part; and

(2) Any property of any individual or other person who does not consent to a search or inspection of that property in accordance with the system prescribed by this part.

(d) *Prohibitions on carrying a weapon, explosive, or incendiary.* Except as provided in §§ 1544.219, 1544.221, and 1544.223, no aircraft operator may permit any individual to have a weapon, explosive, or incendiary, on or about the individual's person or accessible property when onboard an aircraft.

(e) *Staffing.* Each aircraft operator must staff its security screening checkpoints with supervisory and non-supervisory personnel in accordance with the standards specified in its security program.

### § 1544.203 Acceptance and screening of checked baggage.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each aircraft operator must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized explosive or incendiary onboard aircraft in checked baggage.

(b) *Acceptance.* Each aircraft operator must ensure that checked baggage carried in the aircraft is received by its authorized aircraft operator representative.

(c) *Screening of checked baggage.* Except as provided in its security program, each aircraft operator must ensure that all checked baggage is inspected for explosives and incendiaries before loading it on its aircraft, in accordance with § 1544.207.

(d) *Control.* Each aircraft operator must use the procedures in its security program to control checked baggage that it accepts for transport on an aircraft, in a manner that:

(1) Prevents the unauthorized carriage of any explosive or incendiary aboard the aircraft.

(2) Prevents access by persons other than an aircraft operator employee or its agent.

(e) *Refusal to transport.* Each aircraft operator must refuse to transport any individual's checked baggage or property if the individual does not consent to a search or inspection of that checked baggage or property in accordance with the system prescribed by this part.

(f) *Firearms in checked baggage.* No aircraft operator may knowingly permit any person to transport in checked baggage:

(1) Any loaded firearm(s).

(2) Any unloaded firearm(s) unless—

(i) The passenger declares to the aircraft operator, either orally or in writing before checking the baggage that any firearm carried in the baggage is unloaded;

(ii) The firearm is carried in a hard-sided container;

(iii) The container in which it is carried is locked, and only the individual checking the baggage retains the key or combination; and

(iv) The checked baggage containing the firearm is carried in an area that is inaccessible to passengers, and is not carried in the flightcrew compartment,.

(3) Any unauthorized explosive or incendiary.

(g) *Ammunition.* This section does not prohibit the carriage of ammunition in checked baggage or in the same container as a firearm. Title 49 CFR part 175 provides additional requirements governing carriage of ammunition on aircraft.

### § 1544.205 Acceptance and screening of cargo.

(a) *General requirements.* Each aircraft operator must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of unauthorized explosives or incendiaries in cargo onboard a passenger aircraft.

(b) *Screening of cargo baggage.* Each aircraft operator must ensure that, as required in its security program, cargo is inspected for explosives and incendiaries before loading it on its aircraft in accordance with § 1544.207.

(c) *Control.* Each aircraft operator must use the procedures in its security program to control cargo that it accepts for transport on an aircraft in a manner that:

(1) Prevents the carriage of any unauthorized explosive or incendiary aboard the aircraft.

(2) Prevents access by persons other than an aircraft operator employee or its agent.

(d) *Refusal to transport.* Each aircraft operator must refuse to transport any cargo if the shipper does not consent to a search or inspection of that cargo in accordance with the system prescribed by this part.

### § 1544.207 Screening of individuals and property.

(a) *Applicability of this section.* This section applies to the inspection of individuals, accessible property, checked baggage, and cargo as required under this part.

(b) *Locations within the United States at which TSA conducts screening.* Each aircraft operator must ensure that the individuals or property have been inspected by TSA before boarding or loading on its aircraft. This paragraph applies when TSA is conducting screening using TSA employees or when using companies under contract with TSA.

(c) *Aircraft operator conducting screening.* Each aircraft operator must use the measures in its security program and in subpart E of this part to inspect the individual or property. This paragraph does not apply at locations identified in paragraphs (b) and (d) of this section.

(d) *Locations outside the United States at which the foreign government conducts screening.* Each aircraft operator must ensure that all individuals and property have been inspected by the foreign government. This paragraph applies when the host government is conducting screening using government employees or when using companies under contract with the government.

### § 1544.209 Use of metal detection devices.

(a) No aircraft operator may use a metal detection device within the United States or under the aircraft operator's operational control outside the United States to inspect persons, unless specifically authorized under a security program under this part. No aircraft operator may use such a device contrary to its security program.

(b) Metal detection devices must meet the calibration standards established by TSA.

**§ 1544.211 Use of X-ray systems.**

(a) *TSA authorization required.* No aircraft operator may use any X-ray system within the United States or under the aircraft operator's operational control outside the United States to inspect accessible property or checked baggage, unless specifically authorized under its security program. No aircraft operator may use such a system in a manner contrary to its security program. TSA authorizes aircraft operators to use X-ray systems for inspecting accessible property or checked baggage under a security program if the aircraft operator shows that—

(1) The system meets the standards for cabinet X-ray systems primarily for the inspection of baggage issued by the Food and Drug Administration (FDA) and published in 21 CFR 1020.40;

(2) A program for initial and recurrent training of operators of the system is established, which includes training in radiation safety, the efficient use of X-ray systems, and the identification of weapons, explosives, and incendiaries; and

(3) The system meets the imaging requirements set forth in its security program using the step wedge specified in American Society for Testing Materials (ASTM) Standard F792–88 (Reapproved 1993). This standard is incorporated by reference in paragraph (g) of this section.

(b) *Annual radiation survey.* No aircraft operator may use any X-ray system unless, within the preceding 12 calendar months, a radiation survey is conducted that shows that the system meets the applicable performance standards in 21 CFR 1020.40.

(c) *Radiation survey after installation or moving.* No aircraft operator may use any X-ray system after the system has been installed at a screening point or after the system has been moved unless a radiation survey is conducted which shows that the system meets the applicable performance standards in 21 CFR 1020.40. A radiation survey is not required for an X-ray system that is designed and constructed as a mobile unit and the aircraft operator shows that it can be moved without altering its performance.

(d) *Defect notice or modification order.* No aircraft operator may use any X-ray system that is not in full compliance with any defect notice or modification order issued for that system by the FDA, unless the FDA has advised TSA that the defect or failure to comply does not create a significant risk of injury, including genetic injury, to any person.

(e) *Signs and inspection of photographic equipment and film.* (1) At locations at which an aircraft operator uses an X-ray system to inspect accessible property the aircraft operator must ensure that a sign is posted in a conspicuous place at the screening checkpoint. At locations outside the United States at which a foreign government uses an X-ray system to inspect accessible property the aircraft operator must ensure that a sign is posted in a conspicuous place at the screening checkpoint.

(2) At locations at which an aircraft operator or TSA uses an X-ray system to inspect checked baggage the aircraft operator must ensure that a sign is posted in a conspicuous place where the aircraft operator accepts checked baggage.

(3) The signs required under this paragraph (e) must notify individuals that such items are being inspected by an X-ray and advise them to remove all X-ray, scientific, and high-speed film from accessible property and checked baggage before inspection. This sign must also advise individuals that they may request that an inspection be made of their photographic equipment and film packages without exposure to an X-ray system. If the X-ray system exposes any accessible property or checked baggage to more than one milliroentgen during the inspection, the sign must advise individuals to remove film of all kinds from their articles before inspection.

(4) If requested by individuals, their photographic equipment and film packages must be inspected without exposure to an X-ray system.

(f) *Radiation survey verification after installation or moving.* Each aircraft operator must maintain at least one copy of the results of the most recent radiation survey conducted under paragraph (b) or (c) of this section and must make it available for inspection upon request by TSA at each of the following locations—

(1) The aircraft operator's principal business office; and

(2) The place where the X-ray system is in operation.

(g) *Incorporation by reference.* The American Society for Testing and Materials (ASTM) Standard F792–88 (Reapproved 1993), "Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas," is approved for incorporation by reference by the Director of the Federal Register pursuant to 5 U.S.C. 552(a) and 1 CFR part 51. ASTM Standard F792–88 may be examined at the Department of Transportation (DOT) Docket, 400 Seventh Street SW, Room Plaza 401, Washington, DC 20590, or on DOT's Docket Management System (DMS) web page at *http://dms.dot.gov/search* (under docket number FAA–2001–8725). Copies of the standard may be examined also at the Office of the Federal Register, 800 North Capitol St., NW, Suite 700, Washington, DC. In addition, ASTM Standard F792–88 (Reapproved 1993) may be obtained from the American Society for Testing and Materials, 100 Barr Harbor Drive, West Conshohocken, PA 19428–2959.

(h) *Duty time limitations.* Each aircraft operator must comply with the X-ray operator duty time limitations specified in its security program.

**§ 1544.213 Use of explosives detection systems.**

(a) *Use of explosive detection equipment.* If TSA so requires by an amendment to an aircraft operator's security program, each aircraft operator required to conduct screening under a security program must use an explosives detection system approved by TSA to screen checked baggage on international flights.

(b) *Signs and inspection of photographic equipment and film.* (1) At locations at which an aircraft operator or TSA uses an explosives detection system that uses X-ray technology to inspect checked baggage the aircraft operator must ensure that a sign is posted in a conspicuous place where the aircraft operator accepts checked baggage. The sign must notify individuals that such items are being inspected by an explosives detection system and advise them to remove all X-ray, scientific, and high-speed film from checked baggage before inspection. This sign must also advise individuals that they may request that an inspection be made of their photographic equipment and film packages without exposure to an explosives detection system.

(2) If the explosives detection system exposes any checked baggage to more than one milliroentgen during the inspection the aircraft operator must post a sign which advises individuals to remove film of all kinds from their articles before inspection. If requested by individuals, their photographic equipment and film packages must be inspected without exposure to an explosives detection system.

**§ 1544.215 Security coordinators.**

(a) *Aircraft Operator Security Coordinator.* Each aircraft operator must designate and use an Aircraft Operator Security Coordinator (AOSC). The AOSC and any alternates must be appointed at the corporate level and must serve as the aircraft operator's primary contact for security-related

activities and communications with TSA, as set forth in the security program. Either the AOSC, or an alternate AOSC, must be available on a 24-hour basis.

(b) *Ground Security Coordinator.* Each aircraft operator must designate and use a Ground Security Coordinator for each domestic and international flight departure to carry out the Ground Security Coordinator duties specified in the aircraft operator's security program. The Ground Security Coordinator at each airport must conduct the following daily:

(1) A review of all security-related functions for which the aircraft operator is responsible, for effectiveness and compliance with this part, the aircraft operator's security program, and applicable Security Directives.

(2) Immediate initiation of corrective action for each instance of noncompliance with this part, the aircraft operator's security program, and applicable Security Directives. At foreign airports where such security measures are provided by an agency or contractor of a host government, the aircraft operator must notify TSA for assistance in resolving noncompliance issues.

(c) *In-flight Security Coordinator.* Each aircraft operator must designate and use the pilot in command as the In-flight Security Coordinator for each domestic and international flight to perform duties specified in the aircraft operator's security program.

**§ 1544.217 Law enforcement personnel.**

(a) The following applies to operations at airports within the United States that are not required to hold a security program under part 1542 of this chapter.

(1) For operations described in § 1544.101(a) each aircraft operator must provide for law enforcement personnel meeting the qualifications and standards specified in §§ 1542.215 and 1542.217 of this chapter.

(2) For operations described in § 1544.101(b) or (c) each aircraft operator must—

(i) Arrange for law enforcement personnel meeting the qualifications and standards specified in § 1542.217 of this chapter to be available to respond to an incident; and

(ii) Provide its employees, including crewmembers, current information regarding procedures for obtaining law enforcement assistance at that airport.

(b) The following applies to operations at airports required to hold security programs under part 1542 of this chapter. For operations described in § 1544.101(c), each aircraft operator must—

(1) Arrange with TSA and the airport operator, as appropriate, for law enforcement personnel meeting the qualifications and standards specified in § 1542.217 of this chapter to be available to respond to incidents, and

(2) Provide its employees, including crewmembers, current information regarding procedures for obtaining law enforcement assistance at that airport.

**§ 1544.219 Carriage of accessible weapons.**

(a) *Flights for which screening is conducted.* The provisions of § 1544.201(d), with respect to accessible weapons, do not apply to a law enforcement officer (LEO) aboard a flight for which screening is required if the requirements of this section are met. Paragraph (a) of this section does not apply to a Federal Air Marshal on duty status under § 1544.223.

(1) Unless otherwise authorized by TSA, the armed LEO must meet the following requirements:

(i) Be a Federal law enforcement officer or a full-time municipal, county, or state law enforcement officer who is a direct employee of a government agency.

(ii) Be sworn and commissioned to enforce criminal statutes or immigration statutes.

(iii) Be authorized by the employing agency to have the weapon in connection with assigned duties.

(iv) Has completed the training program "Law Enforcement Officers Flying Armed."

(2) In addition to the requirements of paragraph (a)(1) of this section, the armed LEO must have a need to have the weapon accessible from the time he or she would otherwise check the weapon until the time it would be claimed after deplaning. The need to have the weapon accessible must be determined by the employing agency, department, or service and be based on one of the following:

(i) The provision of protective duty, for instance, assigned to a principal or advance team, or on travel required to be prepared to engage in a protective function.

(ii) The conduct of a hazardous surveillance operation.

(iii) On official travel required to report to another location, armed and prepared for duty.

(iv) Employed as a Federal LEO, whether or not on official travel, and armed in accordance with an agency-wide policy governing that type of travel established by the employing agency by directive or policy statement.

(v) Control of a prisoner, in accordance with § 1544.221, or an armed LEO on a round trip ticket returning from escorting, or traveling to pick up, a prisoner.

(vi) TSA Federal Air Marshal on duty status.

(3) The armed LEO must comply with the following notification requirements:

(i) All armed LEOs must notify the aircraft operator of the flight(s) on which he or she needs to have the weapon accessible at least 1 hour, or in an emergency as soon as practicable, before departure.

(ii) Identify himself or herself to the aircraft operator by presenting credentials that include a clear full-face picture, the signature of the armed LEO, and the signature of the authorizing official of the agency, service, or department or the official seal of the agency, service, or department. A badge, shield, or similar device may not be used, or accepted, as the sole means of identification.

(iii) If the armed LEO is a State, county, or municipal law enforcement officer, he or she must present an original letter of authority, signed by an authorizing official from his or her employing agency, service or department, confirming the need to travel armed and detailing the itinerary of the travel while armed.

(iv) If the armed LEO is an escort for a foreign official then this paragraph (a)(3) may be satisfied by a State Department notification.

(4) The aircraft operator must do the following:

(i) Obtain information or documentation required in paragraphs (a)(3)(ii), (iii), and (iv) of this section.

(ii) Advise the armed LEO, before boarding, of the aircraft operator's procedures for carrying out this section.

(iii) Have the LEO confirm he/she has completed the training program "Law Enforcement Officers Flying Armed" as required by TSA, unless otherwise authorized by TSA.

(iv) Ensure that the identity of the armed LEO is known to the appropriate personnel who are responsible for security during the boarding of the aircraft.

(v) Notify the pilot in command and other appropriate crewmembers, of the location of each armed LEO aboard the aircraft. Notify any other armed LEO of the location of each armed LEO, including FAM's. Under circumstances described in the security program, the aircraft operator must not close the doors until the notification is complete.

(vi) Ensure that the information required in paragraphs (a)(3)(i) and (ii) of this section is furnished to the flight

crew of each additional connecting flight by the Ground Security Coordinator or other designated agent at each location.

(b) *Flights for which screening is not conducted.* The provisions of § 1544.201(d), with respect to accessible weapons, do not apply to a LEO aboard a flight for which screening is not required if the requirements of paragraphs (a)(1), (3), and (4) of this section are met.

(c) *Alcohol.* (1) No aircraft operator may serve any alcoholic beverage to an armed LEO.

(2) No armed LEO may:

(i) Consume any alcoholic beverage while aboard an aircraft operated by an aircraft operator.

(ii) Board an aircraft armed if they have consumed an alcoholic beverage within the previous 8 hours.

(d) *Location of weapon.* (1) Any individual traveling aboard an aircraft while armed must at all times keep their weapon:

(i) Concealed and out of view, either on their person or in immediate reach, if the armed LEO is not in uniform.

(ii) On their person, if the armed LEO is in uniform.

(2) No individual may place a weapon in an overhead storage bin.

**§ 1544.221 Carriage of prisoners under the control of armed law enforcement officers.**

(a) This section applies as follows:

(1) This section applies to the transport of prisoners under the escort of an armed law enforcement officer.

(2) This section does not apply to the carriage of passengers under voluntary protective escort.

(3) This section does not apply to the escort of non-violent detainees of the Immigration and Naturalization Service. This section does not apply to individuals who may be traveling with a prisoner and armed escort, such as the family of a deportee who is under armed escort.

(b) For the purpose of this section:

(1) "High risk prisoner" means a prisoner who is an exceptional escape risk, as determined by the law enforcement agency, and charged with, or convicted of, a violent crime.

(2) "Low risk prisoner" means any prisoner who has not been designated as "high risk."

(c) No aircraft operator may carry a prisoner in the custody of an armed law enforcement officer aboard an aircraft for which screening is required unless, in addition to the requirements in § 1544.219, the following requirements are met:

(1) The agency responsible for control of the prisoner has determined whether the prisoner is considered a high risk or a low risk.

(2) Unless otherwise authorized by TSA, no more than one high risk prisoner may be carried on the aircraft.

(d) No aircraft operator may carry a prisoner in the custody of an armed law enforcement officer aboard an aircraft for which screening is required unless the following staffing requirements are met:

(1) A minimum of one armed law enforcement officer must control a low risk prisoner on a flight that is scheduled for 4 hours or less. One armed law enforcement officer may control no more than two low risk prisoners.

(2) A minimum of two armed law enforcement officers must control a low risk prisoner on a flight that is scheduled for more than 4 hours. Two armed law enforcement officers may control no more than two low risk prisoners.

(3) For high-risk prisoners:

(i) For one high-risk prisoner on a flight: A minimum of two armed law enforcement officers must control a high risk prisoner. No other prisoners may be under the control of those two armed law enforcement officers.

(ii) If TSA has authorized more than one high-risk prisoner to be on the flight under paragraph (c)(2) of this section, a minimum of one armed law enforcement officer for each prisoner and one additional armed law enforcement officer must control the prisoners. No other prisoners may be under the control of those armed law enforcement officers.

(e) An armed law enforcement officer who is escorting a prisoner—

(1) Must notify the aircraft operator at least 24 hours before the scheduled departure, or, if that is not possible as far in advance as possible of the following—

(i) The identity of the prisoner to be carried and the flight on which it is proposed to carry the prisoner; and

(ii) Whether or not the prisoner is considered to be a high risk or a low risk.

(2) Must arrive at the check-in counter at least 1 hour before to the scheduled departure.

(3) Must assure the aircraft operator, before departure, that each prisoner under the control of the officer(s) has been searched and does not have on or about his or her person or property anything that can be used as a weapon.

(4) Must be seated between the prisoner and any aisle.

(5) Must accompany the prisoner at all times, and keep the prisoner under control while aboard the aircraft.

(f) No aircraft operator may carry a prisoner in the custody of an armed law enforcement officer aboard an aircraft unless the following are met:

(1) When practicable, the prisoner must be boarded before any other boarding passengers and deplaned after all other deplaning passengers.

(2) The prisoner must be seated in a seat that is neither located in any passenger lounge area nor located next to or directly across from any exit and, when practicable, the aircraft operator should seat the prisoner in the rearmost seat of the passenger cabin.

(g) Each armed law enforcement officer escorting a prisoner and each aircraft operator must ensure that the prisoner is restrained from full use of his or her hands by an appropriate device that provides for minimum movement of the prisoner's hands, and must ensure that leg irons are not used.

(h) No aircraft operator may provide a prisoner under the control of a law enforcement officer—

(1) With food or beverage or metal eating utensils unless authorized to do so by the armed law enforcement officer.

(2) With any alcoholic beverage.

**§ 1544.223 Transportation of Federal Air Marshals.**

(a) A Federal Air Marshal on duty status may have a weapon accessible while aboard an aircraft for which screening is required.

(b) Each aircraft operator must carry Federal Air Marshals, in the number and manner specified by TSA, on each scheduled passenger operation, and public charter passenger operation designated by TSA.

(c) Each Federal Air Marshal must be carried on a first priority basis and without charge while on duty, including positioning and repositioning flights. When a Federal Air Marshal is assigned to a scheduled flight that is canceled for any reason, the aircraft operator must carry that Federal Air Marshal without charge on another flight as designated by TSA.

(d) Each aircraft operator must assign the specific seat requested by a Federal Air Marshal who is on duty status. If another LEO is assigned to that seat or requests that seat, the aircraft operator must inform the Federal Air Marshal. The Federal Air Marshal will coordinate seat assignments with the other LEO.

(e) The Federal Air Marshal identifies himself or herself to the aircraft operator by presenting credentials that include a clear, full-face picture, the signature of the Federal Air Marshal, and the signature of the FAA Administrator. A badge, shield, or similar device may not

be used or accepted as the sole means of identification.

(f) The requirements of § 1544.219(a) do not apply for a Federal Air Marshal on duty status.

(g) Each aircraft operator must restrict any information concerning the presence, seating, names, and purpose of Federal Air Marshals at any station or on any flight to those persons with an operational need to know.

(h) Law enforcement officers authorized to carry a weapon during a flight will be contacted directly by a Federal Air Marshal who is on that same flight.

**§ 1544.225 Security of aircraft and facilities.**

Each aircraft operator must use the procedures included, and the facilities and equipment described, in its security program to perform the following control functions with respect to each aircraft operation:

(a) Prevent unauthorized access to areas controlled by the aircraft operator under an exclusive area agreement in accordance with § 1542.111 of this chapter.

(b) Prevent unauthorized access to each aircraft.

(c) Conduct a security inspection of each aircraft before placing it into passenger operations if access has not been controlled in accordance with the aircraft operator security program and as otherwise required in the security program.

**§ 1544.227 Exclusive area agreement.**

(a) An aircraft operator that has entered into an exclusive area agreement with an airport operator, under § 1542.111 of this chapter must carry out that exclusive area agreement.

(b) The aircraft operator must list in its security program the locations at which it has entered into exclusive area agreements with an airport operator.

(c) The aircraft operator must provide the exclusive area agreement to TSA upon request.

(d) Any exclusive area agreements in effect on November 14, 2001, must meet the requirements of this section and § 1542.111 of this chapter no later than November 14, 2002.

**§ 1544.229 Fingerprint-based criminal history records checks (CHRC): Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions.**

(a) *Scope.* The following individuals are within the scope of this section. Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions, are collectively referred to as "covered functions."

(1) *New unescorted access authority or authority to perform screening functions.* (i) Each employee or contract employee covered under a certification made to an airport operator on or after December 6, 2001, pursuant to 14 CFR 107.209(n) in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001) or § 1542.209(n) of this chapter.

(ii) Each individual issued on or after December 6, 2001, an aircraft operator identification media that one or more airports accepts as airport-approved media for unescorted access authority within a security identification display area (SIDA), as described in § 1542.205 of this chapter (referred to as "unescorted access authority").

(iii) Each individual, on or after December 6, 2001, granted authority to perform the following screening functions at locations within the United States (referred to as "authority to perform screening functions")—

(A) Screening passengers or property that will be carried in a cabin of an aircraft of an aircraft operator required to screen passengers under this part.

(B) Serving as an immediate supervisor (checkpoint security supervisor (CSS)), and the next supervisory level (shift or site supervisor), to those individuals described in paragraph (a)(1)(iii)(A) of this section.

(2) *Current unescorted access authority or authority to perform screening functions.* (i) Each employee or contract employee covered under a certification made to an airport operator pursuant to 14 CFR 107.31(n) in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001), or pursuant to 14 CFR 107.209(n) in effect prior to December 6, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001).

(ii) Each individual who holds on December 6, 2001, an aircraft operator identification media that one or more airports accepts as airport-approved media for unescorted access authority within a security identification display area (SIDA), as described in § 1542.205 of this chapter.

(iii) Each individual who is performing on December 6, 2001, a screening function identified in paragraph (a)(1)(iii) of this section.

(3) *New authority to perform checked baggage or cargo functions.* Each individual who, on and after February 17, 2002, is granted the authority to perform the following checked baggage and cargo functions (referred to as "authority to perform checked baggage or cargo functions"), except for individuals described in paragraph (a)(1) of this section:

(i) Screening of checked baggage or cargo of an aircraft operator required to screen passengers under this part, or serving as an immediate supervisor of such an individual.

(ii) Accepting checked baggage for transport on behalf of an aircraft operator required to screen passengers under this part.

(4) *Current authority to perform checked baggage or cargo functions.* Each individual who holds on February 17, 2002, authority to perform checked baggage or cargo functions, except for individuals described in paragraph (a)(1) or (2) of this section.

(b) *Individuals seeking unescorted access authority, authority to perform screening functions, or authority to perform checked baggage or cargo functions.* Each aircraft operator must ensure that each individual identified in paragraph (a)(1) or (3) of this section has undergone a fingerprint-based CHRC that does not disclose that he or she has a disqualifying criminal offense, as described in paragraph (d) of this section, before—

(1) Making a certification to an airport operator regarding that individual;

(2) Issuing an aircraft operator identification medium to that individual;

(3) Authorizing that individual to perform screening functions; or

(4) Authorizing that individual to perform checked baggage or cargo functions.

(c) *Individuals who have not had a CHRC.* (1) *Deadline for conducting a CHRC.* Each aircraft operator must ensure that, on and after December 6, 2002:

(i) No individual retains unescorted access authority, whether obtained as a result of a certification to an airport operator under 14 CFR 107.31(n) in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001), or under 14 CFR 107.209(n) in effect prior to December 6, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001), or obtained as a result of the issuance of an aircraft operator's identification media, unless the individual has been subject to a fingerprint-based CHRC for unescorted access authority under this part.

(ii) No individual continues to have authority to perform screening functions described in paragraph (a)(1)(iii) of this section, unless the individual has been subject to a fingerprint-based CHRC under this part.

(iii) No individual continues to have authority to perform checked baggage or

cargo functions described in paragraph (a)(3) of this section, unless the individual has been subject to a fingerprint-based CHRC under this part.

(2) *Lookback for individuals with unescorted access authority or authority to perform screening functions.* When a CHRC discloses a disqualifying criminal offense for which the conviction or finding was on or after December 6, 1991, the aircraft operator must immediately suspend that individual's unescorted access authority or authority to perform screening functions.

(3) *Lookback for individuals with authority to perform checked baggage or cargo functions.* When a CHRC discloses a disqualifying criminal offense for which the conviction or finding was on or after February 17, 1992, the aircraft operator must immediately suspend that individual's authority to perform checked baggage or cargo functions.

(d) *Disqualifying criminal offenses.* An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty by reason of insanity, of any of the disqualifying crimes listed in this paragraph in any jurisdiction during the 10 years before the date of the individual's application for authority to perform covered functions, or while the individual has authority to perform covered functions. The disqualifying criminal offenses are as follows:

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.

(2) Interference with air navigation; 49 U.S.C. 46308.

(3) Improper transportation of a hazardous material; 49 U.S.C. 46312.

(4) Aircraft piracy; 49 U.S.C. 46502.

(5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504.

(6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.

(7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.

(8) Conveying false information and threats; 49 U.S.C. 46507.

(9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).

(10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.

(11) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.

(12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.

(13) Murder.

(14) Assault with intent to murder.

(15) Espionage.

(16) Sedition.

(17) Kidnapping or hostage taking.

(18) Treason.

(19) Rape or aggravated sexual abuse.

(20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.

(21) Extortion.

(22) Armed or felony unarmed robbery.

(23) Distribution of, or intent to distribute, a controlled substance.

(24) Felony arson.

(25) Felony involving a threat.

(26) Felony involving—

(i) Willful destruction of property;

(ii) Importation or manufacture of a controlled substance;

(iii) Burglary;

(iv) Theft;

(v) Dishonesty, fraud, or misrepresentation;

(vi) Possession or distribution of stolen property;

(vii) Aggravated assault;

(viii) Bribery; or

(ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

(27) Violence at international airports; 18 U.S.C. 37.

(28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d).

(e) *Fingerprint application and processing.* (1) At the time of fingerprinting, the aircraft operator must provide the individual to be fingerprinted a fingerprint application that includes only the following—

(i) The disqualifying criminal offenses described in paragraph (d) of this section.

(ii) A statement that the individual signing the application does not have a disqualifying criminal offense.

(iii) A statement informing the individual that Federal regulations under 49 CFR 1544.229 impose a continuing obligation to disclose to the aircraft operator within 24 hours if he or she is convicted of any disqualifying criminal offense that occurs while he or she has authority to perform a covered function.

(iv) A statement reading, "The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or both. (See section 1001 of Title 18 United States Code.)"

(v) A line for the printed name of the individual.

(vi) A line for the individual's signature and date of signature.

(2) Each individual must complete and sign the application prior to submitting his or her fingerprints.

(3) The aircraft operator must verify the identity of the individual through two forms of identification prior to fingerprinting, and ensure that the printed name on the fingerprint application is legible. At least one of the two forms of identification must have been issued by a government authority, and at least one must include a photo.

(4) The aircraft operator must:

(i) Advise the individual that a copy of the criminal record received from the FBI will be provided to the individual, if requested by the individual in writing; and

(ii) Identify a point of contact if the individual has questions about the results of the CHRC.

(5) The aircraft operator must collect, control, and process one set of legible and classifiable fingerprints under direct observation by the aircraft operator or a law enforcement officer.

(6) Fingerprints may be obtained and processed electronically, or recorded on fingerprint cards approved by the FBI and distributed by TSA for that purpose.

(7) The fingerprint submission must be forwarded to TSA in the manner specified by TSA.

(f) *Fingerprinting fees.* Aircraft operators must pay for all fingerprints in a form and manner approved by TSA. The payment must be made at the designated rate (available from the local TSA security office) for each set of fingerprints submitted. Information about payment options is available though the designated TSA headquarters point of contact. Individual personal checks are not acceptable.

(g) *Determination of arrest status.* (1) When a CHRC on an individual described in paragraph (a)(1) or (3) of this section discloses an arrest for any disqualifying criminal offense listed in paragraph (d) of this section without indicating a disposition, the aircraft operator must determine, after investigation, that the arrest did not result in a disqualifying offense before granting authority to perform a covered function. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(2) When a CHRC on an individual described in paragraph (a)(2) or (4) of this section discloses an arrest for any disqualifying criminal offense without

indicating a disposition, the aircraft operator must suspend the individual's authority to perform a covered function not later than 45 days after obtaining the CHRC unless the aircraft operator determines, after investigation, that the arrest did not result in a disqualifying criminal offense. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(3) The aircraft operator may only make the determinations required in paragraphs (g)(1) and (g)(2) of this section for individuals for whom it is issuing, or has issued, authority to perform a covered function; and individuals who are covered by a certification from an aircraft operator under § 1542.209(n) of this chapter. The aircraft operator may not make determinations for individuals described in § 1542.209(a) of this chapter.

(h) *Correction of FBI records and notification of disqualification.* (1) Before making a final decision to deny authority to an individual described in paragraph (a)(1) or (3) of this section, the aircraft operator must advise him or her that the FBI criminal record discloses information that would disqualify him or her from receiving or retaining authority to perform a covered function and provide the individual with a copy of the FBI record if he or she requests it.

(2) The aircraft operator must notify an individual that a final decision has been made to grant or deny authority to perform a covered function.

(3) Immediately following the suspension of authority to perform a covered function, the aircraft operator must advise the individual that the FBI criminal record discloses information that disqualifies him or her from retaining his or her authority, and provide the individual with a copy of the FBI record if he or she requests it.

(i) *Corrective action by the individual.* The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record, subject to the following conditions—

(1) For an individual seeking unescorted access authority or authority to perform screening functions on or after December 6, 2001; or an individual seeking authority to perform checked baggage or cargo functions on or after February 17, 2002; the following applies:

(i) Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the aircraft operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The aircraft operator must obtain a copy, or accept a copy from the individual, of the revised FBI record or a certified true copy of the information from the appropriate court, prior to authority to perform a covered function.

(ii) If no notification, as described in paragraph (h)(1) of this section, is received within 30 days, the aircraft operator may make a final determination to deny authority to perform a covered function.

(2) For an individual with unescorted access authority or authority to perform screening functions before December 6, 2001; or an individual with authority to perform checked baggage or cargo functions before February 17, 2002; the following applies: Within 30 days after being advised of suspension because the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the aircraft operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The aircraft operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to reinstating authority to perform a covered function.

(j) *Limits on dissemination of results.* Criminal record information provided by the FBI may be used only to carry out this section and § 1542.209 of this chapter. No person may disseminate the results of a CHRC to anyone other than:

(1) The individual to whom the record pertains, or that individual's authorized representative.

(2) Officials of airport operators who are determining whether to grant unescorted access to the individual under part 1542 of this chapter when the determination is not based on the aircraft operator's certification under § 1542.209(n) of this chapter.

(3) Other aircraft operators who are determining whether to grant authority to perform a covered function under this part.

(4) Others designated by TSA.

(k) *Recordkeeping.* The aircraft operator must maintain the following information.

(1) *Investigation conducted before December 6, 2001.* The aircraft operator must maintain and control the access or employment history investigation files, including the criminal history records results portion, for investigations conducted before December 6, 2001.

(2) *Fingerprint application process on or after December 6, 2001.* The aircraft operator must physically maintain, control, and, as appropriate, destroy the fingerprint application and the criminal record. Only direct aircraft operator employees may carry out the responsibility for maintaining, controlling, and destroying criminal records.

(3) *Protection of records—all investigations.* The records required by this section must be maintained in a manner that is acceptable to TSA and in a manner that protects the confidentiality of the individual.

(4) *Duration—all investigations.* The records identified in this section with regard to an individual must be maintained until 180 days after the termination of the individual's authority to perform a covered function. When files are no longer maintained, the criminal record must be destroyed.

(l) *Continuing responsibilities.* (1) Each individual with unescorted access authority or the authority to perform screening functions on December 6, 2001, who had a disqualifying criminal offense in paragraph (d) of this section on or after December 6, 1991, must, by January 7, 2002, report the conviction to the aircraft operator and surrender the SIDA access medium to the issuer and cease performing screening functions, as applicable.

(2) Each individual with authority to perform a covered function who has a disqualifying criminal offense must report the offense to the aircraft operator and surrender the SIDA access medium to the issuer within 24 hours of the conviction or the finding of not guilty by reason of insanity.

(3) If information becomes available to the aircraft operator indicating that an individual with authority to perform a covered function has a possible conviction for any disqualifying criminal offense in paragraph (d) of this section, the aircraft operator must determine the status of the conviction. If a disqualifying criminal offense is confirmed the aircraft operator must immediately revoke any authority to perform a covered function.

(4) Each individual with authority to perform checked baggage or cargo functions on February 17, 2002, who had a disqualifying criminal offense in paragraph (d) of this section on or after February 17, 1992, must, by March 25 2002, report the conviction to the aircraft operator and cease performing check baggage or cargo functions.

(m) *Aircraft operator responsibility.* The aircraft operator must—

(1) Designate an individual(s) to be responsible for maintaining and controlling the employment history investigations for those whom the aircraft operator has made a certification to an airport operator under 14 CFR 107.209(n) in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001), and for those whom the aircraft operator has issued identification media that are airport-accepted. The aircraft operator must designate a direct employee to maintain, control, and, as appropriate, destroy criminal records.

(2) Designate an individual(s) to maintain the employment history investigations of individuals with authority to perform screening functions whose files must be maintained at the location or station where the screener is performing his or her duties.

(3) Designate an individual(s) at appropriate locations to serve as the contact to receive notification from individuals seeking authority to perform covered functions of their intent to seek correction of their FBI criminal record.

(4) Audit the employment history investigations performed in accordance with this section and 14 CFR 108.33 in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001). The aircraft operator must set forth the audit procedures in its security program.

**§ 1544.231 Airport-approved and exclusive area personnel identification systems.**

(a) Each aircraft operator must establish and carry out a personnel identification system for identification media that are airport-approved, or identification media that are issued for use in an exclusive area. The system must include the following:

(1) Personnel identification media that—

(i) Convey a full face image, full name, employer, and identification number of the individual to whom the identification medium is issued;

(ii) Indicate clearly the scope of the individual's access and movement privileges;

(iii) Indicate clearly an expiration date; and

(iv) Are of sufficient size and appearance as to be readily observable for challenge purposes.

(2) Procedures to ensure that each individual in the secured area or SIDA continuously displays the identification medium issued to that individual on the outermost garment above waist level, or is under escort.

(3) Procedures to ensure accountability through the following:

(i) Retrieving expired identification media.

(ii) Reporting lost or stolen identification media.

(iii) Securing unissued identification media stock and supplies.

(iv) Auditing the system at a minimum of once a year, or sooner, as necessary to ensure the integrity and accountability of all identification media.

(v) As specified in the aircraft operator security program, revalidate the identification system or reissue identification media if a portion of all issued, unexpired identification media are lost, stolen, or unretrieved, including identification media that are combined with access media.

(vi) Ensure that only one identification medium is issued to an individual at a time. A replacement identification medium may only be issued if an individual declares in writing that the medium has been lost or stolen.

(b) The aircraft operator may request approval of a temporary identification media system that meets the standards in § 1542.211(b) of this chapter, or may arrange with the airport to use temporary airport identification media in accordance with that section.

(c) Each aircraft operator must submit a plan to carry out this section to TSA no later than May 13, 2002. Each aircraft operator must fully implement its plan no later than November 14, 2003.

**§ 1544.233 Security coordinators and crewmembers, training.**

(a) No aircraft operator may use any individual as a Ground Security Coordinator unless, within the preceding 12-calendar months, that individual has satisfactorily completed the security training as specified in the aircraft operator's security program.

(b) No aircraft operator may use any individual as an in-flight security coordinator or crewmember on any domestic or international flight unless, within the preceding 12-calendar months or within the time period specified in an Advanced Qualifications Program approved under SFAR 58 in 14 CFR part 121, that individual has satisfactorily completed the security training required by 14 CFR 121.417(b)(3)(v) or 135.331(b)(3)(v), and as specified in the aircraft operator's security program.

(c) With respect to training conducted under this section, whenever an individual completes recurrent training within one calendar month earlier, or one calendar month after the date it was required, that individual is considered to have completed the training in the calendar month in which it was required.

**§ 1544.235 Training and knowledge for individuals with security-related duties.**

(a) No aircraft operator may use any direct or contractor employee to perform any security-related duties to meet the requirements of its security program unless that individual has received training as specified in its security program including their individual responsibilities in § 1540.105 of this chapter.

(b) Each aircraft operator must ensure that individuals performing security-related duties for the aircraft operator have knowledge of the provisions of this part, applicable Security Directives and Information Circulars, the approved airport security program applicable to their location, and the aircraft operator's security program to the extent that such individuals need to know in order to perform their duties.

## Subpart D—Threat and Threat Response

**§ 1544.301 Contingency plan.**

Each aircraft operator must adopt a contingency plan and must:

(a) Implement its contingency plan when directed by TSA.

(b) Ensure that all information contained in the plan is updated annually and that appropriate persons are notified of any changes.

(c) Participate in an airport-sponsored exercise of the airport contingency plan or its equivalent, as provided in its security program.

**§ 1544.303 Bomb or air piracy threats.**

(a) *Flight: Notification.* Upon receipt of a specific and credible threat to the security of a flight, the aircraft operator must—

(1) Immediately notify the ground and in-flight security coordinators of the threat, any evaluation thereof, and any measures to be applied; and

(2) Ensure that the in-flight security coordinator notifies all crewmembers of the threat, any evaluation thereof, and any measures to be applied; and

(3) Immediately notify the appropriate airport operator.

(b) *Flight: Inspection.* Upon receipt of a specific and credible threat to the security of a flight, each aircraft operator must attempt to determine whether or not any explosive or incendiary is present by doing the following:

(1) Conduct a security inspection on the ground before the next flight or, if the aircraft is in flight, immediately after its next landing.

(2) If the aircraft is on the ground, immediately deplane all passengers and submit that aircraft to a security search.

(3) If the aircraft is in flight, immediately advise the pilot in