THE PORT AUTHORITY OF NY & NJ

Airport Security Guidelines Manual

December 30, 2019

Revision History

Revision No.	Description	Date
0	Final Draft Version Incorporates PA Comments	May 3, 2019
1	Incorporates Law and Aviation Comments	September 16, 2019
2	Final Document for Release	December 30, 2019
3		
4		
5		
6		
7		
8		

***Note**: The revision history table is to be updated with the noted revisions before every re-distribution of this document.*

Table of Contents

1. INTRODUCTION

This document (hereinafter referred to as the "Guidelines") is a guide to security standards that all tenants, operators, vendors and others responsible for construction, operation, or maintenance of space within the airport ("Responsible Persons") will be required to incorporate into the development and management of facilities within Port Authority airports, i.e. John F. Kennedy International (JFK); LaGuardia (LGA); Newark Liberty International (EWR); New York Stewart International (SWF); and Teterboro (TEB) . The Guidelines set forth policies and procedures for Port Authority staff to ensure that the Port Authority airports comply with existing federal requirements and Port Authority security standards. Note that compliance with the Guidelines carries with it no guarantee of protection against acts of terrorism, other crimes, or any of their consequences. While following the Guidelines will help reduce risk, it cannot eliminate it. All Responsible Persons remain responsible for ensuring compliance with federal requirements and meeting reasonable standards of care and responsibility associated with their respective facilities. The Responsible Persons retain full responsibility for fulfilling the security obligations contained within the Guidelines. The Guidelines are not controlling with regard to airport sponsor conduct; rather, it establishes the policies and procedures to be followed in ensuring compliance with existing federal security requirements and Port Authority security standards. The Port Authority does not consent to the Guidelines being incorporated into the Airport Security Program, Exclusive Area Agreements, or Airport Tenant Security Programs.

1.1. Purpose

The Guidelines serve as a guide to the security standards that have been established by the Port Authority of New York & New Jersey (hereinafter referred to as the "Port Authority") for the planning, design, construction, operation and maintenance of facilities at its airports. These security standards incorporate the guidance issued by the Transportation Security Administration ("TSA"), airport security best practices and the Port Authority's requirements for the safe and secure planning, design, construction, operation and maintenance of facilities, sites and spaces on the airport.

These security standards are intended to inform existing and prospective Responsible Persons of security considerations to be addressed in accordance with applicable Port Authority security policies, guidelines, laws and regulations. These standards supplement existing building code requirements for any Port Authority facilities and will be incorporated into all new construction design approvals as part of the Tenant Construction and Alteration Process. The Guidelines will be incorporated into new Port Authority Aviation Department agreements as well as renewals. While a Responsible Person may construct or alter its facility with measures that exceed the Security Guidelines, it must adhere to the minimum requirements established by the Guidelines. The Port Authority may conduct surveys of a space at any time prior to, during and after construction or an alteration, or during occupancy to ensure the Guidelines standards are satisfied.

Responsible Persons shall refer to the Guidelines for the minimum standards for security designs, technologies, and protocols to be applied to design and operations at each aviation facility. The intent is to maintain a culture and environment where security is a central consideration in planning, design, construction, and operations.

The standards described in the Guidelines assume that the Responsible Person's planning, design, construction and operations will be in full compliance with all TSA regulations and Security Directives (SD) issued by the TSA or other applicable government agencies. The Guidelines may be updated from time to time in response to emerging threats and new technology.

1.2. Applicability

Requirements contained in the Guidelines shall apply in total to new construction, as applicable to the construction type (for example, terminal, cargo facility, parking garage, etc.). For alteration, renovation, and/or modification activities to existing premises, the applicability of the requirements shall be proportionate and commensurate with the nature of such alteration, renovation, and/or modification, as determined by the Port Authority. This will also be the case for new leases and/or lease renewals of existing premises.

1.3. Threats to Airport Safety and Security

The basic threats from terrorism can take the form of physical attacks using conventional weapons, vehicles, explosives, flammables, chemical and biological agents or the use of cyber methods to adversely impact public safety systems and infrastructure. Threats from natural hazards, such as wind and flood, need to be considered in planning and operating safety and security measures.

1.4. Airport Security Manager

The Airport Security Manager (ASM) is the primary contact at each Port Authority airport for compliance with TSA regulations, and Port Authority security standards and policies. The ASM is the designated Airport Security Coordinator (ASC) under TSR 1542, and in this capacity, is the Port Authority's liaison with the local TSA on regulatory matters and with airport tenants and permittees. The ASM prepares and maintains the Airport Security Program and approves Airport Tenant Security Programs, Exclusive Area Agreements, and construction-related security plans. The ASM is charged with analyzing security risk to the airport through use of security audits and risk assessments to identify vulnerabilities; engaging airport employees in awareness programs; training PA and tenant staff in best security practices; recommending capital security improvements, and implementing procedures and policies to correct or enhance the airport security posture. The ASM oversees a variety of security equipment for access control, intrusion detection, surveillance, and physical protection. The ASM oversees a civilian guard force for access control, surveillance and inspection patrol. The ASM works in close collaboration with the Airport General Manager and staff, Port Authority Police Department ("PAPD"), the Transportation Security

Administration ("TSA"), Customs and Border Protection ("CBP"), and the Federal Bureau of Investigation ("FBI").

1.5. Law Enforcement Support for Airport Security

The Port Authority operates facilities and systems at which terrorism or other criminal acts may have a significant impact on life safety and key infrastructure. Tenants, vendors, and contractors are required to cooperate with the Port Authority and its employees in complying with the security standards set forth in this Guideline.

Operational security plans rely upon the presence of a quick and strong response force. At Port Authority airports, that response force is provided by armed law enforcement consisting of the Port Authority Police Department (PAPD) at JFK, EWR, LGA, and TEB and the NY State Police (NYSP) at SWF, sometimes supplemented by other law enforcement entities and the National Guard, as authorized by the Governor in times of heightened alert.

The PAPD is also supported by the US Department of Homeland Security through the TSA when it comes to anti-terrorist training, drills, equipment and canine patrol forces.

PAPD operations and response are coordinated with TSA Security operations and US Customs (at international airport facilities.)

2. GENERAL SECURITY REQUIREMENTS

2.1. Security System Logic and Design

This section addresses a general approach to the following types of security related systems:

- Access Control Systems
- CCTV (Closed Circuit Video Cameras)
- Video Management & Surveillance Systems (VMSS)
- Public Address Systems
- Emerging Security Technologies

To be effective, these security systems need to be well planned and integrated in a manner that results in logic to achieve a security objective. This logic is formally known as a Concept of Operations or ConOps.

During the planning and design phases of a project, operational security mitigations should be documented by developing ConOps. The ConOps is a set of formal documents that describe how the building systems (space layout, structures, finishes, electrical, electronics, communications, HVAC, physical access control, barrier gates, and fire protection) will support and coordinate with the operational security plans to mitigate the various threat scenarios on a daily basis.

In planning technology-based security solutions, project planners need also to provide for expansion and evolution of systems and facilities. Allowing capacity for future design technologies in the present alleviates much of the burden for additional costs in retrofitting infrastructure in the future. This ‘forward thinking’ approach to planning and project design also minimizes downtime, loss of space and services, and inconvenience to airport passengers. Security project planning shall also incorporate back-up redundant features, such as alternate power sources, to ensure that critical systems remain resilient during emergency events.

The tenant shall also be required to build into the technology-based security systems a Quality Assurance element that will allow for monitoring that the required procedures are being followed by employees by generating a compliance report.

3. AIRPORT SECURITY AREAS

3.1. Overview of Aviation Facility Security Operations

Airport Security Areas encompass designated zones for the operation of airline terminals, commercial aircraft, air cargo facilities, and general aviation facilities. Security areas for airline terminal operations are addressed first in the guidelines. Air cargo facilities are covered in Section 7, and General Aviation is covered in Section 9.

Airline terminal operations encompass enplaning and deplaning activities of passengers. For the purposes of this document, the term "terminal" refers to that main building, or group of buildings, where the screening, boarding, and unloading of passengers and property occurs.

Essential considerations in TSA guidelines for terminal security planning[1] required at Port Authority airports include:

1. Restricted access to the AOA, Security Identification Display Area (SIDA), Secured Area, and Sterile Area, which are defined in 49 CFR § 1542 and in each airport's security program;
2. Flow of both passengers and employees from landside to airside and back;
3. Efficient and effective security screening of persons and property entering Sterile Areas, including consideration for queuing space during peak loads;
4. Effective screening of employees entering the AOA, Secured Area, and Sterile Area;
5. Separation of security areas and use of required and recommended signage;
6. Identification and protection of other vulnerable areas and assets;
7. Protection of aircraft, people, and property;
8. Blast mitigation measures;
9. Baggage screening requirements including checked baggage inspection systems (CBIS) and Checked Baggage Resolution Area (CBRA) Design Standards;
10. Space and infrastructure for checked baggage explosives detection systems (EDS) and devices;
11. Space for advanced and next-generation technologies at passenger screening checkpoints;
12. Accommodation of integrated infrastructure for advanced surveillance, and access controls with biometrics;
13. Command and control capabilities for improved situational and domain awareness; and
14. Cyber security requirements

Terminal operators are subject to the terms of the **Airport Planning Standards, Aviation Department – Port Authority of New York and New Jersey, Preliminary Draft, Version 3, dated September 2018** ***(Airport Planning Standards)***, where applicable. The *Airport Planning Standards* establish a general set of

[1] *TSA Recommended Security Guidelines for Airport Planning, Design and Construction (Latest edition)*

standards and performance criteria to maintain safe, functionally efficient, and code-compliant terminal area operations while ensuring airport customer satisfaction. This Security Guidelines Manual shall take precedent over the Airport Planning Standards with respect to any security standards or terms that may seem contradictory.

Subject to a tenant area–specific security program or plan approved by the Port Authority, the tenant assumes responsibility for specific security systems, measures, or procedures, except for law enforcement. Law enforcement at Port Authority NYC metropolitan area airports is under the oversight of Port Authority Police Department **(PAPD)**, members of which patrol the airports, and constitute the first line response force to any emergency, criminal or otherwise on airport property. Airport security policies and protocols that all tenant terminal operators and airlines are required to follow are managed by the Port Authority Civilian Airport Security Managers (ASM), also known as the Airport Security Coordinator (ASC), but at all times, remain the user's responsibility.

Pursuant to 49 C.F.R. 1542.5, the ASMs have the regulatory responsibility for compliance with applicable TSA regulations and must ensure that all tenants and airlines are in compliance with the TSA and Port Authority requirements. The ASMs also coordinate the sharing of information and meet with all the tenants on a regular basis to coordinate safety and security activities. They also conduct security audits and provide appropriate security countermeasures for vulnerabilities identified. Both the PAPD and ASMs report through a chain of command to the Port Authority's Chief Security Officer (CSO).

The general layout of Port Authority aviation facilities, as defined in ***TSA Recommended Security Guidelines for Airport Planning, Design & Construction,*** consists of three areas typically referred to by the industry as ***airside***, ***landside***, and ***terminal***. Each major area of the airport (airside, landside, and terminal) has its own special security requirements. Maintaining the integrity of airside/landside/terminal boundaries plays a critical role in reducing unauthorized access to, attacks on, or the introduction of dangerous devices aboard passenger aircraft.

3.2. Airside

The airside is a designated nonpublic area, as it generally includes security areas to which certain requirements apply under 49 CFR § 1542 (e.g., the AOA and Secured Areas).

Facility plans must reduce the number of delivery portals and access points to public restricted areas such as the Sterile and Secured/SIDA Areas to the absolute minimum number required.

3.3. Landside

Landside infrastructure is separate from terminal and airside facilities. In general, the landside facilities at Port Authority airports available to the public include patron and other public parking lots and garages, walkways, public access roadways, rental car facilities, taxi and ground transportation staging areas, AirTrain stations, and any other on-airport tenant facilities that serve the public such as hotels.

Based upon the Port Authority's agency-wide risk assessment for its airports, which takes into account actual past threats and acts of terrorism at Port Authority facilities, the surrounding NY/NJ Metro Area, and other major airports around the world, the Port Authority's landside facilities also have significant security requirements. Further information on these requirements is contained in the Guidelines.

The landside must also 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.

3.4. Terminals

The varied nature of functional activities in terminals calls for a wide range of security, safety, and operational standards. Many of these standards are closely linked to the locations of restricted areas such as Sterile and security areas within, and near, the terminal. Since the terminal usually straddles the boundary between airside and landside, certain portions of a terminal must meet the requirements of both areas.

3.4.1. Introduction of Security at Planning/Design Inception

Physical and operational security requirements must be introduced into the airport tenant project in the planning and design phase, to the degree required, for leases that cover new construction. In addition, projects that involve renovation of existing construction, or leasing and operation of an existing on-airport building that is being re-purposed may have similar requirements. For the latter category of projects, it is necessary to check with the ASM.

In the project's preliminary planning/design phase, the tenant developer shall retain an experienced anti-terrorism security professional and protective design engineer to perform security planning based upon the threats provided by the Port Authority for the specific airport. The aforementioned security professional shall demonstrate sufficient previous experience in completing protective design for building projects of a similar nature.

Any threat related information that is generated in the planning, design and construction process shall be classified as Confidential Privileged Information (CPI). Any individuals on the developer's planning and design team who will be involved in generating or handling the Port Authority's CPI for the security planning and design shall be required to undergo a background check through the Port Authority's Personal Assurance Program, currently provided by Secure Worker Access Consortium (SWAC), and execute a Non-Disclosure Agreement (NDA), all in accordance with the requirements contained in The Port Authority's Information Security Handbook.

The developer shall be required to designate a Security Information Manager (SIM) to ensure that the Security Information Handbook is strictly adhered to by the planning and design team and that they maintain related documentation.

Due to their confidential nature, the specific threats and threat magnitudes to the Port Authority Airports ("Port Authority Threat Matrix") are not included in this document. The types of threats and minimum threat magnitudes to be used for site specific threat and vulnerability assessments at a Port Authority airport will be provided to the tenant's designated SIM under a separate cover.

The tenant's anti-terrorism security professional in conjunction with the tenant's Architect/Engineer of record, shall prepare a Protective Design Narrative (PDN), if applicable to the project as determined by the ASM. The PDN shall document the threat mitigation strategies and specify the level of design performance required for each threat scenario in the Port Authority Threat Matrix. The identified mitigations shall then be refined in each later phase of the design all the way through to the construction phase and shall be subject to audit by the Port Authority as a basis for issuance of a Permit to Use or Occupy from the Port Authority.

The PDN shall document the specific strategies for mitigating threats by either: (a) screening them out through the use of physical barriers or electronically based access control, (b) defining the physical level of performance of the facility structural building elements and finishes that are required to limit damage to property and occupants from threats, (c) or otherwise employing security technology and personnel to detect, deter and defend the facility from threats. As such, the PDN shall rely on both physical force protection mitigations that are "built in" to the facility and operational security measures that shall be provided on a daily 24/7 basis.

The security planning and design process described above applies to all tenant development projects to be constructed and operated at Port Authority airports. This includes but is not limited to: airline terminals, elevated frontage roadway viaducts, parking garages, certain cargo facilities, General Aviation facilities, car rental facilities, and facilities that house utilities essential to airport operations.

3.4.2. Security Requirements for Terminals

Each airport terminal has a unique road system, architectural design, and operational layout. Each tenant terminal operator is required to tailor security design solutions to resolve fundamental security vulnerabilities and meet operational needs.

TSA best practice guidelines[2] are considered a minimum requirement at Port Authority airports. Tenants must implement the following security design strategies for new terminals and for renovation and expansion projects as outlined in the following sections:

[2] *TSA Recommended Security Guidelines for Airport Planning, Design and Construction (Latest edition)*

1. Approach roadways and unscreened parking facilities must have adequate standoff distances from the terminal that are enforced with crash-rated vehicle barriers (bollards) that prevent vehicles from driving close to or into the terminal (see Section 4.2).
2. Blast resistant façade and glazing materials or fabrications (see Section 4.3).
3. Structural columns and beams that are resistant to explosive blasts and progressive collapse (see Section 4.4).
4. Surveillance systems (such as CCTV cameras, video analytics, etc.) at curbside, doorways and perimeters, and within the departures hall, baggage claim and arrivals hall areas (see Sections 3.4.4 and 3.4.5).
5. Capability for vehicle inspection stations with ample space for vehicle queuing and standoff distances (see Section 4.1).
6. Consolidation of points where employees can enter any Secure Area (as defined in these Guidelines) and technology at those entry points to implement 100% screening of employees.
7. The comprehensive security plan between the Port Authority and airport tenants shall stipulate the measures by which the tenant shall perform terminal security functions. This comprehensive security plan shall contain descriptions of areas in which security measures are specified at each Port Authority airport in addition to all other security requirements related to a tenant's premises.

3.4.3. Access Control Systems (ACS)

Tenant terminal operators shall, at a minimum, electronically monitor, record and control portals, doors, and access points for authorized personnel passing between the following areas:

1. Sterile Area to/from Secured Area/SIDA
2. Public Area to/ from Sterile Area
3. Sterile Area to/from TSA Exit Lanes
4. Public Area to/from Secured Area/SIDA
5. Loading Docks to/from Public Area or Secured/Restricted areas
6. Any of the above areas to/from Back of House (BOH) spaces
7. Baggage Belt from Public Area

Security systems, such as CCTV cameras and electronic access control systems, must be integrated with a tenant's operations center (i.e. Security Operations Center (SOC)), operating on a 24-hour basis with dedicated and trained security operations staff. The systems shall be tied into the PANYNJ's Airport Operations Center (AOC) and there shall be a 5-minute response to door alarms or other access incidents.

3.4.3.1. Access Control System Components

All portals, doors and access points defined above shall be ACS monitored and controlled and must be equipped with an appropriate level door control and locking equipment based on the door or portal's classification. If the door also acts as an emergency exit, it shall be equipped with panic hardware operable from the inside only and otherwise kept secured at all times. In addition, the following integrated system components are required at a minimum for the ACS door interface:

1. Electronic card access reader to unlock door.
2. Monitored and audible alarm sounds when door is unlocked or opened without access card.
3. CCTV camera view of individual accessing the door with video resolution capable of facial recognition and automatically stored in video management system.
4. Door lock, access card reader, camera view and voice communication tied and integrated into the SOC so that the camera view automatically records and displays visual and audible alerts on console screen when any component is activated.
5. Capability to upgrade to/add biometric identification ID layer (see Section 3.4.3.5).
6. Minimum 4-hour UPS for the system. An audible alarm, connected to the AOC, to indicate UPS malfunction must be operational when the UPS is activated and in use.

3.4.3.2. Access Control to Back of House Areas

Back of house (BOH) areas are those tenant spaces that accommodate electrical, mechanical, HVAC, communications, operations, and other systems essential to the safe and secure day to day operation of the facility. As such, these spaces shall be access controlled to exclude any unauthorized persons including, passengers, vendors, contractors, delivery persons, and anyone who has no official purpose from entering them. All doors and roof hatches that provide access to back of house spaces to authorized personnel shall be ACS monitored, controlled and locked based on the BOH utility space door or hatch type[3] and must meet the requirements in Section 3.4.3.1 above.

3.4.3.3. Access Control Base System and Integration

The Access Control System design must include a level of reliability and redundancy that ensures:

1. No single point failure in the system.
2. Computer system controlled and local controller.
3. Alarm monitoring shall not be interrupted.
4. Access control passages shall be operational without any failure.
5. ACS management functions.

[3] *The type of door lock and key card entry may be different for a single door, double door, or roof hatch access to utility space rooms and roof mounted equipment areas.*

Tenant planners shall coordinate with the Port Authority during the design phase for direction on connectivity to the Port Authority's AOC and other monitoring centers.

The following systems shall be interfaced with the Access Control System:

1. Identity Management and Control System.
2. Video Management System.
3. Intelligent Video Analytics.
4. Biometric Readers.
5. Intercom System.
6. Fire Alarm System.
7. Baggage Handling System.
8. Anti-tailgating (anti-piggybacking) sensors for all Sterile Area and SIDA unmanned doors.

Access control systems shall be interconnected to the Port Authority central monitoring stations so that any individual's access control privileges in the terminal can be immediately terminated when the Port Authority revokes access privileges related to a Port Authority-issued Airport Security ID card. Tenants may not restrict, in any manner, the Port Authority's access to any of the tenant's premises that would prevent it from inspecting the tenant's compliance with any security requirements with respect to any Secured, Sterile or SIDA Areas. Requirements for connecting into the Port Authority network are detailed in the Port Authority Technology Department - *Technology Standards Overview*.

3.4.3.4. Access Control System Management Policies

The Port Authority requires that a terminal operator establish management policies that are regularly monitored and enforced including but not limited to the following.

1. Issue written access control policies and procedures that employees and authorized visitors must follow (e.g., no tailgating/piggy-backing policy).
2. Investigate access incident violations and maintain documentation of investigation and follow up with employees or authorized visitors based upon review of ACS audit records.
3. Conduct periodic random spot inspections of employee and authorized visitor electronic access cards and their personal identification credentials.

3.4.3.5. Biometric Authentication

Fingerprint readers, facial recognition CCTV cameras, or other biometric readers must be compatible with the identity verification method established by the terminal operator. The type of biometric reader to be considered shall comply with the Port Authority specific requirements and instructions. Terminal plans may propose the latest manufacturer products during the design phase that are compatible with the credentialing and Access Control systems for Port Authority consideration and approval. The facility operator should coordinate with the ASM to determine the necessary requirements.

3.4.3.6. Badging or Credentialing

Each Port Authority airport has an Airport Security Credentialing Office that issues airport-specific Airport Security ID Cards. The Airport Security ID card, when properly displayed by a cardholder, permits them access to non-public, Secured or Sterile Areas of the airport to perform job duties. All persons entering non-public, Secured or Sterile Area shall comply with all applicable security regulations and procedures as established by the Port Authority or pursuant to 49 CFR, Parts 1540 and 1542.

3.4.3.7. Electronic Card Access

At a minimum, tenant electronic ACS systems shall be configured to reliably meet the following performance criteria:

1. Prevent unauthorized visitor access.
2. Restrict employee access to sensitive areas.
3. Support management of access credentials.
4. Accommodate trusted vendors and suppliers.
5. Generate traffic reports by time-of-day, day-of-week and more.
6. Track entry/exit times by employee or department.
7. Retrieve audit data for review in case of an incident.
8. Perform centralized lock-down in the event of an emergency security threat.
9. Equip exterior entrance doors and sensitive interior doors with high security locks.
10. Limit employee access to only areas where they have an operational need to be.
11. The ACS shall be capable of being upgraded to incorporate identification technologies in addition to just an access card. For example, requiring a card and a personal identification number (PIN) or utilizing a fusion biometric device (e.g., facial and iris or fingerprint identification).

3.4.3.8. Manhole Lock Systems (Access Covers)

Where utility manholes are located within the tenant space, AOA apron or adjacent to a security fence, lockable covers with a standard locking tool are required. These manholes must be maintained in a locked status at all times to restrict access for authorized use only.

3.4.4. CCTV (Closed Circuit Video Cameras)

At a minimum, tenants are required to plan for, install, maintain and operate a comprehensive CCTV System (CCTV). CCTV surveillance should provide continuous views of persons for tracking from the point of entry to the terminal (i.e. sidewalk, but not restrooms), through the passenger screening checkpoint, and up to the boarding gate. CCTV shall be configured to reliably meet the following performance criteria:

1. Capability to configure and provide computer aided monitoring alerts to console operator in SOC when anomalies are noted (also referred to as supporting programmable computer analytics).

2. Utilize only Internet Protocol (IP) cameras that have capabilities to send and receive data via a computer network based on camera models and firmware that are appropriate for the environmental conditions, required Field of Views, and are compatible and capable to integrate with all the ACS, VMS and other systems called for in the Guidelines.
3. At a minimum, camera display and storage system image quality shall be compatible with facial recognition software, whether or not it is a currently required feature.
4. Enable all CCTV camera views to be electronically streamed (monitored and displayed) by the Port Authority upon request on a 24/7 basis by tying in system to the Port Authority's AOC. Contact the Airport Security Manager for the specific technical requirements.
5. Tenants must provide copies of any recorded video upon Port Authority request to be used for any lawful purpose (i.e. forensic, law enforcement).
6. All elements covered herein for the CCTV system shall have an UPS that can sustain operations for a minimum of four hours. An audible alarm, connected to the AOC, to indicate UPS malfunction must be operational when the UPS is activated and in use.
7. In addition to the CCTV camera locations that are integrated with the Access Control System under Section 3.4.3 (Access Control Systems) and 3.4.5 (Video Management & Surveillance Systems), provide the following minimum CCTV coverage for situational awareness and incident management in airline terminals:
    a. Coverage of landside areas including but not limited to: each level and all lanes of the frontage roadways; the full width and length of sidewalk areas for passenger and package drop off and pick-up; and all loading docks and restricted parking areas near the front of the terminal.
    b. Coverage inside the terminal from the terminal entrance/exit doors to the departure gates including but not limited to: terminal public areas, pre-TSA checkpoint queuing, ticketing, baggage claim, meter-greeter areas, ground transportation, unclaimed baggage, concessions, and all back of house spaces.
    c. Coverage of airside areas including, but not limited to, AOA entry/exit points.
    d. Coverage of Sterile areas including, but not limited to, retail corridors, vertical and horizontal transportation corridors, all secure entry/exit doors and baggage handling areas.
    e. Coverage of Secured areas, specifically the Ramp and Aircraft gate areas.
    f. Coverage of baggage make-up areas and TSA baggage screening areas.

3.4.5. Video Management & Surveillance Systems (VMSS)

At a minimum, tenant Video Management & Surveillance Systems (VMSS) shall be configured to reliably meet the following performance criteria:

1. Enable the display of live and recorded security camera video feeds at designated locations and support archiving video feeds on redundant VMSS servers.

2. Enable the users to operate on the video streams, distribute the video, store the video and perform other functions
3. Ability to call-up cameras, monitor and process images, and organize how images are stored, retrieved and integrated to third party applications
4. Enable all video from the integrated VMSS to be electronically shared (i.e. for monitoring and display) with the Port Authority upon request on a 24/7 basis and shared on stored media if requested.
5. Store all video for a minimum of 31 days for future retrieval and provide to the Port Authority if requested.
6. Configure the distributed video recording server architecture and supporting software application to allow each of the master servers to operate in an independent mode, furnishing identical capabilities for live viewing, video recording and review functions to its connected review workstations.
7. Configure the Network Attached Video Storage solution to avoid any single point of failure and to operate independently of one another and support all integrated security systems.
8. All elements covered herein for the VMSS shall have an UPS that can sustain operations for a minimum of four hours. An audible alarm, connected to the AOC, to indicate UPS malfunction, must be operational when the UPS is activated and in use.

3.4.6. VMSS Base System

The design of any video expansion or renovation project shall be configured as follows:

1. Core system hardware shall be located in a secure communications room (see Section 3.4.3.2 Access Control to Back of House Areas)
2. Contractor shall furnish equipment with the most current compatible version of firmware

3.4.7. TSA Checkpoint CCTV and VMSS Requirements

When the TSA Checkpoint CCTV and VMSS systems are the responsibility of the lessee and/or terminal developer, and require integration into the terminal systems, the following shall apply:

1. For CCTV coverage of TSA Passenger Security Screening Checkpoints (SSCP), see the requirements in *TSA Checkpoint Design Guide (CDG).*
2. TSA prefers CCTV design as an extension of an existing facility security system within the airport. When CCTV is part of an extended system, the equipment shall match the existing hardware in order to minimize maintenance costs and provide operator familiarity.
3. All camera “Field of Views” must be approved by the local TSA office assigned to the specific Port Authority airport and camera feeds must go to the location designated by TSA.
4. Local TSA and law enforcement (PAPD) shall be able to access the system at or near the checkpoint.

5. VMSS system shall be configured so that any recorded video of the SSCP may not be disclosed unless approved by local TSA and the ASM.
6. Configure Airport Checkpoint Digital Closed-Circuit Television (ACDTV) Systems (a component of the Airport Video Surveillance Program) to record activity at passenger screening checkpoints and to provide the PAPD and the TSA with a tool to assess and deal with security incidents more effectively.
7. Provide full size design drawings to the local TSA office assigned to the specific Port Authority airport that show the following:
    a. CCTV & Electrical System Abbreviations, Symbols and General Notes.
    b. CCTV Camera Mounting Details, system demolition (components to remain or be removed).
    c. CCTV camera schedule indicating the focus, aim, mounting, and applicable remarks for each new or existing CCTV camera.

3.4.8. Public Address Systems

1. Public address (PA) systems must be sufficiently flexible to handle the various planned usages including emergency notifications.
2. PA systems shall be configured by zones so that advisory messages and emergency announcements can be directed to specific areas where an emergency develops.
3. Emergency notifications shall take priority over all other messages. Standard wording of the distinct types of emergency messages shall be developed in advance.
4. PA systems shall be integrated to enable alarm notifications to be precise, indicating location, type of danger and evacuation directions in calmly spoken live or recorded messages.
5. PA system shall provide: sufficient sound volume and audible clarity of messages, a clear source of the message, proper routing of audio signals, appropriate equipment selection and acoustic design to avoid acoustic feedback and echo and to ensure that sound quality is maintained.
6. PA systems shall have a minimum 4-hour uninterrupted power source.
7. PA systems shall be connected to the Port Authority central monitoring station for the purpose of auditory monitoring and for remote operation in an emergency.
8. The PA system must be tied into the Port Authority AOC. Actual emergency messaging may come from PAPD as directed by the Incident Commander.

3.4.9. Variable Message Signage

1. Variable message signage must be sufficiently flexible to handle the various planned usages including emergency notifications.
2. Variable message signage must be coordinated with advisory messages and emergency announcements on the PA system and follow the same protocols.

3. Variable message signage shall be connected to the Port Authority central monitoring station for remote operation in an emergency.
4. Variable message signage must be tied into the Port Authority AOC. Directing of messaging may come from PAPD as directed by the Incident Commander.
5. All elements covered herein for the variable message signage shall have an UPS that can sustain operations for a minimum of four hours. An audible alarm, connected to the AOC, to indicate UPS malfunction must be operational when the UPS is activated and in use.

3.4.10. HVAC Systems

Comply with the following security requirements:

1. Air intakes for the building shall be located so that they are inaccessible to the public or other unauthorized personnel and shall be protected by a detection system.
2. If they are located on the roof, access to the roof shall be controlled by hatches that are entry controlled, alarmed and monitored by CCTV (or by another type of unauthorized entry detection system)
3. The HVAC systems shall have a highly effective air filtration system and the ability to isolate airflow under the tenant lease. Filtration and air-cleaning systems may protect a building and its occupants from the effects of a chemical, biological or radiological attack.[4]
4. Air recirculation intakes, mechanical rooms, and HVAC plenums shall be secured against unauthorized access and provide immediate detection of unauthorized access. All HVAC back of house (BOH) spaces shall be for authorized personnel only and shall be enforced by employee background checks, official ID credentials, key card entry tied into CACS, and CCTV surveillance.
5. Video surveillance equipment shall be installed at all entry points and all entries shall be monitored and recorded.

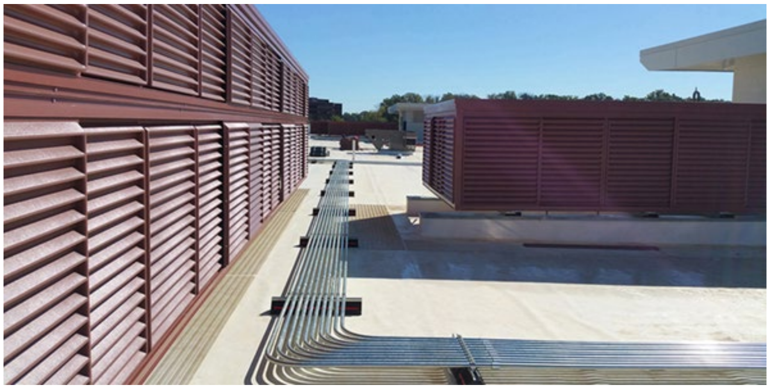


Figure 1 – Protected Rooftop HVAC Configuration

[4] *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attack (Published by US CDC, April 2003)*

3.4.11. Accommodation of Space in Public Areas for Police Screening Operations

1. Terminal plans shall incorporate space on the floors of the departures level and arrivals level that can be made available to PAPD to set up random screening operations.
2. Allow space for PAPD to set up a table to randomly select passengers for the purpose of inspecting luggage and packages for concealed threats.
3. Screening operations shall apply to passengers entering the building at the departures level with luggage or people entering the arrivals level to meet arriving passengers.

3.4.12. Accommodation of New Security Technologies and Protocols

Tenant terminal designs, especially at entrance locations, shall be sufficiently flexible and adaptable to be capable of accommodating new, emerging, and next generation security technologies (e.g. “at-speed” explosives and weapons detection at entrances) with minimal installation disruption. Accommodations may include spare conduits routed to electrical power and communications rooms to minimize the need to disrupt ceilings, floors, and walls in the future.

3.4.13. Terminal Airside Operations Areas

Terminal planners and designers must limit the number of delivery portals to Sterile and Secured/SIDA areas to the absolute minimum number possible based on the terminal’s physical configuration. The ultimate goal is to consolidate all deliveries to a specific location or a reduced number of locations, increase ramp safety and security, and reduce inspection costs.

3.5. Security Related Areas

3.5.1. Secured Area

Although the Secured Area generally includes portions of the airside and terminal, it is important to locate Secured Areas contiguously or as close together as possible to maximize ease of access by response personnel, utilize common areas of CCTV surveillance coverage, and minimize requirements for redundant boundaries and electronic access controls. Where there are several unconnected Secured Areas, such as baggage makeup areas, movement areas, safety areas, each shall require separate but integrated electronic access controls.

3.5.2. Sterile Area

General security requirements of the Sterile Area include:

1. All portals that serve as potential access points to Sterile Areas (i.e., doors, windows, passageways, etc.) must be secured to prevent bypassing the security screening checkpoint.

2. The number of access points shall be limited to the minimum that is operationally necessary, as determined by the airport operator.
3. Portals, including gates and fire egress doors, must prevent unauthorized entry by any person to the Sterile Area, and to the Secured Area, which includes airside and baggage make-up areas. Doors must also comply with applicable local fire and life safety codes and Americans with Disabilities Act (ADA) requirements, among others. The reliance upon security guards in lieu of electronic access control technology is not permitted. Discussions with local building and/or life safety code officials shall take place early to resolve special design issues, including how to accomplish the securing of fire doors.
4. Sterile Areas shall be designed and constructed to prevent articles from being passed from non-Sterile Areas into Sterile or Secured Areas such as restrooms, airline lounges and kitchen facilities, through plumbing chases, air vents, drains, trash chutes, utility tunnels, or other channels.
5. During construction or modification of facilities, provisions must be made to ensure that any individual who has not undergone screening is prevented from having contact with a screened person inside the Sterile Area.
6. New terminal plans shall provide as much distance as possible between exits from the Sterile Area and the nearest TSA screening checkpoint.
7. No vendors or other material deliveries shall be processed through the passenger screening checkpoint into the Sterile Area.

3.5.3. Exclusive Use Area

An exclusive use area is any portion of a Sterile or Secured Area, AOA, or SIDA, including individual access points, for which an aircraft operator or foreign air carrier with a security program under 49 CFR §§ 1544 or 1546 assumes security responsibilities under an Exclusive Area Agreement (EAA) with the Port Authority, under 49 CFR § 1542.111. The EAA, which is incorporated into the Port Authority's Airport Security Program (ASP), must be approved first by the Port Authority and thereafter by TSA.

Within the exclusive use area, the responsible aircraft operator or foreign air carrier must perform security control requirements described in the EAA. Pursuant to the EAA, the aircraft operator, not the Port Authority, must control access and movement within the exclusive area.

Specific requirements and conditions are contained in the EAA, including a description of very specific areas for which the aircraft operator assumes security responsibilities. This does not include law enforcement responsibilities, which always remain with the Port Authority.

3.5.4. Airport Tenant Security Program Area

The Airport Tenant Security Program (ATSP) identifies areas within the Port Authority aviation facilities specified by agreement between the Port Authority and airport tenants that stipulates the measures by which the tenant shall assume security responsibility under 49 CFR § 1542.113. ATSPs detail the security measures tenants must implement within exclusive use areas and are similar to EAAs, except that a tenant that is not regulated under 49 CFR § 1544 or 1546 may not assume responsibility for a passenger terminal. The ATSP, which is incorporated into the Port Authority's ASP, must be approved first by the ASM and then final TSA approval.

4. SECURITY REQUIREMENTS FOR TERMINALS AND OTHER BUILDINGS IN PUBLIC AREAS

Terminal public areas consist of the following areas: arrivals, departures, ticketing, check in, baggage claim, passenger drop off and pick up, public frontage roadway, truck loading docks and any other area accessible to the public prior to the TSA security checkpoint.

4.1. Frontage Roadway and Sidewalk Areas

Efficient traffic control is required to keep the building frontage open and quickly accessible to emergency access by police, first responders and emergency vehicles when an emergency occurs. Port Authority requirements include:

1. The design shall maximize the standoff distance between vehicles on the roadway and the building façade which must be enforced by crash rated bollards which are specified in Section 4.2.
2. Provide a sufficient number of traffic lanes for passenger drop off while affording strict operational enforcement of "no standing" rules for vehicles.
3. Provide clear and easily understood traffic signage to direct expeditious movement of vehicles and pedestrians through the frontage roadways and sidewalks.
4. Collaboration with the Port Authority in the planning phase on the use and expansion of landside taxi hold areas and for hire vehicle cell phone lots at on-airport locations accessible to the terminal.
5. Vehicle entrances and exits to public parking facilities directly in front of terminals are not permitted.

4.2. Enforcement of Vehicle Standoff (Use of Bollards)

1. Standoff protection measures from vehicles must be provided adjacent to critical building assets along a standoff limit.
2. Security bollards are required to be installed for the full length of the building roadway frontage providing a generous standoff distance from the sidewalk curb to the terminal façade.
3. The standoff distance between the bollard line and the terminal façade is relied upon for protection and as such shall be maximized by the designer and shall equal or exceed the distance determined by the security engineer's Protective Design Narrative defined in Section 3.4.1, or as required by similar Port Authority facilities.
4. When bollards are installed at existing building frontages, they shall be set at a distance of 18" from the terminal frontage sidewalk curb line that is closest to the terminal façade.

5. Security bollards shall have been tested and found to resist the dynamic impact for the maximum required vehicle weight and speed specified by ASTM F2656 criteria with a Dynamic Penetration Rating P1 less than or equal to 3.3 feet.
6. The vehicle impact speed may be reduced if it can be shown by vector analysis that the highest 90-degree impact speed achievable is less than the maximum.
7. Protective bollard dimensions and stainless-steel exterior sleeve are required to comply with Port Authority design standards.
8. For bollards, the clear distance between the structural members shall not exceed 48" and the clear opening between the finished bollard covers shall be ADA compatible.
9. ADA compliant curb cuts with tactile warning surface shall be provided between bollards per local codes and ordinances.
10. A minimum curb height of 6 inches must be provided at roadway frontages that accommodate ADA compliant kneeling buses.
11. Where there is no sidewalk curb required or constructed, a continuous ADA compliant tactile warning surface must be provided for the full length of the bollard line to establish the edge of roadway.
12. Where the maximum bollard spacing is not adequate to accommodate the building operator's clear opening requirement for operational or maintenance access, an equivalent crash rated horizontal beam barrier system or approved equal may be utilized at those locations.
13. Horizontal beam barriers shall have equivalent structural crash rating as the standard bollard system. They may be operated manually or power operated, with backup power provided.
14. Horizontal beam barriers shall be capable of being locked with access monitored by CCTV.

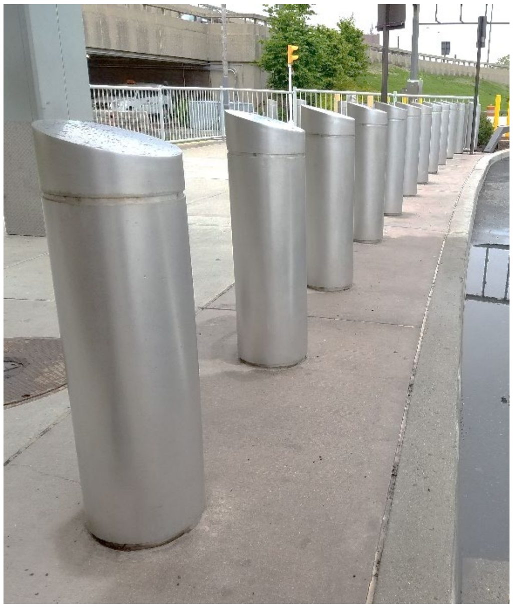


Figure 2 – Security Bollards at Terminal Frontage Roadway

4.3. Terminal Building Entrances, Curtainwall and Façade Glazing System

1. Security concerns must be addressed during planning and design of terminal building facades. The exterior curtain wall shall incorporate a blast debris mitigating system that shall provide a level of protection that is consistent with glazing systems designed to achieve a "high level" of protection as defined by the ISC Security Design Criteria for Federal Buildings, consistent with GSA Performance Condition 3b or better which provides a "High Level" of protection and "Low Hazard Level".
2. Glazing panels themselves shall meet ASTM F2912 - 17 Standard Specification for Glazing and Glazing Systems Subject to Air Blast Loadings.
3. This area of the terminal requires critical security planning considerations to reduce risks associated with close-proximity to vehicles and unscreened passengers, luggage and packages.
4. Entrance doors on the arrivals level shall be designed to be capable to operate in "exit only mode" so that during security alerts PAPD can restrict taxi or for hire drivers and others meeting arriving passengers to the sidewalk frontage area due to security concerns.
5. Entry/exit portals shall be designed with sufficient width to accommodate mass pedestrian exit during emergency evacuation.

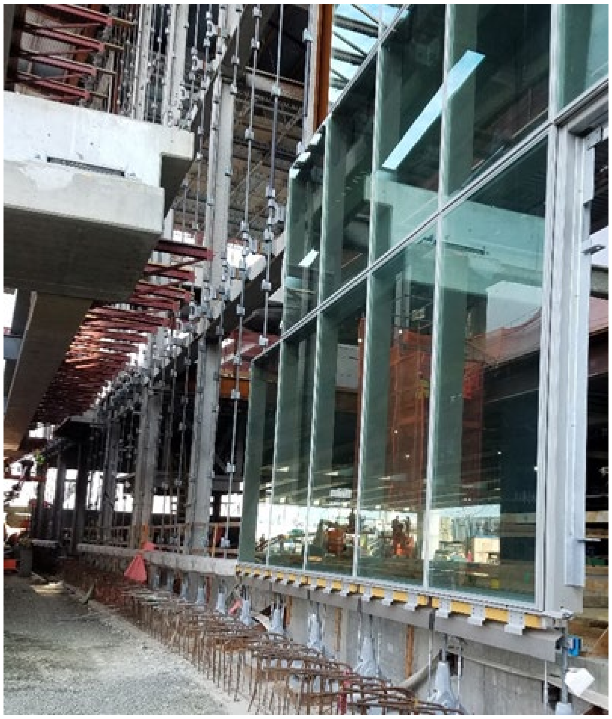


Figure 3 – Blast Resistant Terminal Façade Under Construction

4.4. Building Construction for Blast Loading

The Port Authority has established specific threat definitions and threat magnitudes to be used by building designers and applied by blast analysis experts at its facilities. The standoff protection distances are defined in Section 4.2. Based upon the standoff distance determined by the designer's PDN, the following criteria shall be followed for the design of building structures.

1. Threat magnitudes will be provided by the Port Authority.
2. Resistance to blast effects must be designed in accordance with the specific PDN Report developed for the building structure in the planning phase.
3. The Engineer-of Record (EOR) for blast analysis and blast mitigations shall demonstrate sufficient previous experience in force protection design for building projects of a similar nature. See Section 3.4.1 for additional information.
4. The performance requirement for the building structure when considering the blast effects from a vehicle threat on the roadway frontage is that no global or progressive collapse shall occur for the structural framing system and that post event, there shall be no worse than repairable damage to the building structure.
5. Damage from a hand carried explosive device threat inside the building in the pre-TSA screening public areas of terminals (departures area, baggage claim area, or arrivals hall area) shall result in no more than local floor framing collapse, without collapse progressing to adjacent building framed bays or floors above.
6. The EOR may utilize various means and methods to design the terminal building structure to meet the blast performance requirements including, but not limited to, any combination of the following:
    a. increasing threat standoff or reliably controlling threat access
    b. providing structural building system redundancy so that a locally damaged structural element shall not lead to global or progressive collapse and overall, the structure shall be repairable
    c. physically hardening individual structural elements to resist blast effects so they do not fail and are repairable

4.5. Landside Vehicular Parking Lots and Garages

1. Vehicular parking lots and structures for public use shall be proven to have adequate standoff distance from airline terminals, and parking structures shall be designed to resist progressive collapse due to blast forces.
2. Vehicle height in parking structures shall be limited to 9'-6" vertical clearance.
3. Damage to the structure from the vehicle threat shall be limited to ASCE 59-11 "Heavy Damage" limits or better.

4. Maximum damage shall result in only localized collapse of no more than two adjacent structural columns that extends vertically through the structure but does not extend laterally.
5. Restricted parking areas close to the terminal must be access controlled, allowing vehicle access to only known persons or screened individuals who exhibit proper credentials.
6. Access control shall consist of a staffed guard post with a “sally port” consisting of two lines of movable barriers to limit entry to only one vehicle at a time that meets the criteria for the maximum required vehicle weight and speed specified by ASTM F2656.
7. Access control shall be supervised by a guard and monitored remotely by CCTV.
8. The perimeter of the restricted parking area shall be separated from any adjacent roadways, or from any sidewalks/curbs mountable by vehicles, by a fixed crash rated barrier or bollards that meet the criteria for the maximum required vehicle weight and speed specified by ASTM F2656 to deny unauthorized vehicle entry.
9. Consult with the ASM to identify and determine physical and electronic security countermeasure requirements.

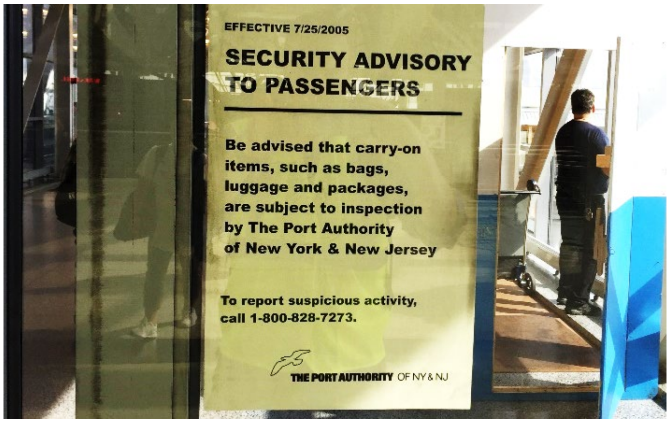
4.6. Terminal Airside (AOA) Lighting

1. Provide sufficient levels of lighting without blind spots in terminal areas abutting the airside to ensure proper visibility and detection of intruders.

4.7. Operational Security at Terminal Frontage, Arrivals and Departures Halls

4.7.1. Tenant Coordination with Airport Security Manager (ASM) and Port Authority Police (PAPD)

1. Terminal operators shall coordinate their security operations and communications plans with PAPD by working through the Airport Security Manager for approval.
2. Provide space for PAPD to perform scheduled random screening of passenger luggage at the roadway frontage and at the airline terminal arrivals and departures halls as described in Section 3.4.11.
3. Post advisory announcements distributed by the Port Authority that all persons, luggage and packages are subject to random searches for safety and security reasons and run audible announcements related to security awareness as requested by the ASM.
4. Manage terminal pick up and drop off operations to maintain steady traffic flow so as not to impede emergency response.
5. Unattended vehicles, luggage or packages are not permitted on the frontage roadway or sidewalk.



EFFECTIVE 7/25/2005

SECURITY ADVISORY TO PASSENGERS

Be advised that carry-on items, such as bags, luggage and packages, are subject to inspection by The Port Authority of New York & New Jersey

To report suspicious activity, call 1-800-828-7273.

THE PORT AUTHORITY OF NY & NJ

Figure 4 – Airport Luggage Screening Signage Advisory

4.7.2. Terminal Public Areas

The public areas of the terminals consist of airline ticketing counters, baggage claim, retail stores, restaurants, elevators, escalators, seating areas and other spaces in the terminal departures and arrivals hall public areas. The minimum Port Authority security requirements in these areas are described in this section.

1. These areas are required to be monitored from the terminal SOC for situational awareness of suspicious behavior utilizing CCTV. CCTV coverage shall be sufficient to cover all areas where the public gather upon departure or arrivals. See Section 3.4.4 on CCTV (Closed Circuit Video Cameras).
2. The terminal operator's security personnel shall be trained to observe and report unusual behavior or suspicious activity, particularly in the pre-screening public areas of the departures lobby.
3. Security management must also ensure their security personnel are provided up-to-date situational awareness information to improve their readiness to react correctly to observed anomalies.
4. During implementation of crisis contingency plans, expect terminal operations to be affected by special security measures as determined by Port Authority and ASMs.
5. Public areas shall be planned to provide for easy egress in event of emergency.
6. Public storage lockers are not permitted in any terminal building.
7. Avoid sight lines from adjacent stair landings or balconies looking down on ticket counters, baggage claim or TSA screening lines
8. Minimize the number of terminal entry points to those necessary to accommodate throughput.
9. Minimize concealment areas in public space, yet provide for defensive shelter for the public if under attack and for rapid evacuation.
10. Minimize or eliminate seating in ticketing areas.

4.7.3. Security at Baggage Claim and Inbound Baggage Areas

The baggage claim for domestic flights is located in the non-secure public areas of the terminal arrival hall with direct access to the curbside and accessible to unscreened transient ground transportation agents.

The planning and design of terminals shall incorporate the following operational security practices in the baggage claim area:

1. Utilize trained security personnel to provide claim ticket monitoring, provide customer assistance to arriving passengers and to engage any suspicious persons who exhibit abnormal behavior
2. Where possible, pick up of checked firearms shall be in a separate location from baggage claim area.
3. Any passenger who is picking up checked firearms must be escorted out by a Port Authority Police Officer.
4. Position CCTV cameras, with facial recognition capabilities, for surveillance and situational awareness of any suspicious behavior, and place at all exit and entrance doors to the arrivals level.
5. Baggage claim systems must be designed as to prevent direct access to the baggage make up area.
6. Arrivals level doors to the terminal frontage shall be adaptable to operate as follows:
    a. All doors can operate as “exit only” when needed
    b. In such cases, ground transportation agents may be required to enter through one central entrance where they shall be subject to random screening for weapons or other threats before being allowed to enter
    c. The central entrance door to be used for random screening shall be able to operate manually as a “Sally Port” with exterior door opening first, then closing after person enters, before the interior door is opened.

4.7.4. Trash and Recycling Receptacles in Public Areas

1. Trash receptacles with opaque walls that conceal items placed within them are not permitted.
2. Trash receptacles with heavy walls, such as aggregate cement/stone trash containers are not permitted.
3. Utilize only DHS approved trash containers with see-through plastic walls that allow ease of visual inspection of contents through clear plastic liners, as shown in Figure 5. See-through walls also allow security personnel or police to quickly vet a bomb threat.
4. Trash containers must not be located next to structural building columns.
5. Limit trash and recycling containers to the minimum number required.
6. Empty trash containers frequently.

Figure 5 **– DHS Approved See-Through Trash Receptacle**

4.8. Emergency Response Technologies

4.8.1. Gunshot Detection Systems

Gunshot Detection Systems which use acoustic and infrared sensors to detect the noise and the flash of light associated with the discharge of a weapon shall be installed in all public areas of airline terminals. The systems use this technology to rapidly locate the source of gunshots within a terminal by triangulation on the origin of the shot. It will be used by law enforcement to improve the speed of response to the incident and provide the operations center with information that shall be used to alert, instruct, or advise the building occupants.

4.8.2. Emerging Emergency Response Technologies

Other emerging emergency response technologies under consideration include:

1. Chemical / Biologic Sensor Detection – detection systems that provide faster response to potential chemical or biological release.

4.9. AirTrain Stations

AirTrain light rail system stations may be located across the frontage circulation roadway from the terminal, in which case the AirTrain passengers arrive at the terminal entrance by either an at-grade cross walk or an elevated pedestrian bridge. In other cases, AirTrain stations may be located within the public area of terminals. Security within AirTrain stations is the responsibility of the system operator, however, any emergency response event at an AirTrain terminal station shall require coordination between the terminal operator, the AirTrain operator and PAPD and the ASM. For that reason, the following security measures are required:

1. When AirTrain stations are located within the terminal, the terminal operator is required to provide CCTV coverage and public-address system coverage at the station entrance portals to the terminal in accordance with Sections 3.4.4 CCTV (Closed Circuit Video Cameras), 3.4.5 Video Management & Surveillance Systems (VMSS), and 3.4.8 Public Address Systems.
2. Station entrances to the terminal are required to be treated as any other entrance to the terminal, therefore, for security planning and operations purposes, Sections 3.4.11 Accommodation of Space in Public Areas for Police Screening Operations, and 3.4.12 Accommodation of New Security Technologies and Protocols, shall apply.
3. For the same reason as above, for security operations, Section 4.6 Operational Security at Terminal Frontage, Arrivals and Departures Halls shall apply.

4.10. Loading Docks for Delivery to Vendors

1. All new terminals are required to incorporate a remote, consolidated distribution center, located outside the airport, in another part of the airport or at the far edge of the terminal, which must provide the tenant an opportunity to screen deliveries by electronic methods, canine methods or other types of inspections as per TSA directives, for prohibited items and explosives prior to entry to the airport or terminal.
2. Deliveries shall be pre-scheduled and confirmed by the airline terminal operator.
3. Otherwise, goods destined for vendors must have direct access to the drop-off or pick-up location from a public (possibly restricted) roadway that does not require access to the AOA, SIDA, or Secured Area. The drop-off location to the terminal must provide loading dock facilities for trucks as large as tractor-trailers. Trucks shall only be permitted when the loading dock fully complies with items 4., 5. and 6. below.
4. In no case shall loading docks be placed adjacent to critical infrastructure and facilities.
5. The Port Authority requires that all vehicles intended for deliveries to landside loading docks be pre-screened and cleared by the tenant prior to entry access pursuant to TSA directives. This shall be achieved by operation of a truck-specific access point at the required standoff distance based upon the security designer’s criteria and configured with a staffed guard post and a “sally port” consisting of two lines of movable barriers to limit entry to only one vehicle at a time that meets the criteria for the maximum required vehicle weight and speed specified by ASTM F2656. Security guard personnel shall verify cargo loads, shipping authorization documents, and conduct visual vehicle inspection as per guard post orders.
6. Space in the “sally port” must be allocated and configured to allow for physical inspection of vehicles and their contents. During heightened security conditions, physical inspection, including

the under-carriage, of all delivery vehicles approaching the terminal may be required, with consideration for additional temporary vehicle inspection points and holding pens.

7. When pre-screening is not possible, the goods themselves need to be received in an area where they can be inspected and/or screened upon arrival.
8. Delivery personnel who use the airport loading docks and delivery areas must be provided with appropriate ID such as a driver's license, or company ID and may be subject to random inspection background checks.

4.11. Terminal Non-Public Areas

Service Corridors, Stairwells and Vertical Circulation: The following sections are similar to *Part III – TSA Recommended Guidelines, Section D – Terminal,* in reference[5] but need to be treated as mandatory:

1) *To avoid opening portals for unauthorized access to Secured or Sterile areas, service corridors shall be designed so as not to cross area boundaries; if crossings are unavoidable, transitions must be minimized, access-controlled, and with supporting electronic surveillance.*
2) *Service corridors shall be used to minimize the quantity and types of security access points. If access requirements are clustered by similarities of personnel or tenant areas (such as airline ticket offices, concession storage areas, concessionaires, or equipment maintenance access points), a common service corridor shall be used to serve multiple entities, and provide greater control of security than separate access points for each user.*
3) *The planning and design of non-service corridors shall consider placement and possible use by airport emergency personnel and law enforcement agencies. While use of service corridors by emergency and Law Enforcement Officer personnel is not a security requirement, proper corridor placement and design characteristics enhance response times as well as allow for private, non-disruptive transport of injured persons or security detainees.*
4) *Vertical circulation and stairwells … provide access not only to multiple floors, but often to multiple security levels as well. Fire stairs typically connect as many of the building's floors/levels as possible. Since they are located primarily to meet code separation requirements and provide egress from the facility, they are not often conveniently located regarding security boundaries or airport operation. In these instances, additional non-fire stairs, escalators, and elevators must be integrated into planning and design. Optimally, vertical cores will be shared for egress and operational movement. The Port Authority will have direct access to these areas.*

[5] *TSA Recommended Security Guidelines for Airport Planning, Design and Construction, Latest Edition*

5) *When any elevator serves one or more Sterile area floors it shall not open at any floor serving public areas. The same shall be true for any elevator serving a public area floor. It shall not open at Sterile floors. The elevator control panel will only allow the fire department to override this feature.*

Airport and Tenant Administrative/Personnel Offices: The following sections are similar to *Part III – TSA Recommended Guidelines, Section D – Terminal* in reference[5] but need to be treated as mandatory:

1) *Office areas shall be located close to the primary activity of the occupants to minimize the need for multiple security transitions. There may be various office areas within multiple security areas depending upon the function and preferences of the airport personnel. Office areas shall be located and connected via corridors and vertical circulation, to minimize the amount that the office personnel will need to cross security boundaries in their daily activities. Likewise, office spaces shall be planned with consideration for visitors and public access, to avoid the likelihood that any visitors will be left unattended or unescorted, providing unintended access to security areas.*

Figure 6 **– Vertical Circulation (EWR Terminal B)**

Law Enforcement & Public Safety Areas: The following sections are similar to *Part III – TSA Recommended Guidelines, Section D – Terminal in reference*[6] *but need to be treated as mandatory:*

1) *Terminal space planning related to law enforcement shall be coordinated with PAPD through the ASM.*

[6] *TSA Recommended Security Guidelines for Airport Planning, Design and Construction, Latest Edition*

2) *Allocate dedicated terminal parking spaces for PAPD with direct controlled landside/airside access and with quick access capability in both directions integrated with the access control system.*
3) *Allocate storage areas for PAPD tactical supplies and equipment in tactically identified areas.*
4) *When terminal plans include the allocation of operational space for contract security personnel and their equipment, include the need for inter-jurisdictional communications into the space planning, emphasizing the requirement to have in-depth discussions with all affected security and PAPD staff before designing their integrated space.*
5) *Communication/Dispatch facilities, equipment repair areas and other support functions near security personnel and police functions shall be located away from high threat areas and be considered for protection and control treatments.*

Local Security Operations Center: The following sections are similar to *Part III – TSA Recommended Guidelines, Section D – Terminal in reference*[7] *but need to be treated as mandatory:*

1) *SOCs are sometimes known by other names, particularly where they may co-locate with other terminal operational functions; such designations may include: Communications Center, Operations Center, or Security Control Center.*
2) *SOC shall be located close to the terminal's Fire Command Station, and in a controlled area because the Airport Incident Command Post must manage the emergency while the terminal operator deals with continuing regular operational concerns, and each must coordinate with the other. From the standpoint of cabling interconnections, a relatively central geographic location serves to maintain reasonable cable lengths to all the detection devices in a terminal security system that report alarms to the SOC. In addition, if facilities other than the SOC handle the airport's non-security communication functions (information, paging, telephones, maintenance dispatch, etc.), co-location or geographical placement of the SOC and the other facilities shall be considered such that cabling, equipment, maintenance, and emergency operations can be installed, operated and maintained in a cost-effective manner.*
3) *Other communications functions, equipment and operational areas shall be co-located with the SOC. Consider the merit and operational impact of consolidating the following functions within or adjacent to the SOC:*
    a. *Automatic notification system for emergency response recall of personnel;*
    b. *Direct phone lines to PAPD, Airport Operations Center (AOC)/Admin Building, control tower, and other sites, etc.;*
    c. *Fire alarm monitoring;*

[7] *TSA Recommended Security Guidelines for Airport Planning, Design and Construction, Latest Edition*

- d. *Flight Information Display (FIDS) systems; Baggage Information Display (BIDS) systems;*
- e. *ID management department;*
- f. *Information specialists for customer information lines, courtesy phones, airport paging;*
- g. *Landside/terminal operations;*
- h. *Maintenance control/dispatch or alarm monitoring (includes energy management of HVAC systems);*
- i. *Monitoring of PIDS, public safety, duress or security alarms;*
- j. *Personnel call-down paging system;*
- k. *Contract security department;*
- l. *Radio systems;*
- m. *Recording equipment; and*
- n. *Weather monitoring/radar/alert systems.*

5. TSA PASSENGER SECURITY SCREENING CHECKPOINTS (SSCP)

5.1. SSCP Overview

The TSA is responsible for the screening of personnel and carry-on baggage at SSCPs prior to entering the Sterile Area. As such, all SSCP designs and reconfigurations must be coordinated with TSA Headquarters (TSA HQ), the local Federal Security Director (FSD) and staff, and local airport stakeholders for adaptation to site-specific requirements. For specifics, review the most recent version of the full ***TSA Checkpoint Design Guide (CDG).***

5.2. Regulations and Guidelines

The regulations governing airport security and passenger SSCPs include:

1. 49 CFR § 1540 (Security: General Rules)
2. 49 CFR § 1542 (Airport Security)
3. 49 CFR § 1544 (Aircraft Operator Security)
4. 49 CFR § 1546 (Foreign Air Carrier Security)

While the regulations do not define the specific technical requirements that govern design of SSCPs, they define in general terms what must be accomplished by the design. All TSA regulations can be obtained on the TSA website.

5.3. Essential Coordination

Key individuals from TSA HQ, local TSA FSD offices, government agencies, airport, and airline operations must be involved early during the SSCP design process. These groups will be able to facilitate dialog regarding local building codes, mutual aid agreements with local law enforcement/emergency responders, and joint commercial/military presence that could factor into the checkpoint design, especially during emergencies.

5.4. Planning Considerations

Designing for the Future: As the number of enplanements per year increases and the equipment and technology evolve, the SSCP needs to have the flexibility for change and the ability to expand. Allowance for future modifications must be included in Terminal planning.

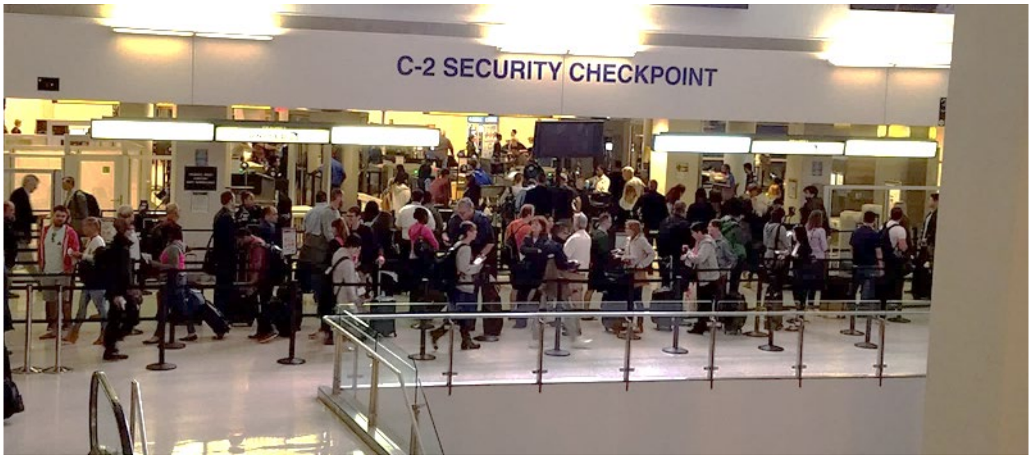


Figure 7 – TSA Security Checkpoint (EWR Terminal C)

5.5. SSCP Power, Data and CCTV

The power and IT requirements for security screening equipment and ancillary equipment is unique regarding the circuit type, receptacle type and quantity of data drops required. TSA checkpoints shall have a UPS so that they can operate during an emergency power outage.

CCTV requirements for SSCP are covered under Section 3.4.4. At each Port Authority airport, the SSCP CCTV feeds shall be transmitted to specific TSA designated locations both locally and regionally and shared locally with Port Authority. As noted in Section 3.4.4, any recorded CCTV video must be provided to the Port Authority upon request. Any recorded CCTV video of the SSCP may not be disclosed unless approved by the local TSA.

5.6. Safety

SSCPs must not only screen passengers and their carry-on baggage but must do so without compromising the safety of either the passengers or the Transportation Security Officers conducting the screening. Security requirements and safety related considerations shall be built into the SSCP design from the beginning and shall be treated as an integral part of the design process. Subject Matter Experts in security shall be included in every phase of the design to provide input on conceptual plans and/or construction drawing packages. With respect to security and safety, the following concerns shall be mitigated:

1. Sight lines of queued passengers from any horizontally adjacent or elevated vantage points in the terminal public area must be visually blocked by an opaque screen or shielded from ballistics by “see through” bullet proof glass to the extent possible.
2. TSA screening lanes shall be designed to accommodate increased passenger loads over the term of the lease in order to increase throughput and minimize crowding.

6. AIR OPERATIONS AREA

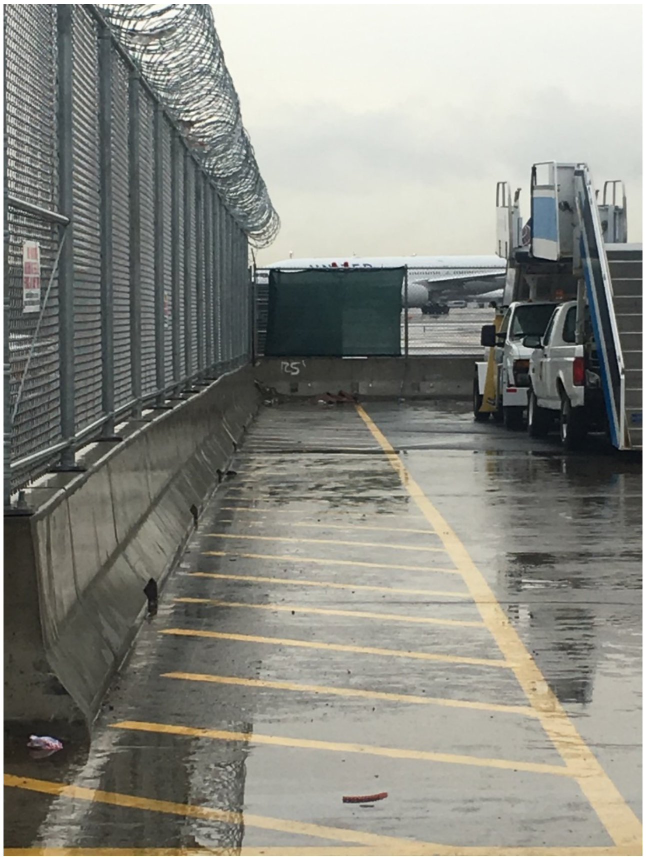
6.1. AOA Perimeter Protection

6.1.1. Perimeter Intrusion Detection System (PIDS)

1. The PANYNJ's PIDS is a multi-sensor, layered security system, incorporated into the perimeter fence system which is designed to protect airport perimeters against unauthorized entry twenty-four hours a day, seven days a week (24/7), in all weather conditions.
2. The PIDS is installed and operational at all PANYNJ Airports except SWF and since it is a program maintained by a third-party provider, temporary and permanent installation or removal of PIDS sensor equipment, design, installation, test and operator training of PIDS sensor equipment shall be subcontracted to the authorized system maintainer.
3. A tenant will be required to install, monitor on a 24/7 basis, and maintain a PIDS in any perimeter fencing on its leasehold, which must integrate with the Port Authority's PIDS system.
4. If any tenant construction or perimeter fence system modifications impact the AOA perimeter or are within a facility that affects existing infrastructure supporting the PIDS system, then the tenant's EOR must engage the Port Authority to obtain the proper design for the PIDs features and to coordinate with the PIDS contractor for the requirements, standards and product information.
5. Any design, installation or modification to the existing PIDS shall need to comply fully with PIDS Standards.
6. PIDS applications are scalable and may be linked to other sensor technologies designed for intruder detection and tracking such as Video Motion Detection (VMD) and Tracking (VMDT); Ground Surveillance Radars (GSR); and linear-type perimeter sensors, such as fence sensors, infrared trip lines, and buried cables sensitive to ground vibrations.

6.1.2. Perimeter Fencing

The AOA perimeter must be protected along its entire length by a security fence that conforms to Port Authority requirements.



Port Authority AOA Security Fence Requires a Continuous Reinforced Concrete Base Where Any Vehicles May Access the Surrounding Terrain

Figure 8 **– Example of Port Authority AOA Security Fences**

The basic features of Port Authority AOA Perimeter Security Fences are as follows:

1. A continuous crash resistant concrete base is required where any type of vehicle may have access to the terrain where the fence line is constructed.
2. The minimum fence fabric height is 8’-0” above the top of concrete barrier or above finished grade (Total fence height will include the concrete barrier, where required, and the barbed wire/concertina wire).
3. Chain link fabric is 1 ¾” x 1 ¾" with 0.192” OD wire, anti-climb with metal coated (galvanized) or polyvinyl chloride (PVC) coated.
4. Fence is topped with 3 lines of barbed wire, plus concertina wire.
5. Use of a non-metallic/non-conductive security fence shall be required in limited areas as required to ensure that the fencing does not conflict with the operational requirements of the airport such as when metal fencing will interfere with electronic aeronautical approach landing system equipment.

6. To assist in surveillance and security patrol inspections, fences shall be configured as straight and uncomplicated as area conditions will allow to preserve long straight lines of sight and detection zones for visual observations from patrols, CCTV monitoring, and various fence system detection sensors.
7. Contact the ASM for the current Port Authority AOA Security Fence design criteria when altering an existing security fence or constructing a new security fence.

AOA Security Fence Clear Zones

1. A clear zone must be maintained on both sides of the security fence at all times to prevent visual obstruction of any potential security breach by climbing or otherwise cutting the fence fabric to achieve unauthorized access.
2. A minimum clear zone of 10 feet from the AOA security fence line shall be maintained on both sides for its entire length at all airports.
3. Within clear zones there shall be no stored materials (boxes, stackable crates, pallets or other objects), and no parked vehicles, baggage carts, storage containers, climbable objects, trees, utility poles or other visual obstructions near the fence lines.

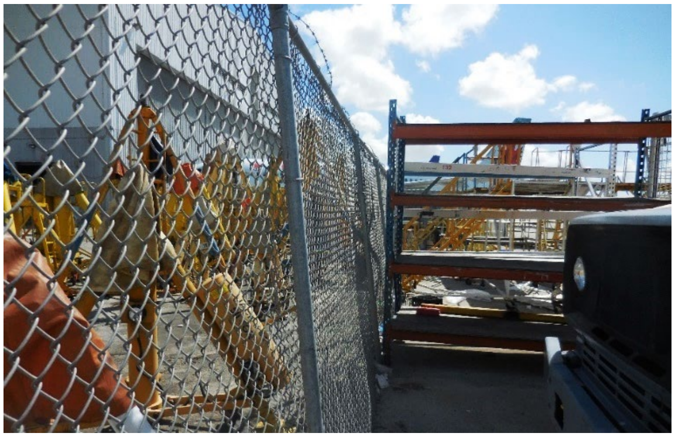


Figure 9 – Example of AOA Clear Zone Violation by Stored Objects

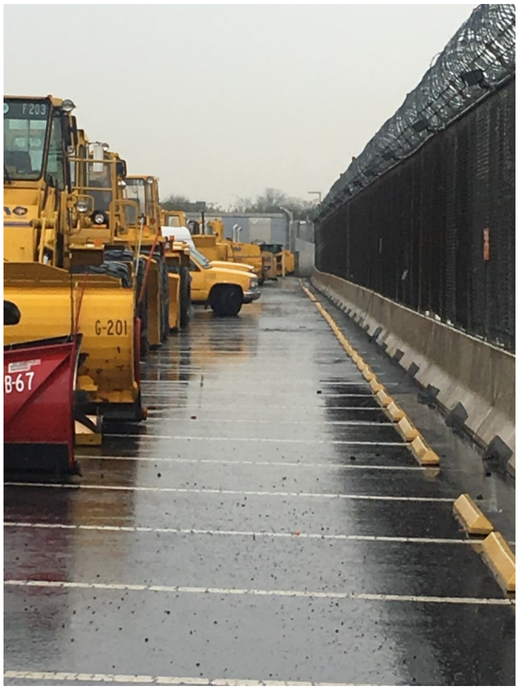


Figure 10 – Example of Compliant AOA Clear Zone

6.1.3. AOA Perimeter Guard Posts

6.1.3.1. General

1. AOA security guard posts permit passage of authorized vehicles and passengers into the AOA. The guard post locations must be approved in advance by the Port Authority.
2. Any vehicles, persons or cargo passing through the guard post, whether they require access to perform routine activities to service aircraft on the airside of the terminals, or to perform construction or inspections on the airside, are subject to inspection by a Port Authority security guard for a valid Airport Security ID Card for the driver and routing checks of all individuals in the vehicle, and inspection of vehicles and their contents for any contraband or illegal items.
3. If a tenant project scope of work includes an AOA perimeter guard post, contact the ASM for the latest design and construction requirements.
4. Any vehicles intended to work routinely on airside must have Port Authority plates.

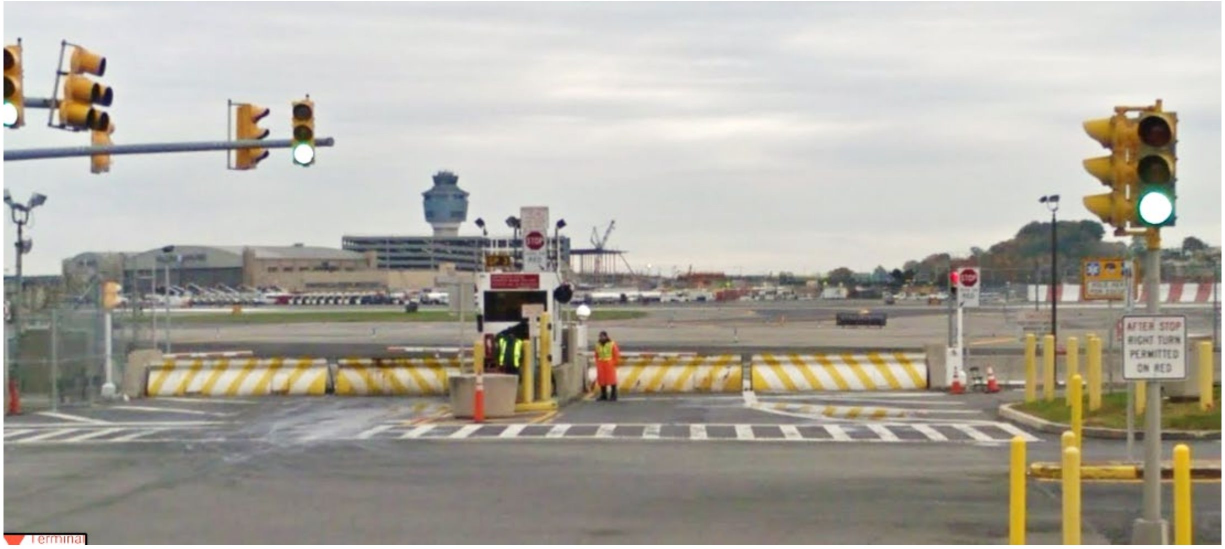


Figure 11 **– LaGuardia Airport AOA Guard Post**

6.1.3.2. Vehicle Barrier Gates

1. Guard posts at vehicle portals must be configured with crash rated moveable vehicle barrier gates meeting Port Authority requirements that must be manually controlled from inside the guard booth with automated safeguards.
2. Guard posts safeguard requirements include barrier gate control arms and vehicle detection loops in the pavement to detect or prevent vehicle spacing that is too close (piggy backing) which automatically prevents vehicle barrier gate from being lowered.

3. The moveable or arrestor barrier model shall have been tested by the manufacturer to meet or exceed the ASTM F2656 criteria for the maximum vehicle weight and vehicle speed.
4. Once a vehicle, its cargo and all occupants are cleared by the guard for entry, the vehicle barrier is lowered by guard manual control to permit access of the vehicle and occupants, and then raised again to prevent entry of the next vehicle, if any.
5. See Figure 12 and 13 for the types of moveable crash rated barriers that may be required by the Port Authority.
6. It is recommended that guard posts be configured as vehicle “Sally Ports” for positive control.

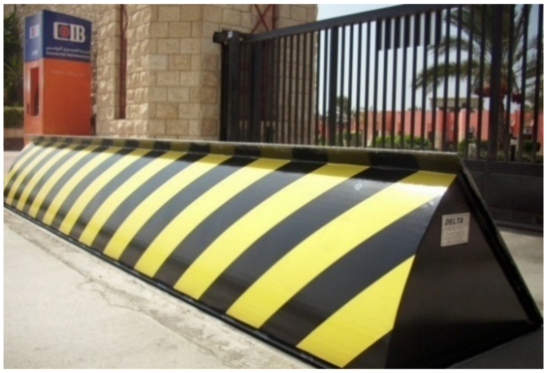


Figure 12 – Permanently Installed Moveable Vehicle Barrier (Delta Barrier or Equal)

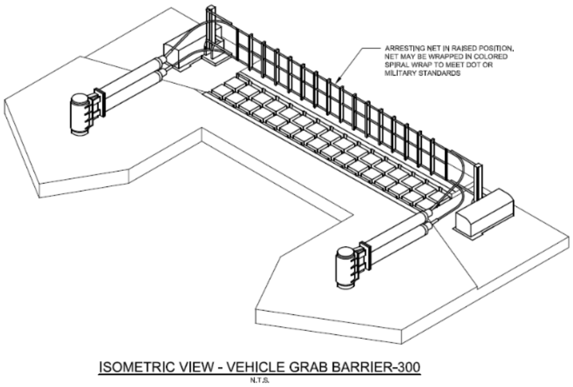

ARRESTING NET IN RAISED POSITION, NET MAY BE WRAPPED IN COLORED SPIRAL WRAP TO MEET DOT OR MILITARY STANDARDS
ISOMETRIC VIEW - VEHICLE GRAB BARRIER-300
N.T.S.

Figure 13 **– Vehicle Arrestor Gate**

6.1.3.3. AOA Guard Post Configuration and Booths

1. A climate-controlled guard booth is required that provides maximum visibility over the immediate area of the station and provides easy access for the guard to carry out the duties of inspecting passengers, vehicles and their contents.
2. Booth foundation shall be on a concrete island with protective pipe guard bollards.
3. The guard booth shall be designed so that the guard can perform all inspection functions without leaving the protection of the guard booth. This includes microphone and speakers for audio communication, bullet-resistant glass (UL Level 3), a transaction drawer that permits the passing of vehicle driver and occupant credentials only.
4. The guard booth shall be designed so it can comfortably accommodate a second guard.
5. Provide adjustable booth interior lighting level and minimum guard post exterior lighting level contours of 20.0 foot-candles around booth and 2.5 foot-candles at end of vehicle queuing line.
6. Dependable and instant voice and video communications from the guard post to the Security Operations Center (SOC) or other appropriate central location should be installed, maintained, and frequently tested.

7. Video from CCTV camera coverage providing face view of driver in vehicle, front and rear view of stopped vehicle, and license plate reader shall be tied into the Port Authority's video management system.
8. A duress alarm system tied to the PAPD and AOC shall be provided.
9. Provide ample vehicle queuing distance and vehicle inspection portals to avoid long traffic backups and delays.
10. Provide a pull-off space for waiting vehicles or for conducting a secondary inspection.
11. Provide turn-around space so that a vehicle denied entry does not have to enter the SIDA to turn around.
12. Provide traffic signals integrated with the vehicle barrier gate.
13. Other guard booth features shall include: crash barrier control panel, LCD monitor, Biometric reader (fingerprint or other), non-corrosive stainless-steel bullet-resistant (UL Level 3) booth enclosure, pedestrian intrusion detection annunciator, 2 card readers, outside fresh air intake protection.

6.2. Identity Checks, Background Screening and Issuance of Photo Identification Badges/Cards

1. No person shall be permitted within the Sterile or Secured Areas without an Airport Security ID Card issued by the Port Authority or an authorized escort. An individual who has previously been denied an Airport Security ID or had access privileges revoked cannot be escorted into the Sterile or Secured Areas at any time. A person who has an Airport Security ID with escort privileges may escort up to five persons into the Sterile or Secured Areas, and must follow the escort procedures as noted in the Port Authority's website at http://www.panynj.gov/airports/security-id-office-escourts.html. Persons that are escorted into Sterile and Secured Areas may be required to submit to a screening program also referred to as "Info-Corp," which checks Federal, state and local databases.
2. Contractor employees who work landside on site at the airport in security sensitive areas may be required to undergo background checks through SWAC and obtain SWAC ID cards. Information on the SWAC process specific to the Port Authority on NY and NJ requirements, including office locations and hours of operation, is available on the following website: http://www.secureworker.com.

7. TENANT AIR CARGO AND AIRLINE SERVICES FACILITIES

7.1. Cargo Facilities and Security Considerations

Generally, cargo facilities are subject to precisely the same physical security requirements for planning and design purposes as any other facility on the airport, although their procedural and operational differences often require some site-specific modifications or upgrades.

7.1.1. Requirements for Air Cargo Screening

1. The TSA requires 100 percent screening of all cargo that is to be loaded on passenger aircraft.
2. TSA has adopted security measures throughout the air cargo supply chain that apply to aircraft operators, foreign air carriers, indirect air carriers (freight forwarders), and participants in the Certified Cargo Screening Program (CCSP).
3. Under CCSP, shippers and other entities can screen cargo at an earlier point in the cargo supply chain, which also has an impact on the planning and design of cargo facilities both on and off the airport.
4. The security considerations during planning and design of cargo facilities revolve around a facility’s location and the type of cargo businesses/facilities: those accepting and processing cargo that will be transported in passenger aircraft; those accepting and processing cargo that will be transported in all-cargo aircraft (freighters); those accepting both types of cargo, and whether the cargo shipping involves international export or import.

7.1.2. Cargo Facility Security Requirements

In general, the following security requirements shall be followed when planning, designing and operating cargo facilities at Port Authority airports. The cargo facility parameters are as follows:

1. Air cargo facilities must be separated from critical passenger loading areas and general aviation areas.
2. The airside ramp area adjacent to air cargo facilities must be designated as SIDA according to ASP (see ASM for further details).
3. Appropriate lighting levels are also necessary around the perimeter of the facility as well as inside the facility with an UPS. An audible alarm, connected to the AOC, to indicate UPS malfunction must be operational when the UPS is activated and in use.
4. On the public side, non-delivery vehicle parking must be separated from truck parking and located away from the building.
5. The public area of the cargo facility must be separated from the Secure/SIDA area by metal fencing or solid walls. Any portals used for personnel access or cargo movements must be closed when not actively used. They may not be left open and must be guarded by guard personnel when open.

6. All personnel must access the Secure/SIDA area through door/portal that allows the passage of only one person at a time (e.g. a HEET turnstile matching the fence height or sally port) and such doors or portals must be controlled by a computerized access control system that is compliant with PA and TSA requirements of denial of unauthorized access, audible alarm, and record retention of all access attempts, etc. The only exception to this rule is personnel in the process of moving cargo across the guarded boundary between public and secure/SIDA sections. If turnstiles are utilized, a section of fence should be added to the top of the turnstile to match the height of the chain link fence, along with concertina wire for any small sections that are exposed, to avoid giving someone the ability to climb the gates.
7. All authorized-personnel doors or gates that permit access to the airside portion of an airport, as well as airside-facing and landside-facing cargo doors, require access control in accordance with the ASP.
8. Emergency exits in the Public Area shall only exit to landside, not AOA/SIDA.
9. Cargo service doors of the roll up variety are required for access control on both the public side and AOA/SIDA side of building and they must be kept closed when there is no active loading/unloading. Cargo service doors that are open must have a security guard posted at all times that the door remains open.
10. Where ventilation is required, rollup doors with small perforations that prevent passing of contraband items are permitted (see Figure 15).

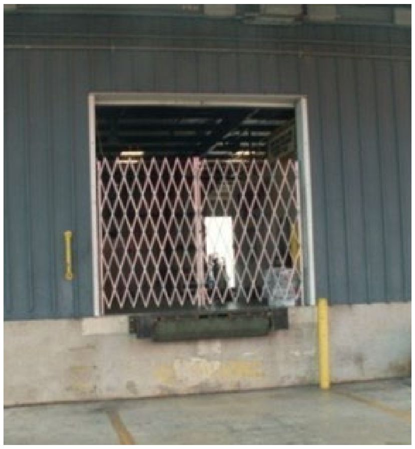


Figure 14 - Scissor Gates are Not Permitted (unless used in combination with additional barrier such as rollup doors)

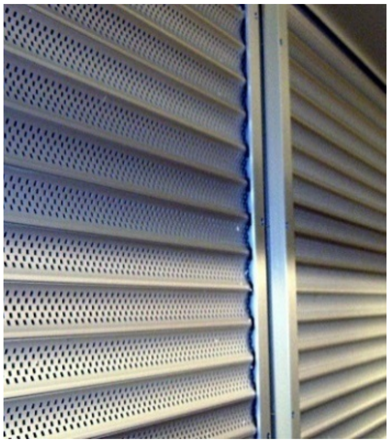


Figure 15 - Rollup Doors With and Without Perforations

11. Cargo Doors with Scissor Gates are not permitted (unless used in combination with additional barrier such as rollup doors) (see Figure 14 and Figure 15). Scissor gates can be used as a barrier

for gaps between the cargo warehouse door when trucks are unloading or receiving shipments but must not be used as the primary cargo bay door.

12. AOA Perimeter security fence meeting the requirements of Sections 6.1.1 and 6.1.2 must be installed from the exterior face of the cargo building to the tenant’s property line, on the AOA fence alignment established by the Port Authority, and physically abutting any existing AOA security fence without any gaps.
13. Cargo screening areas are required to be segregated and items that have been screened shall be sectioned off. Provide adequate space for accepted unscreened cargo and space allocated for bulk pallet inspections.
14. Any public area of a cargo facility must be separated from the secured area by a metal fence or wall.
15. Cargo facilities are required to meet the requirements for Access Control Systems (ACS) in Section 3.4.3, CCTV (Closed Circuit Video Cameras) in Section 3.4.4, and Video Management & Surveillance Systems (VMSS) in Section 3.4.5.
16. CCTV cameras with VMS systems are required at the following locations to monitor, record and store video:
    a. Truck loading dock
    b. Interior of cargo facility including cargo unloading and receiving area, cargo screening area, and staged cargo storage area
    c. AOA service doors
    d. Service counter area
    e. Each SIDA access control portal
17. CCTV cameras shall be mounted high enough and with unobstructed line of sight such that camera views of all cargo handling and screening activities are not visually blocked by cargo handlers, stored cargo or equipment.
18. Any interior offices, hallways, doors, or other space accessible to the public may not provide uncontrolled access to the Secure side of the facility.

7.1.3. Cargo Facility Security Operational Practices

1. A cargo tenant/subtenant is required to submit a comprehensive tenant security plan (CTSP) to the Port Authority’s ASM.
2. Cargo tenants may be required to enter into an EAA (if an air carrier) or an ATSP with the Port Authority, which will be a subpart of the CTSP.
3. All cargo facility personnel shall have their Airport Security ID Card displayed at all times and if applicable, a US Customs seal for CBP security areas.
4. Individuals being escorted must remain within line of sight of escort. A valid temporary badge or escort authorization form must be presented for anyone who is escorted.

5. The CTSP shall also cover security measures that shall be followed to combat insider threat. For this purpose, it is acceptable that the cargo tenant allows TSA to conduct security threat assessments to check the names of workers with access to air cargo against government terrorist watchlists. The threat assessments shall be conducted upon initial employment at a CCSP facility or on-airport air cargo facility and every five years thereafter while employed as an air cargo worker. Employees with SIDA badges have already been screened by TSA.
6. All security service providers, including security guard companies must have a Port Authority privilege permit in order to operate at an airport.
7. All security companies must meet established Port Authority security services guidelines and have the required state license. All security guards must attend SIDA training and PA Security Guard training.
8. The cargo facility has the option to maintain its entire warehouse as secured or SIDA area (depending on airport) or as a combination of SIDA (interior of the warehouse) and secured (exterior/ramp area) areas, as approved by the ASM.
9. Utilize technologies that assist with prescheduled deliveries and/or utilize check-in kiosks to limit the number of visitors in the cargo warehouse at any given time.
10. All aircraft loading/boarding stairs must have locks to prevent unauthorized access.
11. The cargo facility shall schedule the appropriate number of security guards on each shift to monitor all cargo handling and screening activities during both peak, normal and off-peak hours of operation as well as all entrances and exits to the SIDA/AOA.

7.2. Airline Hangars and Other Aircraft Maintenance Facilities

Airline hangars and other 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 requirements for aircraft maintenance facility location, layout and operation include:

1. Compliance with 49 CFR 1542.
2. Aircraft hangars and other maintenance facilities wholly or partially within the AOA are required to meet the requirements for Access Control Systems (ACS) in Section 3.4.3, CCTV (Closed Circuit Video Cameras) in Section 3.4.4, and Video Management & Surveillance Systems (VMSS) in Section 3.4.5.
3. Access control, CCTV and VMS systems are required to prevent, detect and record unauthorized access to the aircraft, or tampering with aircraft parts and equipment.
4. Large hangar doors or openings cannot be relied upon as a security boundary/demarcation line.

5. Location of loading and delivery docks landside shall have provisions and controlled procedures to screen all deliveries for contraband and any items other than aircraft equipment, parts, lubricants, etc. that are to be used or stored within the facility.

7.3. In-Flight Catering Facilities

Facilities for in-flight catering service may be located on-airport (landside, airside, or may be a boundary facility with portions of both) or off-airport. Due to the nature of such facilities, as well as the typical placement near the passenger terminal, security requirements may involve substantial amounts of coordination, both architecturally and procedurally. The Port Authority expects all such facilities to be in full compliance with TSA regulations and to follow best practices for facility planning, design and operations.

Security plans for on-airport in-flight catering facility layout and operation include:

1. Compliance with 49 CFR 1544.
2. An on-airport in-flight catering facility shall be required to provide a comprehensive security plan for Port Authority approval.
3. Access control, CCTV and VMS systems are required to prevent, detect and record unauthorized access to the facility, or tampering with catered deliveries. CCTV coverage must tie into TSA local headquarters and the PANYNJ AOC.
4. Everything brought into the facility or packaged and sealed for delivery to aircraft must be completely screened.
5. All personnel entering the AOA perimeter shall have their Airport Security ID Card displayed at all times.
6. The comprehensive security plan shall also cover security measures that shall be followed to combat insider threat
7. Security guards at Port Authority AOA perimeter guard posts may conduct random checks for compliance with TSA regulations.

8. COMMERCIAL TENANT BUILDING COMPLEXES ON AIRPORT PROPERTY

8.1. Hotels and On-Airport Accommodations

On-airport hotels and their event facilities are either located landside in an independent building or within the public area of an airline terminal complex. Due to the nature of the facility, as well as its placement near or within the passenger terminal, security requirements may involve substantial amounts of coordination, both architecturally and operationally. The Port Authority expects all such facilities to be in full compliance with TSA regulations and to follow best practices for their planning, design and operations.

Security plans for hotel facility layout and operation include:

1. If the hotel is located so that it borders on the AOA/SIDA, there shall be no hotel balconies facing the airside. In addition, any hotel windows facing the airside shall not be openable. These features are to prevent the passing (dropping) of contraband to the AOA/SIDA per TSA requirement.
2. If the hotel is located within the public area of an airline terminal, all hotel entrances and exits, including emergency exits, shall be connected only to the terminal public areas.
3. If the hotel roof borders on the AOA/SIDA, it shall have complete roof access control integrated with CCTV and VMS systems including roof stair doors or roof hatches allowing access only to hotel maintenance staff possessing an Airport Security ID Card.
4. Roof access control systems are required to meet the requirements for Access Control Systems (ACS) in Section 3.4.3, CCTV (Closed Circuit Video Cameras) in Section 3.4.4, and Video Management & Surveillance Systems (VMSS) in Section 3.4.5.
5. All landside deliveries to the hotel through the terminal public area shall be scheduled, delivered, inspected and screened at the terminal loading dock. Hotel deliveries at the frontage roadway shall not be permitted.
6. The tenant shall be required to provide a comprehensive security plan for Port Authority approval which shall cover all security measures that shall be followed to combat threats.

9. GENERAL AVIATION

9.1. Operational Practices

Tenant Fixed Base Operators (FBOs) who operate General Aviation services must follow the TSA Security Guidelines for General Aviation Airport Operators and Users, unless stated otherwise by the ASM. In addition, FBOs comply with the following operational practices:

1. FBOs submit a comprehensive security plan to the Port Authority.
2. Remove air stairs away from larger aircraft when unattended.
3. Use heat shields and aircraft covers to block windows to prevent visibility of the aircraft's contents.
4. Increase accountability for access control onto the AOA, for example stronger pilot and passenger verification processes.
5. Pilots must be escorted by FBO operator at all times on the ramp or a system must be established where pilot is issued with a pass.
6. FBO must have a procedure that requires a pilot to establish a connection (identify) between names reported on a passenger manifest and persons he/she is escorting onto the ramp/aircraft.

9.2. Security Control of Personnel

FBOs who operate General Aviation services, or other GA aircraft at Port Authority airports are required to comply with the following:

1. Escort all individuals visiting the airport into and out of aircraft movement and parking areas.
2. Prior to boarding, the pilot in command shall ensure that: the identity of all passengers is verified; all passengers are aboard at the invitation of the aircraft owner/operator; and all baggage and cargo is identified by the passengers or flight crew.
3. Develop and use an internal "vetted traveler" type of program for regular travelers including completion of a background check before adding the traveler to a list of individuals approved for travel aboard company aircraft.
4. The identity of an individual renting an aircraft requires verification by presentation of a government issued photo ID, an airman certificate and a current medical certificate necessary for that operation.
5. Operators shall establish procedures to identify any pilots and aircraft using their facilities who are not normally based there (transient pilots).
6. Operators providing rental aircraft must first provide the pilot renter with the security awareness training program developed by TSA and shall also familiarize the pilot with local airport operations, including their security responsibilities at the facility.
7. Operators providing rental aircraft shall be vigilant for suspicious activities and report them to the Airport Security Manager or Port Authority Police.

8. Where flight training is permitted, comply with 49 U.S.C. § 44939 and 49 CFR 1552.

9.3. Security Control of Aircraft

FBOs who operate General Aviation services, or other GA aircraft at Port Authority airports are required to employ multiple methods of securing their aircraft to make it as difficult as possible for an unauthorized person to gain access to it by complying with the following:

1. Ensure that aircraft door locks are consistently used to prevent unauthorized access or tampering with the aircraft.
2. Use keyed ignitions for aircraft where appropriate.
3. Use an auxiliary lock to further protect aircraft from unauthorized use and strictly control access to all aircraft keys.
4. If none of the above (3., 4., 5. or 6.) is feasible or acceptable to the aircraft operator, the operator must hire a guard company (with a Port Authority Privilege Permit, if applicable at the airport) to guard the aircraft while parked at a Port Authority airport.
5. When hangars are available at the airport facility, store idle aircraft in hangars with locked doors
6. Park aircraft in the hangar facing away from the door, or into the corner of the building, or any other position of the aircraft that requires a prior engagement of ground handling equipment (towing) for the aircraft to be ready for taxiing. This is also considered secure even if none of the above stated measures are used.
7. Ensure that aircraft ignition keys are not stored inside the aircraft.
8. Practice strict transfer of control for aircraft and keys before and after maintenance procedures.
9. Never leave an unattended aircraft open with keys before or after repairs are completed.

9.4. Security Control of Bags and Baggage

FBOs who operate General Aviation services, or other GA aircraft at Port Authority airports are required to oversee security control of bags and baggage as follows:

1. GA cargo, baggage, or other passenger luggage shall never be left outside the aircraft unattended.
2. An FBO may have its own access gate to the AOA provided that physical barriers are in place (i.e. bollards or jersey barriers) and permission has been granted from the Airport Security Manager.
3. An FBO is not permitted to operate their own vehicle gate with access to the airfield unless the Port Authority and or authorized representative have been notified in advance.

9.5. Security Control of Infrastructure

FBOs who operate General Aviation services, or GA aircraft facilities at Port Authority airports are required to comply with the following:

2. Display signage as directed by Port Authority. Signage may include warning against tampering with aircraft, unauthorized use of aircraft and trespassing, as well as how to report suspicious activity.
3. Hangars shall preferably have a computerized access control system with card readers and access cards. Access codes and cards shall be changed (or manual locks rekeyed) with every new tenant sublet.
4. In addition to hangar door locks, provide an electric bypass switch and/or alarm and intrusion detection system for hangars.
5. Provide adequate levels of lighting without blind spots around hangars and on all airside/landside areas for proper visibility of ramps and parking lots.
6. The Airport Security Manager shall have access to inspect hangars at any time with short notice.
7. GA tenants shall have a strict key or access card control program for hangars which will be periodically audited by the Airport Security Manager.
8. For AOA security fencing and clear zone requirements see Section 6.1.2 Perimeter Fencing.
9. For GA (Non-AOA) perimeter security fencing shall comply with the following:
   a. The minimum fence fabric height shall be 8’-0” above finished grade.
   b. Chain link fabric shall be 1 ¾” x 1 ¾” with 0.192” OD wire, metal coated (galvanized) or polyvinyl chloride (PVC) coated.
   c. Fence shall be topped with 3 lines of barbed wire.
   d. Keep perimeter fencing clear of vegetation growth with applicable “Clear Zone” rule observed.
   e. Fencing shall have no gaps underneath greater than 2”.
   f. Poles of fencing must be buried into the ground/pavement.
   g. Signage that details “no trespassing” must be attached to fence.
   h. Minimize access points to the airfield and ensure they are regularly monitored.
10. Other types of security fences are permissible if previously approved by the Airport Security Manager.
11. FBO’s and other tenants, shall provide outdoor security lighting and CCTV cameras with an uninterrupted power source to monitor and record activities for the following areas:
    a. FBO shall monitor the ramp with the pathway leading to the aircraft in clear sight,
    b. Aircraft parking and hangar areas,
    c. Fuel storage areas and fuel trucks,
    d. Airfield access control points, and
    e. Other appropriate areas, such as vehicle parking, fences, or obstructed areas

10. MAINTENANCE AND CONSTRUCTION ACTIVITY

The Port Authority requires multiple layers of security standards for the performance of contract work, including standards for contractors, their staff, and subcontractors and their staff, which shall depend upon the level of security required, as determined by the Port Authority Airport Security Manager. In addition to following the Port Authority's rules and regulations, a contractor shall, and shall instruct its subcontractors, to cooperate with the Port Authority and its staff in complying with and adopting the following security requirements:

1. All persons entering a Terminal shall comply with all applicable security regulations and procedures as established by the Port Authority pursuant to 49 CFR, Parts 1540 and 1542. Any violations and any subsequent fines imposed due to any violation(s) shall be the responsibility of the contractor.

2. **UPON ISSUANCE OF NOTICE OF AWARD, A CONTRACTOR MUST CONTACT THE AIRPORT SECURITY OFFICE AND REQUEST A SECURITY MEETING TO FINALIZE THE PROJECT SECURITY PLAN (PSP). ALL WORK SHALL BE COMPLETED IN ACCORDANCE WITH THE CONTRACT SPECIFICATIONS AND THE APPROVED PSP.**

3. The PSP is the documentation depicting project specific security requirements and is submitted after a contractor is selected. The PSP is coordinated in detail with the project phasing and includes access points, delivery routes, security guard locations, details for construction of internal security perimeters, identification of worksites, transport of equipment and tools onto the worksite, and any other job specific security requirements. The Contractor shall complete the following portions of the PSP for the review and approval by the ASM or designee:

    a. Name and contact information for the Contractor's Security Coordinator and a designated alternate, who is in charge of enforcing the approved security requirements for the project as a whole.
    b. Name and contact information for each Contract Security Liaison/Worksite Supervisor and designated alternates (can be the same individual) responsible for security requirements unless otherwise approved by the Port Authority.
    c. Approximate dates for each phase of construction, duration, location, and access points. Staging areas must be identified, including, the security measures to control non-badged individuals, equipment, associated tools, and Security Sensitive Information (SSI).

4. The PSP shall also consist of all labor and materials necessary to establish one or more secure perimeters around the construction site and provide personnel to maintain secure access/escorting to and from secure worksites, and within the site itself, for the duration of the project.

5. The Port Authority shall have the right to rescind permission for the use of any access control device and confiscate any Airport Security ID Card for any lawful reason, including, but not limited to, violations of airport security and violations of Airport Rules and Regulations.

6. Any action required by the TSA or the Port Authority in response to security compliance with the PSP shall be addressed immediately by the Contractor at their expense.

7. The following is the general hierarchy of responsibility for personnel working in restricted public/SIDA/Sterile/Secured areas. TSA personnel may contact any individual at any point in the hierarchy. In most cases, the Project Manager/Engineer will serve as the liaison between the ASM and the Contractor. However, direct coordination in emergency situations should be expected.

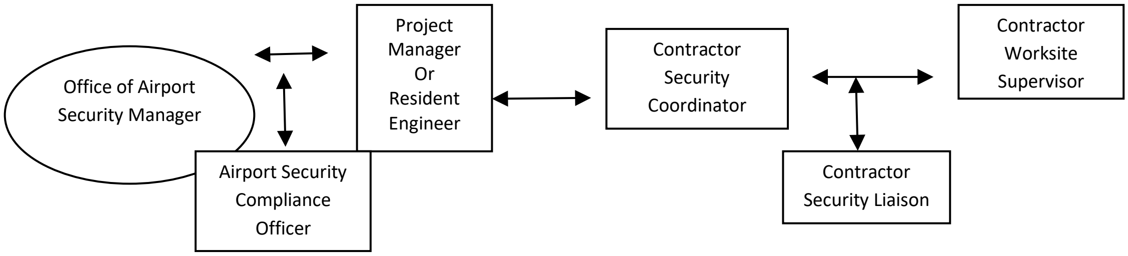

Office of Airport Security Manager
Project Manager Or Resident Engineer
Airport Security Compliance Officer
Contractor Security Coordinator
Contractor Worksite Supervisor
Contractor Security Liaison

Figure 3 – Restricted Area Responsibilities

10.1. Tool Management Plan

The "Tool Management Plan" is for all construction projects that take place in the public, SIDA, Sterile and Secured Areas of a Terminal. Mobilization of the Tool Management Plan must proceed all phases of construction and shall be enforced for the duration of the project. The provisions of the Tool Management Plan are intended to strictly control and account for workers and tools within construction zones and avoid violations of TSA security policies. The Port Authority form: AIRPORT CONTRACTOR SECURITY, TOOL MANAGEMENT AND ESCORT RESPONSIBILITIES ("Contractor's Responsibilities") provides detailed regulatory guidance on rules and responsibilities of contractors, sub-contractors and their employees during construction projects at Port Authority and tenant aviation facilities. The following summarizes critical security measures for workers and tools for projects:

1. Strict accountability of tools through inventories at each shift.
2. Tools on TSA list of prohibited items shall not be removed without authorization from the construction zone.
3. Tools on TSA list of prohibited items shall not be taken through the TSA screening checkpoint.
4. Contractor's security representative shall conduct daily sweeps of construction area for tool and worker compliance.
5. Workers access is restricted to areas and times specified in the PSP.

6. A contractor may be required to use a security guard company approved by the Port Authority if escorting individuals in a Secured or Sterile Area.

The Contractor's Responsibilities must be read and signed by each contractor employee working on site.

10.2. Landside, Terminal & Airside

10.2.1. Security Management Plan

Prior to any work being performed on Port Authority property the PSP along with verification documents attesting to the Employee Background Checks, Tool Management Plan, Perimeter Security Requirements (temporary security fencing and barriers, etc.) and Access Control Plan must be submitted to the ASM for review and approval. The Port Authority form: AIRPORT CONTRACTOR SECURITY, TOOL MANAGEMENT AND ESCORT RESPONSIBILITIES provides specific instruction on compliance requirements for construction projects and workers within the landside, terminal, and airside areas of aviation facilities.

10.2.2. Identity Checks, Background Screening and Issuance of Photo Identification Badges/Cards

No person shall be permitted on or about a construction site in the Sterile or Secured Area (AOA and SIDA) without an Airport Security ID Card issued by the Port Authority or an authorized escort. In addition to displaying IDs issued by the contractor, all employees of the contractor and subcontractor shall wear the Airport Security ID Card or an official escort badge in a clearly visible position. It must be above the waist and below the neck whenever they are working at the construction site.

Contract personnel who cannot get an Airport Security ID Card since they temporarily require access to the Secured Area may be subject to a background check through SWAC for all personnel on this contract. Information on the SWAC process, including office locations and hours of operation, is available on the following website: http://www.secureworker.com

The contractor shall coordinate with the Port Authority at least 30 – 45 business days in advance to submit a company package in order for its employees to obtain Airport Security IDs. For detailed information on the process of obtaining an Airport Security ID can be found at http://www.panynj.gov/airports/security-id-office.html

Airport Security ID Cards are for construction project use only. The contractor and subcontractor personnel shall not use their Airport Security ID at any other location on airport or off airport outside of the construction site. The Port Authority's security auditors and inspectors randomly check for the proper use of Airport Security IDs.

10.2.3. Project Security Guard Plan

The purpose of the Project Security Guard Plan is to prepare, maintain and update detailed security guard and security escort work plans and schedules. These plans must be submitted at least 30 days in advance of each construction stage. The security escort work plan shall be sufficiently detailed to accurately depict all coverage as specified in Port Authority form: AIRPORT CONTRACTOR SECURITY, TOOL MANAGEMENT AND ESCORT RESPONSIBILITIES - “Security Guard Posting Staff Requirements” and “Construction Site Access Control Physical Requirements”, and shall graphically represent the logical sequence and duration of activities, all in accordance with the requirements of the contract.

10.2.4. Radios/Two Way Communication

Furnish to each person assigned to a security post within the project site, including all supervisors and relief personnel, a portable two-way radio voice communication equipment capable of adequate communications throughout the airport including antennas, power supplies, batteries and other associated equipment, with no less than two (2) distinct frequencies, unless otherwise directed by the Project Manager/Engineer and/or Airport Security Manager. This equipment must be maintained in good repair and operating condition. Additional handsets should be supplied for Port Authority personnel’s use in order to maintain contact with project security personnel when necessary.

10.2.5. Admittance to Construction Site

Contractor’s personnel and vehicles may be required to enter the construction site through a secured vehicle guard post at all times, unless otherwise authorized. Contractor’s personnel and vehicles must remain within the construction site at all times during shift activity. Port Authority auditors and inspectors will randomly inspect and monitor the construction site and other airport areas. Violations will result in confiscation of an Airport Security ID Card, loss of privilege to work on the contract and in any Sterile or Secured Area, AOA or SIDA area of a Port Authority airport.

10.2.6. Construction Site Access Control

The Port Authority may provide for construction site access control, inspection and monitoring by security guards retained by the Port Authority at the contractor’s cost. However, this provision shall not relieve the contractor of its responsibility to properly obtain security guards to secure equipment and work at the construction site at its own expense, as stated in the Project Security Guard Plan.

The Project Security Guard Plan must contain specific requirements for the qualifications, performance, uniforms & equipment, static and mobile posts, and reporting responsibilities. The plan includes requirements for both security guards and security guard supervisors and their staffing levels.

10.2.7. Security Guard Posting Staffing Requirements

Haul Route Security Guards

A "Haul Route" shall be a pre-approved path on the Secured Area, clearly delineated in the Plan, where non-Port Authority plated construction vehicles may traverse from a secure access point as indicated in the approved PSP to a defined construction site under escort. Haul route security guards shall ensure all vehicles travel within the designated route as shown in the approved PSP. One security guard shall be posted at a minimum of every 500 feet, provided a clear line-of-sight exists between each security guard.

Work Zone Security Guards

Work zone security guards will generally be deployed in a pre-determined configuration and security function as follows:

- **Entrance and Exit:** A security guard shall be posted at all work site/area entrances and exits and shall be responsible for ensuring vehicles and/or personnel do not leave the area without a contractor provided DR1 or an Authority provided DR2 security escort (as necessary).
- **Perimeter Security Guards**: Perimeter security guards shall be posted when a construction area is defined by low mass barrier. Security guards along the perimeter of the work area shall be spaced no more than 100 feet apart or shall be in accordance with the "Site Security Guards".
- **Site Security Guards**: Any work areas within the AOA that are occupied by construction personnel shall be guarded as a 1:5 (One (1) security guard per five (5) contractor personnel) ratio and work for areas no greater than 100 by 100 feet.

Construction Site Access Control Physical Requirements

All construction areas shall be delineated and protected at all times with barriers and/or barricades. Portions of construction areas, as directed by the Port Authority, including within 600 feet of active runways and/or night work only areas, must be delineated with continuous Low Mass Barriers (LMBs) and protected with guards positioned as required. All other construction areas must be protected and delineated at all times with barricades consisting of a temporary Jersey barrier with eight-foot-high chain link fence, including barbed wire and concertina wire.

All entry and exit points within the guarded work perimeter shall be secured and monitored at all times by contractor provided security guards in combination with barriers and/or barricades. The contractor shall provide area work access control, inspection and monitoring by its retained security guards.

11. ACRONYMS

ADA	Americans with Disabilities Act
AOA	Air Operations Area
AOC	Airport Operations Center
ASC	Airport Security Coordinator
ASM	Airport Security Manager
ASP	Airport Security Program
ATSP	Airport Tenant Security Program
BOH	Back of House
CBIS	Checked Baggage Inspection Station
CBP	Customs and Border Patrol
CBR	Chemical, Biological or Radiological
CCSP	Certified Cargo Screening Program
CCTV	Closed Circuit Television
CDG	Checkpoint Design Guide
CFR	Code of Federal Regulations
CONOPS	Concept of Operations
CPI	Confidential Privileged Information
CSO	Chief Security Officer
DBT	Design-Basis Threat
EAA	Exclusive Area Agreement
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOR	Engineer-of-Record
EWR	Newark Liberty International Airport
FAA	Federal Aviation Administration
FSD	Federal Security Director
FIS	Federal Inspection Services
GSR	Ground Surveillance Radar
HVAC	Heating, Ventilation and Air Conditioning
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
JFK	John F. Kennedy International Airport
LEO	Law Enforcement Officer
LGA	LaGuardia Airport
PA	Public Address
PANYNJ	Port Authority of NY & NJ

PAPD	Port Authority Police Department
PDN	Protective Design Narrative
PIDS	Perimeter Intrusion Detection Systems
PSP	Project Security Plan
SEOC	Security & Emergency Operations Center
SIDA	Security Identification Display Areas
SIM	Security Information Manager
SOC	Security Operations Center
SOP	Standard Operating Procedure
SSCP	Passenger Security Screening Checkpoint
STA	Security Threat Assessment
SWAC	Secure Worker Access Consortium
SWF	New York Stewart International Airport
TAA	Tenant Alteration Application
TEB	Teterboro Airport
TSA	Transportation Security Administration
TSO	Transportation Security Officer
UPS	Uninterrupted Power Supply
VMD	Video Motion Detection
VMDT	Video Motion Detection Tracking
VMS	Video Management System

12. REFERENCES

1. *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attack (Published by US CDC, April 2003)*

2. *PA Technology Department Technology Standards Overview*

3. *Port Authority of New York & New Jersey Airport Contractor Security, Tool Management and Escort Responsibilities* (Revised 6-19-2018)

4. *Port Authority of New York & New Jersey Guidelines for Security Planning and Design at the Inception of Capital and Operating Projects*, May 2005

5. *Airport Planning Standards, Aviation Department – Port Authority of New York and New Jersey,* September 2018, Preliminary Draft, Version 3.

6. *TSA Checkpoint Design Guide (CDG).*

7. *TSA Recommended Security Guidelines for Airport Planning, Design & Construction, Latest Edition*