PORT AUTHORITY NY NJ

AIR LAND RAIL SEA

Airport Security Guidelines Manual

Version – 1.0

Access Control

Situational Awareness

Security Operations

Emergency Communication

Revision History

Revision No.	Description	Date
0	Initial Release	December 30, 2019
1	Airport Security Guidelines Manual – Version 1.0	June 17, 2024
2		
3		
4		
5		

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

The guidelines in this document are intended for Port Authority of New York and New Jersey (hereinafter referred to as "Port Authority", "Authority", or PANYNJ) staff, airport tenants and consultants or contractors that tenants retain to perform design and construction. It is a single document that captures the requirements, is regularly updated, and serves as a guide to security standards that shall be followed at all Port Authority airports. Note that compliance with these security guidelines carries with it no guarantee of protection against acts of terrorism, other crimes, or any of their consequences. While following it will help reduce risk, it cannot eliminate it. All tenants, passengers, service providers and employees at the airports must take their own reasonable standards of care and responsibility associated with the use and application of information provided in this guideline.

1.1. Purpose

This document (hereinafter referred to as the "Airport Security Guidelines Manual" or "Guidelines") serves as a guideline to the security standards that have been established by the Port Authority for the planning, design, construction, operation and maintenance of tenant facilities at its airports. These security standards incorporate the guidance issued by the Transportation Security Administration ("TSA"), aviation industry best practices and the Port Authority's own requirements which it has put into practice for the safe and secure administration of its airport facilities, sites and spaces.

These security standards are intended to inform existing and prospective facility planners, tenants, security managers, and vendors of security considerations to be addressed in accordance with Port Authority security policies and the general threat environment. These standards supplement standard building code requirements for any Port Authority agreements. It should be noted that the Guidelines will be incorporated into new Port Authority Aviation Department agreements as well as renewals, however exclusion of the Guidelines in these agreements shall not be construed as an exemption from implementation. A tenant may construct or alter its premises with measures that are in addition to the Guidelines, however, it must adhere to the minimum requirements of the Guidelines. The Port Authority may conduct surveys of a tenant's leasehold prior to, during and after construction or an alteration to ensure compliance with the Guidelines.

The Port Authority has implemented a strategy to provide a holistic and all-inclusive view of airport-wide systems and activity to increase situational awareness at its properties in support of security and life safety. This will occur across multiple mixed-use facilities, while allowing individual stakeholders to operate and manage their respective areas independently. The intent is to provide for better communication, coordination, logistics planning and response to any event or incident that occurs onsite; thereby aiding in keeping all stakeholders informed about what is occurring at neighboring buildings within the given property or campus. When potential threat events are detected, operators can be alerted of the condition and provide the corresponding emergency response protocols.

Tenant security managers and planning developers shall refer to the Guideline for fundamental requirements for security designs, technologies, and protocols to be applied to design and operations at Port Authority aviation facilities. The intent is to maintain a culture and environment where security is always a central consideration in planning, design, construction, and operations. The security requirements for specific premises as required by this Guideline shall be incorporated into the tenant "Comprehensive Security Plan" which will be approved by the relevant airport ASM.

The standards described in the Guidelines assume that the tenant'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.

1.2. Threats to Airport Safety and Security

The basic threats from terrorism can take the form of physical attack using conventional weapons, vehicles, explosives, flammables, chemical, radiological, 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, shall be considered in planning and operating safety and security measures.

1.3. 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 tenant security programs, and construction -related security plans. The ASM is charged with mitigating security risk to the airport through use of security audits and risk assessments to identify vulnerabilities, engagement of airport employees in awareness programs, training PA and tenant staff in best security practices, recommending capital security improvements, and implementation of 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 and surveillance and inspection patrol. The ASM works in close collaboration with the Airport Manager and staff, Port Authority Police Department ("PAPD"), the TSA, CBP, and FBI. It is also noted that security threats are ever evolving so tenants should check with the ASM for the latest information in this area.

1.4. 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 these Guidelines.

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 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 (ACS)
- Video Surveillance System (VSS)
- Video Management & Surveillance Systems (VMSS)
- Public Address Systems (PAS)
- Automated License Plate Recognition Systems (LPR)
- New Security Technologies and Protocols
- Cybersecurity
- Backup Power for Security Systems

To be effective, these security systems shall be well planned and integrated in a manner that results in an error-free logic to assure that they achieve their 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 shall 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.

Additionally, all technology systems that are part of construction or renovation must be covered by a comprehensive maintenance plan or contract beyond the initial warranty that is provided as part of installation (the “Comprehensive Maintenance Plan”). These Comprehensive Maintenance plan shall ensure the technology systems are kept up to date with the latest manufacturer approved firmware and software patches, software version upgrades, and general maintenance associated with technology systems. This may include physical work such as ensuring hardware is kept cleaned, filters changed and kept dirt/dust free, that HVAC systems supporting technology

are kept in good working condition, and that batteries associated with UPS systems are tested and replaced on a regular basis. Further, necessary system administration of software must be accounted for and included such as software maintenance, backups, archives, and any other tasks required to maintain system functionality. These systems must be maintained and kept in good working condition for their entire useful life and must not be allowed to degrade overtime due to lack of maintenance.

The tenant shall also have a Cybersecurity policy and plan that covers all airline terminal computing resources and is complied with by all airline terminal employees who have access to the computing resources the ("Cybersecurity Policy"). It is intended to clarify and ensure that computing resources are used in a professionally responsible manner and that appropriate steps are taken to safeguard the confidentiality, integrity and availability of all related computing resources, information, data, and equipment.

The Cybersecurity Policy shall include all IT networks, systems and applications operated on site by the tenant. The Cybersecurity Policy shall also be responsible for articulating requirements for the tenant as an external IT partner accessing Port Authority networks. The Cybersecurity policy, and technical requirements shall cover all tenant personnel (such as employees, contractors, vendors, and other individuals), regardless of whether they directly or remotely access Port Authority IT systems and networks.

As a minimum the Cybersecurity Policy shall be in compliance with the TSA's Cybersecurity Emergency Amendment issued on March 7, 2023 (TSA EA 23-01), and all subsequent revisions to that amendment. TSA EA 23-01 requires that impacted TSA-regulated entities develop an approved implementation plan that describes measures they are taking to improve their cybersecurity resilience and prevent disruption and degradation to their infrastructure. They must also proactively assess the effectiveness of these measures, which include the following actions:

- Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate if an information technology system has been compromised, and vice versa.
- Create access control measures to secure and prevent unauthorized access to critical cyber systems.
- Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations.
- Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology.

2.2. Cyber Vulnerability Testing

The tenant shall also perform periodic testing of all their IT systems to uncover vulnerabilities before cyber criminals find them. Technical vulnerability testing, especially when combined with

parallel evaluations of IT administrative processes and procedures, provide Cybersecurity officers, compliance auditors and system mission managers with important information regarding risks to their IT networks, client/servers and applications. The results of cyber vulnerability tests are used to make risk-based decisions regarding the deployment of new systems/applications, drive more purposeful protection policies, better secure (i.e., hardening requirements) networks/systems and address weaknesses in administrative support processes.

2.3. Two Factor Authentication

Port Authority policy articulates security requirements for implementing a two-factor authentication system to protect the Port Authority, when a tenant is connecting to a Port Authority system through an external network connection via VPN. An authentication factor is an independent credential category used for verifying one's identity. The three most common categories are described as, something you know (knowledge factor; i.e., password), something you have (possession factor; i.e., smart card) and something you are (inherence factor; i.e., fingerprint). One of the primary attack vectors for both cybercriminal and white hat hackers is to access potential targets via vulnerable external network connections (ENCs). ENCs include, for example, employees, consultants and contractors connecting remotely via VPN to Port Authority networks. Using two-factor authentication mechanisms reduces the risk of exploiting these classes of external connections.

2.4. Remote Access

Current Port Authority policy precludes any remote access to Port Authority IT and OT/ICS networks from any foreign owned/operated networks. Accordingly, a temporary exception is required from the Port Authority Chief Security Officer to enable said network access. For a list of temporary exceptions contact the ASM.

2.5. Backup Power for Security Systems

All security system shall have as a minimum, a four (4) hours uninterrupted power source (UPS) and a dedicated emergency power generator backup for the system, except the PSLS Radio should have eight (8) hours UPS. An audible alarm, connected to the AOC to indicate UPS malfunction must be operational when the UPS is activated and in use.

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 aircraft operator 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 public, scheduled commercial aircraft passengers and property occurs.

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

1. Restricted access to the AOA, 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 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.
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, as may be amended from time to time. The Airport Planning Standards establish a general set of standards and performance criteria to maintain safe, functionally efficient, and code-compliant terminal area operations while ensuring airport customer satisfaction. The Guidelines 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 airport tenant and space permittees assumes responsibility for specific security systems, measures, or procedures, except for such systems, measures or procedures maintained by law enforcement. Crime and law enforcement at Port Authority NYC metropolitan area airports is under the oversight of the PAPD, members of which are armed, patrol the airports, and constitute the first line response force to any emergency, criminal or otherwise on airport property. Airport security policies, regulations, and protocols that all tenant terminal operators and airlines are required to follow are under the management and enforcement of the **Port Authority civilian ASM or ASC.**

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 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 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 non-Public Area, as it generally includes security areas to which certain requirements apply under 49 CFR § 1542 (e.g., the AOA, fuel farms 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, but are not limited to, patron and other public parking lots and garages, walkways, public access roadways, rental car facilities, taxi and ground transportation staging areas, Air Train stations, and any other on-airport tenant facilities that serve the public such as hotels.

Landside infrastructure also includes facilities that are critical to the continued day to day operation of the airport. These include Port Authority owned and operated assets such as: office buildings, maintenance facilities, electric substations, PAPD facilities, and parking facilities for Port Authority vehicles, among others.

Based upon the Port Authority's agency-wide risk assessment for its airports, which considers 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 facilities 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 Secured 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 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 force protection engineer to perform security planning based upon the threats provided by the Port Authority for the specific airport. The aforementioned security professional, who will serve as the engineer of record (EOR) for blast analysis, blast mitigations and for any other analysis of physical effects from established threats, shall demonstrate sufficient previous experience in completing force protection 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 of New York and New Jersey Information Security Handbook, Revised April 2, 2018, as may be further amended (the "Security Handbook"). Only the Secure Worker Certification: "Secure Worker – High" will be accepted. Secure Worker Certification: "Secure Worker – Limited" will not be accepted.

The developer shall be required to designate a Security Information Manager (SIM) to ensure that the Security 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). 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) employ 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. The Port Authority Document "Security Planning Guideline: Guideline for Security Classification, Planning and Design at Project Inception for Port Authority and Tenant Projects" is a useful reference and provided detailed explanations for these processes.

The definition, communication, and transmittal of information that is classified as Sensitive Security Information shall strictly follow the requirements contained in the Security Handbook (see Appendix). This includes obtaining required security credentials through background checks, training, and strictly adhering to proper classification, marking, handling, transmittal, and storage of security information.

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. Security Planning and Design must be introduced at Planning Inception and followed throughout the Design and Construction phases. The Security Level Categorization is used to prioritize the security efforts and allocated resources more effectively to safeguard the most critical information and systems. It is determined through SPM at project inception. Once categorized, the Security Design Criteria identifies whether the project is classified as confidential or confidential & privilege, that must be followed through each phase of the project.

Selected PDN security design options shall follow throughout the design/construction stages of the project and be reflected in the design and construction submittals.

TSA best practice guidelines are considered a minimum requirement at 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:

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 VSS, video analytics, LPR, etc.) at curbside, doorways and perimeters, and within the departures hall, baggage claim and arrivals hall areas (see Section 3.4.6 and Section 3.4.7)
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 the TSA Guidelines) and technology at those entry points that will screen 100% 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 requirement related to its premises.
8. The comprehensive security plan shall also include design elements or reduce eliminate loiterers including the use of roll up doors, and security shutters to close off concession space at night or when business operations are closed.

In addition to the above security requirements, airport terminal design shall incorporate applicable safety and security strategies from the recommended practices for Crime Prevention Through Environmental Design (CPTED) as outlined in APTA Standards Development Program

Recommended Practice (APTA SS-SIS-RP-007-10) by APTA Transit Infrastructure Security Work Group.

3.4.3. Security Requirements for Terminal Emergency Egress Paths

1. Emergency egress vertical exit paths (enclosed stairways) and horizontal corridors in Public Areas shall only exit to landside, including muster points.
2. Sterile Area egress vertical exit paths, horizontal corridors and muster points shall be separated from the Secure and Restricted Areas including all critical Back of House (BOH) spaces.
3. Where a floor plan cannot provide a separate Sterile and Secure area emergency egress path at a certain location, the doors exiting from the secure side shall be equipped with FAIL SECURE, so that exiting sterile passengers will not be able to enter the Secure Area.
4. Restricted Area (Public Side) emergency egress path exits shall not lead to Sterile, Secure and AOA spaces.
5. There shall be no “free flow” from Secure Areas to Sterile Areas and vice versa.
6. Primary and secondary emergency egress paths leading to the AOA side of the terminal shall avoid design conditions that intersect with active airside operations areas such as baggage cart paths.
7. A detailed ConOps for Terminal Emergency Egress Paths shall be developed and accompany the submittal of egress plans to the Port Authority for review by the CSO.

3.4.4. Airline Tenant Security System General Information, Sharing and Coordination with the Authority

General Information:

1. Security: The transmission of the video signal shall be secure and meet the minimum-security requirements defined by the PANYNJ.
2. Information Security / Non-Disclosure: These requirements and specifications about equipment installed as well as video images and data sharing are sensitive. The parties will restrict access and disclosure to such information to those with a need to know.
3. Maintenance and Support: Tenant shall be responsible for any ongoing maintenance support that is required for their tenant-owned base systems (i.e. video surveillance system, access control, specialty sensors, etc.); however, any maintenance support required for the connectivity to PANYNJ systems will be the responsibility of the PANYNJ. Tenant agrees to allow PANYNJ physical space in their building data rooms to install and maintain equipment necessary for connectivity. Exact location of equipment shall be discussed and agreed upon by both parties. There may be cases where PANYNJ equipment may not need to be installed in tenant spaces, but rather adjacent spaces or buildings.
4. Floor plans and maps: Tenant shall share electronic files of relevant floor plans and maps of their leased space. These files should include clean architectural level drawings for use in PANYNJ systems with the intention of placing cameras and sensors on the maps for

monitoring and situational awareness purposes. Such files should also include drawings and floor plans showing the location of cameras and sensors for the PANYNJ to use as reference when locating devices, creating emergency response plans, etc. Any updates to the leased space, and subsequent updates to any floor plans or maps should be shared with the PANYNJ as well.

Note: Construction drawings showing details related to the physical construction of an area or facility will not be deemed acceptable, as the intent of this requirement is to use the floor plans and Maps for end users at computer workstations once the area or building is completed. Therefore, clean, consolidated, floor plans showing final as-built conditions of all areas shall be provided to Port Authority for this use.

5. Tenant terminal operators are required to provide the information identified in paragraph (6) below for the specific electronic security systems listed herein:

    a. Video Management System
    b. Airport Security ID Card Access Control System
    c. Gunshot detection system (if applicable)
    d. Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) detection systems (if applicable)
    e. Automated License Plate Recognition Systems

6. Required Security System Information for each electronic security system listed in the preceding paragraph (5), tenant terminal operators are required to provide information related to the manufacturer and vendor of the security systems, if a selection has not been made, terminal operators must keep the Port Authority apprised of the vendor that is chosen. This will allow for appropriate planning and interface plans to be completed to meet the requirements of this document. The information required to be shared with Port Authority includes:

    a. Name of the manufacture and product, along with version of software being installed.
    b. Point of contact from the manufacturer that can provide technical information to the Port Authority about the system, and about any available software development kits or API's for integration to third party systems. Note, any requirements from the manufacturer that are needed to provide third party camera sharing to the Port Authority shall be the responsibility of the tenant/stakeholder to provide (i.e. software license for SDK or API).
    c. Point of contact from the tenant who will be managing the integration effort with PANYNJ.

7. Both parties agree to work together to meet the requirements of the Guidelines including all the features and functions listed below:

    a. Network Connectivity:

        i. Tenant will provide connectivity and share data connections for the video surveillance system contained in its leased space with PANYNJ. The tenant's

participation in this aspect of integration will increase the PANYNJ's ability to share critical information with first responders during a large-scale event and respond proactively to potential threat events that may adversely impact other facilities and locations throughout facility campus.

ii. For the program strategy to function as designed, network connections from tenant space to PANYNJ must be established. Tenant agrees to provide space and power for PANYNJ to install network appliances, conduit, and wire to connect to the facility-wide network.

iii. Costs for tenant network appliances along with conduit and wire installation will be the responsibility of the tenant, and costs for PANYNJ network appliances along with conduit and wire installation will be the responsibility of PANYNJ; however the tenant is required to make the Port Authority aware of any opportunities to include the necessary conduit and wire installation as part of any new construction or renovation activity, so that proper planning can be made in conjunction with the tenant.

b. As necessary, the parties shall proceed in good faith and with all due diligence to finalize a plan for data sharing and agree to work collaboratively on additional systems in the future, such as fire alarms systems, CBRNE (if they become available) and others deemed mutually beneficial for integration.

3.4.5. 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 Make-up Areas
8. Baggage Belt from Public Area

Security systems, such as VMSS and electronic access control systems, must be integrated with an operations center VMS or Security Operations Center (SOC), operating on a 24-hour basis with dedicated and trained security operations staff. The system shall be tied into the PANYNJ's Airport Operations Center (AOC) and there shall be a five (5) minute or less response to door alarms (violations) or other access incidents, as designated in the Airport Security Program.

All elements covered herein for the ACS shall have an uninterrupted power source (UPS) that can sustain operations for a minimum of four (4) hours. An audible alarm, connected to the AOC must be operational when the UPS is activated and in use.

3.4.5.1. 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 portals 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. Contactless electronic card access reader to unlock door.
2. Monitored and audible alarm sounds when door is unlocked or opened without access card.
3. VSS view of individual accessing and egressing, and two-way voice communication (located on both sides of 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 two-way voice communication tied and integrated into the SOC so that camera view automatically records and displays visual and audible alerts, VSS and voice communication on console screen when any component is activated.
5. Capability to upgrade to/add biometric identification ID layer (see Section 3.4.5.6).
6. Minimum four (4) hour uninterrupted power source (UPS) and generator backup 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.

3.4.5.2. Access Control to Back of House Areas (BOH)

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 BOH spaces to authorized tenant operations and maintenance staff shall be ACS monitored and controlled and locked based on the BOH utility space door or hatch type and must meet the requirements in Section 3.4.5.1 above.

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.

3.4.5.3. 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 by local controller.
3. Alarm monitoring shall not be interrupted.
4. Access control passages shall be operational without any failure.

5. ACS management functions.

Tenant planners shall coordinate with the Port Authority during the design phase, for direction on connectivity to the 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.
9. Gunshot Detection System.
10. Building Management System.
11. Weapons Detection System (if applicable).

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's revokes their airport access badge. 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.

3.4.5.4. Electronic Access Control and Alarm Monitoring Systems (ACAM)

Specific areas that will be viewable from the Access Control/Alarm Monitoring System shall include, but shall not be limited to:

1. Doors and/or portals leading to runways or AOA areas or corridors; Alarms shall be correlated with the associated VSS providing a visual record of any door breach or alarm event.
2. All doors from any Public Area to any Security Identification Display Area or Secured Area.
3. Panic or duress alarms that may be installed and associated with employee or public safety events.

The Port Authority uses Lenel OnGuard for Access Control and Alarm Monitoring application. Any data sharing or third-party interfaces that may be required shall be compatible with the Port Authority system. Additional dialog will be required to work through the specifics of any design that may or may not be needed.

3.4.5.5. Access Control System Management Policies

The Port Authority requires that the 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.
4. Store tenant access control data for a minimum of three (3) years (i.e. alarms, access granted, denied, etc.).
5. Install alarms that will sound if and when a cabinet storing sensitive security information is accessed.
6. Store tenant card holder record data for a minimum of seven (7) years (i.e. people who have or had a badge in the past seven years and associated personnel data for cardholders).

3.4.5.6. Biometric Authentication

Fingerprint readers, facial recognition Video Surveillance Systems (VSS), 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. Terminal operators shall coordinate with the ASM to determine the necessary requirements. Any TSA regulated access point can only be controlled by access media issued by the Port Authority Credentialing Office (SIDA cards). Alternate access media to BOH areas which is not a regulated access point may be approved by the ASM. All requests for this must be provided to the ASM prior to the submittal of any contract drawings for Port Authority approval.

3.4.5.7. Badging or Credentialing

Each Port Authority airport has an ID Office location at which airport-specific credentials are issued. An Airport Security ID Card, when properly displayed, shows that the cardholder is permitted access to non-public, Secured or Sterile Areas of the airport to perform their job duties. All persons entering non-public, Secured or Sterile Areas shall comply with all applicable security regulations and procedures as established by the Port Authority pursuant to 49 CFR, Parts 1540 and 1542.

3.4.5.8. Electronic Card Access

At a minimum, tenant electronic ACS system 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 present.
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. fingerprint, iris, or facial identification).
12. Access Control events and Transaction Data shall be kept for a minimum of three (3) years by the airline terminal operator.

3.4.5.9. Manhole Lock Systems (Access Covers)

All utility manholes included but not limited to 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.

3.4.6. Video Surveillance Systems (VSS)

At a minimum, tenants are required to plan for, install, maintain, and operate a comprehensive Video Surveillance Systems (VSS). The VSS shall provide continuous views of persons for tracking from the point of entry to the terminal (i.e., terminal roadways and sidewalk), all the way through the terminal, passenger screening checkpoint, and up to the boarding gate, except for restrooms, and 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 this Guidelines.

3. At a minimum, camera display and storage system image quality shall be capable of Identification Surveillance, however it should be noted that not all areas may require that level of resolution, see Section 10.2.8 for additional information.
4. Enable all VSS 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 video stream upon Port Authority request to be used for any lawful purpose (i.e., forensic, law enforcement).
6. All elements covered herein for the VSS shall have an uninterrupted power source (UPS) and generator backup that can sustain operations for a minimum of four (4) 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 VSS camera locations that are integrated with the Access Control System under Section 3.4.5 and Video Management & Surveillance Systems under Section 3.4.7, provide the following minimum camera coverage for situational awareness and incident management in airline terminals. The Surveillance Levels for these areas will vary depending on the operational need and design of the terminal, review of surveillance levels shall be provided to Port Authority as part of the design process; see Section 10.2.8 (Surveillance Video Design Methodology) for additional information:
    a. Coverage of landside areas including but are 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. Building perimeter ensuring all means of ingress and egress are covered by VSS.
    c. Coverage inside the terminal from the terminal entrance/exit doors all the way to the departure gates including but not limited to terminal Public Areas, pre-TSA checkpoint queuing, ticketing, baggage claim, meter greeter, ground transportation, unclaimed baggage, concessions, and all BOH spaces.
    d. Coverage of the security screening areas.
    e. Coverage of airside areas including, but not limited to: AOA entry/exit points.
    f. 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.
    g. Coverage of Secured Areas, specifically the Ramp and Aircraft gate areas.
    h. Coverage of baggage make-up areas and TSA baggage screening areas.
    i. Cameras that view the loading dock areas and adjacent corridors and spaces.
    j. Cameras that view the critical infrastructures rooms/closets (mechanical rooms, electrical rooms, water tank rooms, telecom rooms, etc.).
    k. Cameras that view the fire stairwells and cameras located inside the fire stairwells.

3.4.7. Video Management & Surveillance Systems (VMSS)

At a minimum, tenant Video Management & Surveillance Systems (VMSS) shall be configured to reliably meet the following performance criteria which includes the requirement that the VMSS shall be configured to be shared with the Port Authority ASM and/or PAPD upon request:

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 with (monitored and displayed by) the Port Authority upon request on a 24/7 basis, and on stored media if requested.
5. Store all VSS streams for a minimum of thirty-one (31) days for future retrieval. The OCSO shall have the ability to access to the feeds.
6. Configure the distributed video recording server architecture and supporting software application to allow each of the management or head-end 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 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 uninterrupted power source (UPS) that can sustain operations for a minimum of four (4) hours. An audible alarm, connected to the AOC to indicate UPS malfunction must be operational when the UPS is activated and in use.
9. See Section 10.2.8 Surveillance Video Design Methodology for additional information related to VMSS.

3.4.8. 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 3.4.5.2 Access Control to Back of House Areas).
2. Contractor shall furnish equipment with the most current compatible version of firmware and software. Additionally, provisions shall be made to ensure the equipment is running the current compatible version of firmware and software at all times.

3.4.9. TSA Checkpoint VSS and VMSS Requirements

When the TSA Checkpoint VSS and VMSS systems are the responsibility of the lessee and/or terminal developer and are to be integrated into the terminal systems, the following shall apply:

1. For VSS coverage of TSA Passenger Security Screening Checkpoints (SSCP), see the requirements in TSA Checkpoint Design Guide (CDG).
2. TSA prefers VSS design as an extension of an existing facility security system within the airport. When VSS 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. Access to the system shall also be provided at PAPD locations on airport property which may be outside the terminal. Tenants shall coordinate with Port Authority for specific details on how to achieve that functionality for PAPD.
5. VMSS system shall be configured so that any camera streams 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. Notify the Port Authority, TSA and ASM when ACDTV Systems are modified, extended or restructured at checkpoints. This includes maintenance activity that may take the ACDTV system offline during maintenance window. Times and schedule of maintenance activities must be coordinated with TSA and ASM.
8. Provide full size design drawings to the local TSA office assigned to the specific Port Authority airport that show the following:
    a. VSS & Electrical System Abbreviations, Symbols and General Notes
    b. Camera Mounting Details, system demolition (components to remain or be removed)
    c. VSS schedule indicating the focus, aim, mounting, and applicable remarks for each new or existing camera.
    d. Clean floorplans that clearly show architectural layout of checkpoint areas and camera locations for use by TSA and Port Authority for familiarity and situational awareness purposes.

3.4.10. Public Address Systems (PAS)

1. Public Address Systems (PAS) must be sufficiently flexible to handle the various planned usages including emergency notifications.
2. PAS 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.
   PAS 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.

4. PAS 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.
5. PAS shall have a minimum four (4) hour uninterrupted power source.
6. PAS shall be connected to the Port Authority central monitoring station for the purpose of auditory monitoring and for remote operation in an emergency.
7. The PAS shall be tied into the Port Authority AOC. Actual emergency messaging may come from PAPD as directed by the Incident Commander.
8. The PAS shall allow the AOC and other areas designated by the ASM to have message programming/overriding capability.

3.4.11. 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 PAS 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 uninterrupted power source (UPS) and generator backup that can sustain operations for a minimum of four (4) hours. An audible alarm, connected to the AOC to indicate UPS malfunction must be operational when the UPS is activated and in use.

3.4.12. HVAC Systems

HVAC systems must 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 VMSS (or by another type of unauthorized entry detection system).
3. The HVAC systems shall have a highly effective air filtration system (MERV 14 or higher) 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 CBRNE attack..
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 VMSS.

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

3.4.13. 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 and for use by PAPD canine operations at the terminal frontage.
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.

3.4.14. 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, weapons, and other threat detection technologies such CBRNE 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.

3.4.15. 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 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.

3.4.16. Expansion and/or Replacement of Security Systems Areas

It shall be the responsibility of the airport tenant to expand, update or replace any of the above listed BOH Systems and TSA Checkpoint VSS and VMSS under above Sections (Section 3.4.5 through 3.4.15) in the event the Port Authority is no longer supporting installation of these systems outside of the previous original tenant agreement. Additionally, these systems must be kept in a state of good repair and required functionality must be maintained throughout their useful life. This includes ensuring appropriate maintenance contracts are put in place to maintain the physical and logical (i.e. software upgrades and patching, administration) beyond the warranty period and for as long as the system or component or equipment is in use.

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 VSS 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, etc., 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. Access control readers shall be installed at the checkpoint to verify that a displayed badge is valid.
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, possibly with delayed egress hardware.
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. Sterile Area exit locations/boundaries shall not exist in areas where there is a high passenger traffic (sterile or public). They shall be located a sufficient distance away from any high traffic walkways, corridors so as not to potentially confuse passengers as to their travel path to areas other than the exit location.
6. Security personnel stationed at Sterile Area exit locations/boundaries shall be stationed just outside of the sterile/public boundary line on the sterile side of the exit portal.
7. 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.
8. New terminal plans shall provide as much distance as possible between exits from the Sterile Area and the nearest TSA screening checkpoint. 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 an Airport tenant's Secured Area, Sterile, 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 (Exclusive Use Area). 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.

The Port Authority has the right of inspection of a tenant's operating area to determine compliance with security requirements.

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 are considered exclusive use areas, except that a tenant 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.

The Port Authority has the right of inspection of a tenant's operating area to determine compliance with security requirements.

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.
6. Recognition Surveillance of these areas with coverage adequate for the usage of video analytics and police investigations, minimizing blind spots or sizable gaps in coverage.

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 minimum distance of 18” and maximum distance of 36” 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 sleeves 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” 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 VMS.

Figure 2a – Security Bollards at Terminal Frontage Roadway

Standard for Test Method and Bollard Crash Rating	Rating	Vehicle Weight (Lbs.)	Vehicle Speed (mph.)	L or P Rating	Allowable Truck Bed Penetration (ft.)
For Existing Bollards Certified Under DHS K-Ratings (US DOS Crash Test March 2003)	K – Ratings			L - Rating	
	K4	15,000	30	L1	20 – 50
	K8	15,000	40	L2	3 – 20
	K12	15,000	50	L3	< 3
ASTM F2656-07 Standard for Vehicle Crash Testing of Perimeter Barriers (Current Equivalent to OHS K-Ratings Above)	M – Ratings			P – Ratings	
	M30	15,000	30	P4	> 98
	M40	15,000	40	P3	23.1 – 98.4
	M50	15,000	50	P2	3.31 – 23
				P1	< 3.3

Figure 3b – Crash Test Ratings for 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. See Figure 3 for an example of Blast Resistant Glazing System.
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 either PAPD or the terminal operator can restrict access by taxi drivers, “for hire” drivers and others meeting arriving passengers to the sidewalk frontage area only, due to security, safety or other operational concerns.
5. Entry/exit portals shall be designed with sufficient width to accommodate mass pedestrian exit during emergency evacuation.

Figure 3 – Blast Resistant Cable Supported Building Facade

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 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 other critical airport infrastructure (Section 3.3). 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 parking structures from the vehicle size 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 doesn't 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 VSS.
8. LPRs shall be installed at the access entry and exits points, and shall be integrated with VSS.
9. 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.
10. Consult with the ASM to identify and determine physical and electronic security countermeasure requirements.

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

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

Terminal operators shall coordinate their security operations and communications plans with PAPD by working through the Airport Security Manager for approval, to implement the following criteria:

1. Provide sufficient security staffing at the terminal frontage to support the continuing movement of vehicles and the avoidance of any vehicles being left unoccupied.
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 3.4.13.

Figure 4 – Airport Luggage Screening Signage Advisory

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.

4.6.2. Terminal Public Areas

The Public Areas of the terminals consist of airline ticketing counters, baggage claim, and may also have retail stores, restaurants, elevators, escalators, seating areas and other spaces in the terminal departures and arrivals hall Public Areas. Newer and recently renovated airline terminals, designed after the establishment of the TSA and TSA operated passenger screening facilities at airports have decreased the size of Public Areas in the pre-screening zone and have located most public facilities including waiting areas, retail, dining, and traveler club facilities beyond the TSA screening zone. However, airline terminals that continue to have waiting areas, and other Public Areas in the pre-TSA screening zone are required to diligently monitor those areas via VSS coverage for any suspicious behavior and have assigned security staff to intervene and notify PAPD when there is any suspicious behavior. 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 VSS. VSS coverage shall be sufficient to cover all areas where the public gather upon departure or arrivals. See Section 3.4.6 on VSS.
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. Self-service 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 claims or TSA screening lines. Where such sight lines are unavoidable, bullet proof glass shall be installed on stair and balcony parapets that look down on Public Areas.
8. Minimize the number of terminal entry point 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.

4.6.3. 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, passenger pick up of checked firearms shall be in a separate location from the baggage claim area.
3. The procedure for picking up a checked firearm is as follows:
   a. Firearm must be in a locked box.
   b. PAPD is notified that a passenger is picking up a checked firearm at the terminal. Follow any instructions given by PAPD.
   c. Passenger must first be escorted out of the terminal by a security guard before being handed the firearm.
4. Position VSS, with Identification level surveillance 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. Many of the current systems have doors which open and stay open providing access into Secure areas from public.
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.

4.6.4. Trash and Recycling Receptacles in Public Areas

1. Utilize only DHS approved blast resistant 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.
2. Trash receptacles with opaque walls that conceal items placed within them are not permitted.

3. Trash receptacles with heavy walls, such as aggregate cement/stone trash containers are not permitted.
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

4.6.5. Terminal Interior Landscaping in Public Areas

Interior landscaping which may include plantings, balconies, and pools of water, shall be designed following guidance provided in the Crime Prevention Through Environmental Design (CPTED) for Transit Facilities Recommended Practice published by the American Public Transportation Association (APTA SS-SIS-RP-007-10A) that provides guidance on construction designs that emphasize using the structures, spaces, lighting and people around an area to prevent crime and to increase loss prevention. The purpose of this APTA Transit Recommended Practice is to ensure that each transit system achieves an appropriate level of protection for people, operations and assets, and the public. CPTED involves the design use of five strategies (natural surveillance; natural access control; territorial reinforcement; activity support; and maintenance), all of which are described below:

1. Natural surveillance. This strategy involves reducing crime by decreasing target opportunities in a space/area by placing physical features, activities, and people to maximize visibility.
2. Natural access control. Channeling people into, alongside or out of spaces/areas and deterring entry elsewhere along the boundary are the concepts of this principle (through the judicial placement of entrances, exits, fencing, landscaping, and lighting); This concept denies access to crime targets and creates a perception of risk for adversaries.

3. Territoriality. Territoriality notifies users and non-users of the boundaries of a space/area or facility. It creates a psychological deterrent to crime by notifying users of the space/area/facility that they are being watched and that the community is the space/area/facility for purposeful activities.
4. Activity support. By encouraging authorized activities in public spaces, the community and transit system ridership understand its intended use. Criminal acts are discouraged, and an increase in safety and security of the transit system, its operations, facilities, ridership, and people are realized.
5. Maintenance. Care and upkeep demonstrate expression of ownership for the intended purpose of the area. A lack of care indicates loss of control of a space or area and can be a sign of tolerance for disorder. Establishing care and maintenance standards and continuing the service preserves the intended use of the space/area. CPTED maintenance and care standards also safeguard the best interests of the community and transit agency where they serve.

4.6.6. Terminal Expansion or Renovation

Airline terminals that are planned to undergo expansion or renovation will be required to comply with the current security design standards for new terminals under the ASGM. The scope of the expansion or renovation project and the security related design that is anticipated should be discussed with the Port Authority facility managers early in the process.

4.6.7. 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.

Any gunshot detection system installed by the tenant must be compatible with SDS software and report back to the Port Authority systems such as GDS, CACS and VSS.

The Port Authority uses Shooter Detection Systems (SDS) for gunshot detection in interior spaces. Any gunshot detection sensors must be compatible with SDS software and report back to the Port Authority systems and to integrated with VSS to identify the location of GDS event. The design and architecture of the gunshot detection system must be reviewed and approved by the Port Authority.

4.6.8. Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE), and Detection Sensors

The integration of CBRNE will provide PANYNJ with the capability to monitor the status of the CBRNE field devices. There are different types of modules that can be deployed throughout the

facility, such as chemical, biological, and radiological detectors. The requirements of CBRNE monitoring systems can vary from a single monitored detection point system to multiple detection points that are located across a security network. CBRNE sensors support first responders by providing information as to the release source and type of contaminant as well as provide plume modeling, which can help to predict the direction of travel of the contaminant. As the CBRNE program continues to evolve over time, PANYNJ and tenants will have on-going dialogues and identify the CBRNE systems that should be included for monitoring (if applicable and/or relevant).

Any CBRNE sensors that are installed in the terminal shall be provided with the capability to report back to existing Port Authority Police CBRNE software system, in addition to terminal software system. Technical configuration of sensors such as contaminant libraries (what the sensors are detecting), method of communication, and alarm escalation logic, shall be reviewed and approved by Port Authority in order to ensure consistency in detection and response protocols for PAPD across the airport.

The Port Authority currently uses SIGMA DTECT software for CBRNE monitoring and reporting. The Agency has existing chemical and radiological sensors deployed at certain terminal facilities.

The design and integration will require coordination with the Port Authority to designate or install such sensors to current and future software monitoring integrations.

4.6.9. Automated License Plate Recognition Systems (LPR)

A fully functional Automated License Plate Recognition System to be designed and constructed to be utilized by the Lae Enforcement. This system must adhere to specific performance standards:

1. LPR cameras must seamlessly integrate with the existing LPR system of the Port Authority Police Department, following Port Authority-approved protocols.
2. All necessary infrastructure enabling the new equipment to communicate with the existing system must be provided, with specifications varying by location. A hard-wired connection is mandatory.
3. Installation sites for LPR cameras must strategically cover chokepoints and key areas along roadways to capture both front and rear license plates, ensuring comprehensive coverage of vehicles entering airport premises.
4. Designate shoulders along roadways and terminal frontages to allow PAPD safe access for vehicle pull-overs and operations, minimizing risks from traffic or other hazards. Approval from the Port Authority is required for these locations.
5. Strictly prohibit the use of LPR cameras for revenue collection; they are intended for Law Enforcement purposes and traffic monitoring. Use cases of LPR data shall be reviewed with OCSO as well as Port Authority Operations and Traffic Engineering.
6. Ensure ease of accessibility for maintenance vehicles such as bucket trucks or person-lifts to the locations of LPR cameras.
7. Each LPR camera proposed should accommodate current and anticipated future traffic volumes within the roadway network.

8. Where feasible, supplement LPR cameras with VSS cameras to provide operators with visual validation of traffic conditions. Include necessary infrastructure for VSS.
9. Integrate the system with the Port Authority AOC/SOC and the PAPD desk.
10. Mandate the installation of LPRs at critical vehicular entry points across specified locations, including but not limited to; AOA Perimeter Guard Post Vehicle Gates, Terminal Loading Dock Salley Port to/from Public Roadways, Electrical Substation Vehicle Gates, Loading Docks at Cargo Facility Public Side Service Doors, and Vehicle Access Points to Construction Work Zones.

4.6.10. Public Safety Life Safety (PSLS) Radio systems

PSLS Radio systems shall be designed to provide radio frequency (RF) coverage to accommodate the needs of PAPD including mutual aid and other first responder organizations. PSLS Radio Distributed Antenna System (DAS) shall be independent and separated from the Cellular DAS system. PSLS Radio System shall meet all applicable codes and Port Authority design guidelines. Maintenance, supervisory or trouble alarms related to the associated radio equipment (PSLS and/or DAS) and UPS in the facility shall be sent to the AOC or location designated by the Port Authority. Standard Operating Procedures must be established to correct trouble alarms or any degradation in performance of the PSLS or DAS system that may be caused by RF interference or failed equipment.

The tenant is responsible for maintenance of the radio equipment and distributed antenna system within their facility including preventative maintenance tasks, future upgrades necessary to keep the system in a state of good repair. Coordinate with OCSO the system channels and radio frequencies in addition to required functionality of the radio system.

4.7. 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 shall 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, 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 VSS coverage and public-address system coverage, gunshot detection system and CBRNE sensor detection at the station entrance portals to the terminal in accordance with Sections 4.6.8, Video Surveillance Systems (VSS) Section 3.4.6, Video Management & Surveillance Systems (VMSS) Section 3.4.7, Public Address Systems Section 4.6.10 and Gunshot Detection Systems, and Section 4.6.7.

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, Accommodation of Space in Public Areas for Police Screening Operations Section 3.4.13, and Accommodation of New Security Technologies and Protocols Section 3.4.14 shall apply.
3. For the same reason as above, for security operations Operational Security at Terminal Frontage, Arrivals and Departures Halls Section 4.6 shall apply.

4.8. Loading Docks for Delivery to Vendors

1. The Port Authority requires 100% screening of all vehicles and cargo that is delivered to airline terminals at Port Authority airports by one of the alternative methods of delivery listed below.
2. 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 airport 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.
3. Deliveries shall be pre-scheduled and confirmed by the airline terminal operator.
4. 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 5., 6. and 7. below.
5. In no case shall loading docks be placed adjacent to critical infrastructure and facilities (see Section 4.9 for definition).
6. The Port Authority requires that all vehicles intended for deliveries to landside loading docks be pre-screened and cleared 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.
7. 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.
8. When pre-screening is not possible, the goods themselves shall be received in an area where they can be inspected and/or screened upon arrival.
9. for regulatory and inspection reasons, it is required that the screening facility have adequate VSS coverage, video storage, and be protected by electronic access control. The Port Authority shall have access to conduct security inspections.

10. 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.

4.9. Terminal Non-Public Areas

a. Service Corridors, Stairwells and Vertical Circulation: Following sections are similar to Part III – TSA Recommended Guidelines, Section D – Terminal, in reference but shall 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 (LEO) 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) When any elevator serves one or more Sterile or Secured 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 or Secured Areas floors. The elevator control panel will only allow the fire department to override this feature.

b. Airport and Tenant Administrative/Personnel Offices: Following sections are similar to Part III – TSA Recommended Guidelines, Section D – Terminal in reference[6] but shall be treated as mandatory under these Guidelines:

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.

c. **Law Enforcement & Public Safety Areas:** Following sections are similar to Part III – TSA Recommended Guidelines, Section D – Terminal in reference[6] but shall be treated as mandatory:
   1) Terminal space planning related to law enforcement shall be coordinated with PAPD through the ASM.
   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.

d. **Security Operations Center (SOC):** Following sections are similar to Part III – TSA Recommended Guidelines, Section D – Terminal in reference[6] but shall be treated as mandatory under these Guidelines:

   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.
   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.
   n. Weather monitoring/radar/alert systems.

4.10. Electrical Substations and Critical Infrastructure Facilities

The security design criteria and applicable threats that apply to the design of electrical substations at Port Authority facilities will commence once a Stage I level design has been developed for the specific electrical substation. 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 electrical substation facilities. Threat magnitudes will be provided by the Port Authority. Following are the steps in the security design process.

1. An independent security engineer will be assigned by the Authority to prepare a Design Basis Threat (DBT) Analysis Report. The DBT Analysis will determine the credible threats to be mitigated by various protective methods which may include the following:
   a. A crash-rated, anti-climb, perimeter security fence with crash-rated access-controlled entry/exit gate(s)
   b. The perimeter security fence shall create sufficient standoff distance so that a hand carried threat, if thrown, or a vehicle borne threat post collision, cannot fully breach the protective walls of the substation building enclosure.
   c. Physical ballistic screening to interrupt any visual sight lines of critical substation components from any exterior vantage points.

   d. Physical hardening of the buried electrical utility duct bank to resist damage from the DBT.
   e. Other required “hardening” includes protection of power transmission and communications systems, and protection from cyber-attack.
2. The Engineer of Record (EOR) for blast analysis and blast mitigations shall demonstrate sufficient previous experience in US-DHS force protection design for building projects of a similar nature. See Section 3.4.1 for additional information.
3. The designer shall complete the design by developing appropriate mitigations for the building at each stage of design with supporting engineering analysis including blast analysis. The costs of the required threat mitigations will be included in the total cost of the project at each level of design through final design.

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, but are not limited to:

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.

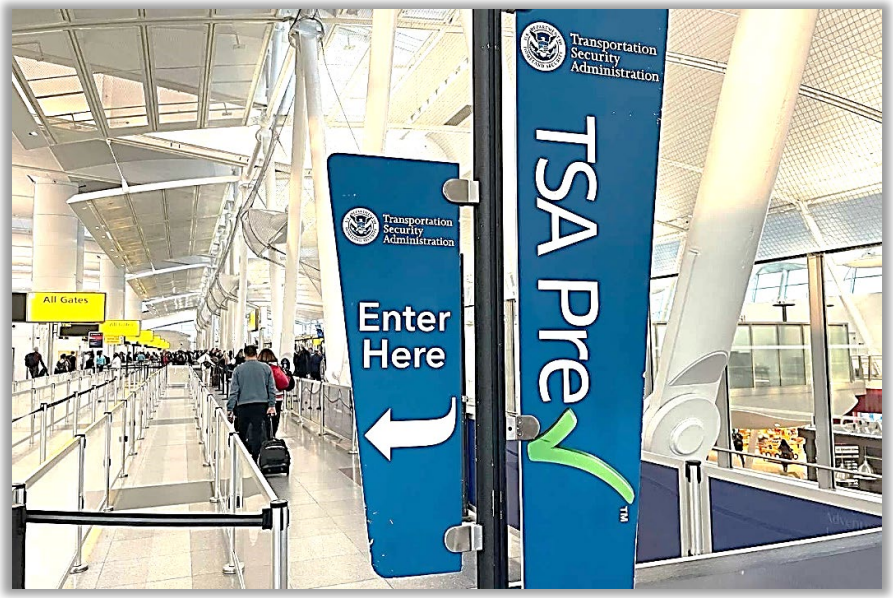

Figure 6 – TSA Security Checkpoint (EWR Terminal C)

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.

5.5. SSCP Power, Data and VSS

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 an uninterrupted power source and generator backup so that it can operate during an emergency power outage.

VSS requirements for SSCP are covered under Section 3.4.6. At each Port Authority airport, the SSCP VSS feeds shall be transmitted to specific TSA designated locations both locally and regionally and shared locally with Port Authority. As noted in Section 3.4.6, any VSS streams must be provided to the Port Authority upon request. Any VSS streams 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 (TSOs) 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 (SMEs) 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 (AOA)

6.1. AOA Perimeter Protection

6.1.1. Perimeter Intrusion Detection System (PIDS)

1. The Port Authority PIDS is a multi-sensor perimeter intrusion layered security system and is incorporated into the AOA perimeter boundary fence. It is designed to protect airport perimeters against unauthorized entry twenty-four hours a day, seven days a week, in all weather conditions. The following are the minimum requirements with preferred/recommended levels of coverage. The PIDS shall maintain a system operational availability (up-time) of 99.9%. It is the PANYNJ's requirement that all tenant lease holds will meet or exceed all PANYNJ's PIDS requirements as outlined within this document. Based on the PANYNJ's security assessment of a tenant's leasehold, PANYNJ may require a tenant to install its own PIDS system. A tenant is not required to install the PANYNJ PIDS.
2. The PANYNJ 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. Perimeter segments must be broken into zones that do not exceed 100 feet in length, however the preferred zone length specified by the Authority is 50 feet to properly identify intrusions points to assist in a rapid response. All zones shall have complete visual assessment capabilities that work in the given lighting conditions and redundant assessment coverage should be provided for all zones to allow for maintenance of an individual camera.
4. Each perimeter segment should be covered by at least one detection technology with a goal of dual/redundant detection coverage and the system shall be scalable/expandable to meet the future needs due to AOA changes and tenant expansion.
5. Sensor technologies include camera system equipment with video analytics and/or video motion detection capabilities, vibration sensors (above ground and/or buried), radars, lasers, thermal cameras, infrared cameras, day/night cameras, and microwave.
6. All video cameras shall meet the latest industry standards at the time of purchase and comply with classification level surveillance as a minimum in lighting requirements of low-light, infrared, and thermal, and have power requirements (POE), network connectivity, weather resistance, data compression and shall be ONVIF compliant (or latest compatibility standard).
7. The system must include a Video Management System (See Section 3.4.7 Video Management & Surveillance Systems (VMSS))
8. 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 SOC.

9. The tenant shall enable all PIDS VSS camera views to be electronically streamed (monitored and displayed) by the Port Authority upon request on a 24/7 basis by integrating the system feed to the Port Authority's PAPD Desk. Contact the Airport Security Manager for the specific technical requirement or operational procedures/ requirements.
10. All perimeter zones shall have complete visual assessment capabilities that work in the given lighting conditions (redundant assessment coverage should be provided for all zones to reduce the likelihood of down time in the event of equipment or camera failure).
11. 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 specific PIDS contractor for the requirements, standards, and product information.
12. Any design, installation, or modification to the existing PIDS shall comply fully with PIDS Standards.
13. 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.
14. PIDS shall provide a visual and audible alarm at the PIDS workstation(s), on a situational awareness map, to inform the system operator of the location of any intrusion(s).
15. Airport tenant inquiries about the PIDS that the Port Authority would recommend installing at Port Authority facilities shall be referred to National Safe Skies who maintains the "FAST" database of security equipment vendors many of which (not all) have been comprehensively tested by National Safe Skies in a real-world airport environment. https://fast.sskies.org/
16. Other requirements:
    a. Exterior components must operate between minus 10 and plus 130 degrees Fahrenheit.
    b. Interior components must operate between minus 10 and plus 120 degrees Fahrenheit.
    c. All components within a control room facility and related equipment rooms shall operate between plus 50- and 95-degrees Fahrenheit.
    d. Prior to formal acceptance/final invoicing, the tenant PIDS must be reviewed and approved by PANYNJ's Cybersecurity Program Group for compliance.

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.

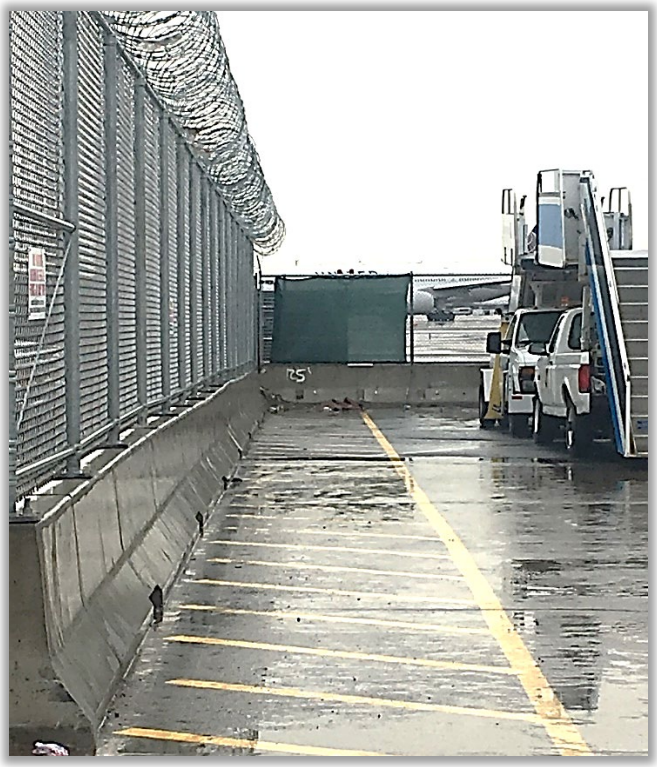

Figure 7 – Example of Port Authority AOA Security Fences

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

1. Chain link fence design and details as a minimum shall comply with High Security Galvanized Steel Chain Link Fence (Type 3) as shown in the current Port Authority of NY & NJ Standard Security Galvanized Steel Chain Link Fence standard drawings.
2. A continuous crash resistant concrete base embedded in the ground is required where any type of vehicle may have access to the terrain where the fence line is constructed.
3. 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).
4. Chain link fabric is 1” x 1" mesh with 0.148” OD wire, anti-climb with metal coated (galvanized) or polyvinyl chloride (PVC) coated.
5. Fence is topped with 6 lines of barbed wire, plus 30" diameter concertina single coil barbed tape.
6. Within the Central Terminal Area (CTA) the AOA perimeter fence shall be a crash rated ornamental metal fence meeting the same height requirements.
7. 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.

8. 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, VSS monitoring, and various fence system detection sensors.
9. 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 (or as agreed to by the ASM in writing) 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.
4. All clear zones shall be clearly marked with surface paint and maintained and shall denote the outer limits of the zone. Signage shall be provided “No Parking or Storage within the described clear zone.

Figure 8 – Example of AOA Clear Zone Violation by Stored Objects

Figure 9 – 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 valid SIDA identification credentials for the driver and routine checks of all individuals in the vehicle, and inspection of vehicles and their contents for any contraband or illegal items.
3. The AOA vehicle inspection shall also include a search of the underside of every vehicle using a high-resolution vehicle undercarriage scanner in the roadway pavement which will also save a digital image. Existing inspection stations without an undercarriage scanner shall use an under-vehicle mirror to search the underside of every vehicle.
4. Dependable and instant voice and video communications from the guard post to the Security Operations Center (SOC), or other appropriate central location, shall be installed, maintained, and frequently tested.
5. If a tenant project scope of work includes an AOA perimeter guard post, tenant shall contact the ASM for the latest design and construction requirements.
6. Any vehicles intended to work routinely on airside must have Port Authority license plates.

Figure 10 – Crash Rated Vehicle Arrestor Bed

6.1.3.2. Vehicle Barrier Gates

1. All new guard posts at vehicle portals must be configured with crash rated vehicle barrier gates such as the “Grab Barrier” or other certified moveable arrestor bed type that meets Port Authority requirements and must be manually controlled from inside the guard booth with automated safeguards.
2. The moveable or arrestor barrier model shall have been tested by the manufacturer to meet or exceed the ASTM F2656-07 criteria for the maximum vehicle weight and vehicle speed.
3. Any existing guard posts with barrier gate control arms shall be of a “break away” design.
4. All guard posts shall have vehicle detection loops in the pavement to detect or prevent vehicle spacing that is too close (piggy backing) which automatically prevents the vehicle barrier gate from being lowered.
5. 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.
6. See Figure 11 and Figure 12 for the types of moveable crash rated barriers that are required by the Port Authority.
7. It is required that guard posts be configured as vehicle “Sally Ports” for positive control.

Figure 11 – Permanently Installed Vehicle Arrestor Bed Gate in Raised Position

Figure 12 – Anti-Ram High Security Fence

6.1.3.3. AOA Guard Post Configuration and Booths

1. A climate-controlled and bullet resistant 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. Pipe guard bollards shall also be installed to protect any equipment that would otherwise be exposed to vehicle collision.
3. The guard booth shall:
    a. 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, bulletproof glass, a transaction drawer that permits the passing of vehicle driver and occupant credentials only.
    b. be designed so it can comfortably accommodate a second guard.
    c. 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.
    d. include 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.
    e. include video streams from VSS camera coverage providing face view of driver in vehicle, front and rear view of stopped vehicle, and license plate reader camera data shall be tied into the Port Authority's video management system and shall be shared with the Port Authority Office of Security Technology and the Port Authority Office for Law Enforcement (Port Authority Police).
    f. include a duress alarm system tied to the PAPD and AOC shall be provided.
    g. provide ample vehicle queuing distance and vehicle inspection portals to avoid long traffic backups and delays.
    h. provide a pull-off space for waiting vehicles or for conducting a secondary inspection.
    i. provide turn-around space so that a vehicle denied entry does not have to enter the SIDA to turn around.
    j. provide traffic signals integrated with the vehicle barrier gate.
4. Other guard booth features shall include crash barrier control panel, LCD monitor, Biometric reader (fingerprint or other), non-corrosive metal booth enclosure, pedestrian intrusion detection annunciator, 2 card readers, outside fresh air intake protection.
5. All guard post barrier equipment shall be placed on Landside.

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

1. No person shall be permitted within the Sterile or Secured Area without an Airport Security ID 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 Area 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 https://www.panynj.gov/airports/en/aviation-security/ecscort-rules-procedures.html. Persons that are escorted or badged and entering into Sterile and Secured Areas may be required to submit to a screening program. Staff under escort may also be required to have a background check through the "Info-Corp" system, 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 the Secure Worker Access Consortium (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 one hundred percent (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 and areas inside the building where cargo is accepted must be designated as SIDA or Secured Area 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 uninterrupted power source (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, automobile 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 portals entering or exiting the Secured Area must be monitored by dedicated VSS coverage.
7. Where ventilation is required, rollup doors with small perforations that prevent passing of contraband items are permitted (see Figure 13).
8. All personnel must access the Secure/SIDA area through a door/portal that allows the passage of only one person at a time, e.g. a High Entry-Exit Turnstile (HEET) turnstile matching the fence height or sally port (see Figure 14), and such doors or portals must be controlled by a computerized access control system that is compliant with Port Authority 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.
9. 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. In addition, all portals entering or exiting the Secured Area must receive dedicated VSS coverage.
10. Emergency exits in the Public Area shall only exit to landside, not AOA/SIDA.
11. 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.

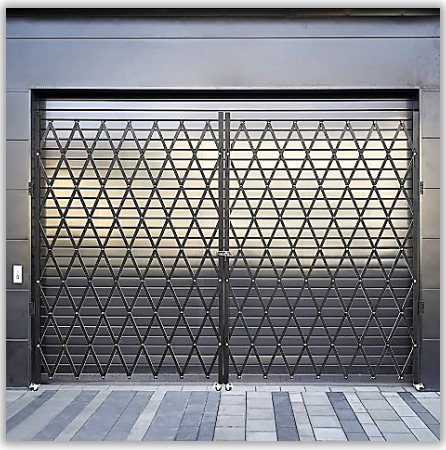

Figure 13 - Scissor Gates and Rollup Door.

Figure 14 – Example of a HEET Turnstile Gate

12. Cargo doors with scissor gates are not permitted unless used in combination with an additional barrier such as rollup doors (see Figure 13). 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.
13. AOA Perimeter security fence meeting the requirements of Section 6.1.1 and Section 6.1.2 must be installed as shown in Figure 7 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.
14. 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.
15. Any Public Area of a cargo facility must be separated from the Secured Area or SIDA by a metal fence or wall.
16. Cargo facilities are required to meet the requirements for Access Control Systems (ACS) in Section 3.4.5, Video Surveillance Systems (VSS) in Section 3.4.6, and Video Management & Surveillance Systems (VMSS) in Section 3.4.7.
17. VMSS system is 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
18. VSS 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.
19. Any interior offices, hallways, doors, or other space accessible to the public may not provide uncontrolled access to the Secured 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 Program (TSP) 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.
3. All cargo facility personnel shall have SIDA badge displayed at all times and if applicable, a US Customs seal for CPB 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 comprehensive ATSP 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 as defined in their ATSP or EAA, to monitor all cargo handling and screening activities during both peak, normal and off-peak hours of operation.

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 3.4.5, Video Surveillance Systems (VSS) in Section 3.4.6, and Video Management & Surveillance Systems (VMSS) in Section 3.4.7.
3. Access control, VSS 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 and that the products produced are intended for direct induction for delivery to a departing aircraft, 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 any in-flight catering facility layout and operation include:

1. Compliance with 49 CFR 1544 and 1546 and all applicable security directives and amendments.
2. An on-airport in-flight catering facility shall be required to provide a comprehensive security plan for Port Authority approval.
3. Access control, VSS and VMS systems are required to prevent, detect and record unauthorized access to the facility, or tampering with catered deliveries. VSS coverage must tie into TSA local headquarters and the PANYNJ locations designated by the ASM 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 SIDA badges 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 any 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 and shall be bullet resistance. 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 VSS and VMS systems including roof, stair doors and 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 3.4.5, Video Surveillance Systems (VSS) in Section 3.4.6, and Video Management & Surveillance Systems (VMSS) in Section 3.4.7.
5. All landside deliveries to the hotel through the terminal Public Area shall be scheduled, delivered, inspected and screened at the terminal loading dock or an approved off-site location. 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 also cover all security measures , including but not limited to combat insider threat.

9. GENERAL AVIATION

9.1. Operational Practices

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

1. 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. Must have a procedure requiring from a pilot to establish a connection (identify) between names reported on a Pax manifest and persons he/she is escorting onto the ramp/aircraft.

9.2. Security Control of Personnel

Tenant 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. Ensure that 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 PPAPD.
8. Flight training schools or student pilots are not permitted at JFK, LGA, or EWR.
9. Where flight training is permitted, comply with 49 U.S.C. § 44939 and 49 CFR 1552.

9.3. Security Control of Aircraft

Tenant 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. If there is adequate space, mark/assign parking spots or transient parking areas to easily identify transient aircraft on the apron.
2. Transient Pilots must be in company uniform display a company ID and/or Pilot Certificate and be vetted by the FBO or tenant authentication prior to accessing the ramp area and must remain within 25-feet of their aircraft or be under escort by a badged employee.
3. At least one of the following aircraft security measures, or combination thereof, must be used to secure any unattended aircraft: Door locks, throttle locks, propeller locks or lockable booths, aircraft tied to the ground with chain and padlock (applicable to small GA aircraft only) must be used on aircraft where applicable.
4. Ensure that aircraft door locks are consistently used to prevent unauthorized access or tampering with the aircraft.
5. Use keyed ignitions for aircraft where appropriate.
6. Use an auxiliary lock to further protect aircraft from unauthorized use and strictly control access to all aircraft keys.
7. If none of the above requirements in subparagraphs (3) through (6) are feasible or acceptable to the aircraft operator, the operator must hire a guard company (with a Port Authority Permit) to guard the aircraft while parked at a Port Authority airport.
8. When hangars are available at the airport facility, store idle aircraft in hangars with locked doors.
9. 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.
10. Ensure that aircraft ignition keys are not stored inside the aircraft.
11. Practice strict transfer of control for aircraft and keys before and after maintenance procedures. Never leave an unattended aircraft open with keys before or after repairs are completed.

9.4. Security Control of Bags and Baggage

Tenant 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. FBO may have own access gate to the AOA provided, physical barriers are in place (i.e. bollards or jersey barriers) and permission has been granted from the ASM.

3. 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

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

1. 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.
2. 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.
3. In addition to hangar door locks, provide an electric bypass switch and/or alarm and intrusion detection system for hangars.
4. Provide adequate levels of lighting without blind spots around hangars and on all airside/landside areas for proper visibility of ramps and parking lots.
5. The Airport Security Manager shall have access to inspect hangars at any time with short notice.
6. GA tenants shall have a strict key or access card control program for hangars which will be periodically audited by the Airport Security Manager.
7. For AOA security fencing and clear zone requirements see Section 6.1.2 Perimeter Fencing.
8. Any (Non-AOA) perimeter security fencing design shall follow the Port Authority of NY & NJ Standard Security Galvanized Steel Chain Link Fence Standard Drawings, and comply with the following:
    a. Keep perimeter fencing clear of vegetation growth with applicable “Clear Zone” rule observed.
    b. Fencing shall have no gaps underneath greater than 2”.
    c. Poles of fencing must be buried into the ground/pavement.
    d. Signage that details “no trespassing” must be attached to fence.
    e. Minimize access points to the airfield and ensure they are regularly monitored.
9. Other types of security fences are permissible if previously approved by the Airport Security Manager in writing.
10. Airport operators and tenants, shall make an effort to provide outdoor security lighting and VSS cameras with an uninterrupted power source to monitor and record activities for the following areas:
    a. 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. Airport access control points.
    a. 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 violation(s) by a contractor 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 Project Security Plan (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, 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 Contractor 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).
    d. Security measures include Installation of Construction cameras at the entrance/exit of construction gates with thirty (30) day storage capacity for situational awareness.

4. The PSP shall also consist of all labor and materials necessary to establish one or more secure perimeters around the construction site. It shall 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 previously given to any individual 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 Transportation Security Administration ("TSA") or the Port Authority in response to security compliance with the PSP shall be addressed immediately by the contractor at contractor's 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/Resident Engineer will serve as the liaison between the ASM and the Contractor. However, direct coordination in emergency situations should be expected.

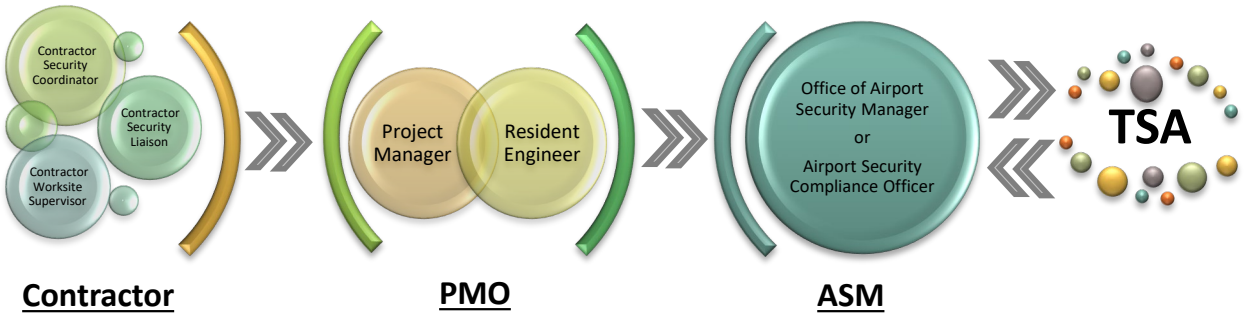

Figure 15 – Restricted Area Responsibilities

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 precede 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 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. Tools must never be left unattended.

3. Contractor's security representative shall conduct daily sweeps of construction area for tool and worker compliance.
4. Workers' access is restricted to areas and times specified in the Project Security Plan.
5. 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.
6. When not in use tools shall be stored away in a locked, tamper proof and hardened storage space that is anchored down to prevent removal from the site. Distribution of keys to the locked storage shall be centrally controlled and the lock (tumbler) shall be changed periodically with new keys issued.

The form 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 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.

Key areas contained in the document are summarized as follows, with details contained in in the reference document itself.

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

No person shall be permitted on or about the construction site in the Secured, Sterile or SIDA Area without an Airport Security ID 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 IDs or an official escort badge in a clearly visible position (above the waist and below the neck) whenever they are working at the construction site.

Contract personnel who cannot get an Airport Security ID since they temporarily require access to the Secured, Sterile or SIDA Areas may be subject to a background check through the Secure Worker Access Consortium (SWAC) for all personnel whose expected duration on-site will be thirty (30) days or greater. 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 https://www.panynj.gov/airports/en/aviation-security/new-applicant-process.html

The issued Airport Security IDs 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 thirty (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. In addition, the contractor shall provide site-specific post orders for each post to all guard companies being employed at the site. The security contractor must acknowledge receipt such orders and ensure all staff are aware. They shall also provide have proof of acknowledgement to the Port Authority.

10.2.4. Radios/Two Way Communication

Contractor shall 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, distributed antenna systems where applicable, and other associated equipment, with no less than two (2) distinct frequencies, unless otherwise directed by the PANYNJ. The equipment shall have an eight (8) hour Uninterrupted Power Source (UPS). It shall have a separate Distributed Antenna System (Public DAS), not on shared DAS. This equipment must be maintained in good repair and operating condition as long as it is in use. Contractor shall supply additional handsets for the Port Authority personnel's use to maintain contact with project security personnel as 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. Authority auditors and inspectors will randomly inspect and monitor the construction site and other airport areas. Violations will result in confiscation of Airport Security ID and loss of privilege to work on the contract and in any restricted 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 and 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

Security Guard Posting Requirements

Contractors shall be required to utilize Port Authority security contractor staff for access to airside construction sites. The cost for these services shall be directly reimbursable to the vendor by the construction contractor.

Haul Route Security Guards

A "Haul Route" shall be a pre-approved path on the Secured, or SIDA Area, clearly delineated as the Project Security 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 feet 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 nine-foot-high chain link fence, including barbed wire, as detailed on contract drawings.

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.

10.2.8. Surveillance Video Design Methodology

In 2019 the federal government restricted use of technology that pose high cyber security risk, and those originating from Chinese manufacturers. The current list of banned/restricted cameras can be found on the Department of Homeland Security website. Camera makes and model information proposed for installation at any PA facility will require approval from the OCSO.

Video surveillance cameras, in addition to meeting the minimum requirements listed by type below, should be capable of at least 1080p HD (1920x1080 at 30 frames per second), IP-addressable, and PoE unless specific conditions require otherwise.

a. Classification Surveillance: Classification video shall enable the operator to detect that an object or person is in the video scene. Images of the intended target shall provide information about where the target goes and comes from, the number of objects in a scene, and other general information.
    i. Minimum pixels on target: 15 pixels per foot
    ii. Live video monitoring frame rate: 30 frames per second
    iii. Minimum recording frame rate: 10 images per second

b. Recognition Surveillance: Recognition video shall enable the operator to recognize or establish the type of object or defining features of an individual. Images of the intended target will provide information about the types of clothing, skin tone, height, weight, or make/model of an object.
    i. Minimum pixels on target: 30 pixels per foot
    ii. Live video monitoring frame rate: 30 images per second
    iii. Minimum recording frame rate: 15 images per second

c. Identification Surveillance: Identification video shall enable the operator to identify or establish distinguishing and unique features of an object or the defining features of an

individual. Images of the intended target will provide information about facial features or make/model of an object.

i. Minimum pixels on target: 60 pixels per foot
ii. Live video monitoring frame rate: 30 images per second
iii. Minimum recording frame rate: 15 images per second

d. Special Purpose Surveillance: Special purpose surveillance provides specific, object-based video surveillance information as needed based on the facility's requirements. Special purpose cameras include, but are not limited to, dedicated license plate recognition, automatic facial recognition systems, thermal-perimeter protections systems, and others. The minimum requirements for these systems shall match the needs of the system being installed.

i. Minimum pixels on target: as per manufacturer specifications and technological limitations
ii. Live video frame rate: as per manufacturer specifications and technological limitations
iii. Recorded video frame rate: as per manufacturer specifications and technological limitations.

11. ACRONYMS AND ABBREVIATIONS

AAR	After Action Reports
ACS	Access Control Systems
ADA	Americans with Disabilities Act
AIT	Advanced Imaging Technology
ALPR	Automated License Plate Recognition
AOA	Air Operations Area
AOC	Airport Operations Center
API's	Application Programming Interfaces
ASC	Airport Security Coordinator
ASM	Airport Security Manager
ASP	Airport Security Program
ATSP	Airport Tenant Security Program
AVS	Alternate Viewing Station
BLS	Bottle Liquid Scanner
BOH	Back of House
CBA	Cost Benefit Analysis
CBP	Customs and Border Patrol
CBRNE	Chemical, Biological, Radiological, Nuclear & Explosive
CCSP	Certified Cargo Screening Program
DAS	Distributed Antenna System
CDG	Checkpoint Design Guide
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
CMS	Changeable Message Signs
ConOps	Concept of Operations
CP	Command Post
CPI	Confidential Privileged Information
CPTED	Crime Prevention through Environmental Design
CSO	Chief Security Officer
DBT	Design-Basis Threat
EAA	Exclusive Area Agreement
ECMNS	Emergency Communications/Mass Notification Systems
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EOR	Engineer-of-Record
ETD	Explosives Trace Detection
EWR	Newark Liberty International Airport
FAA	Federal Aviation Administration
FBO	Fixed Base Operators

FSD	Federal Security Director
FIS	Federal Inspection Services
GDS	Gunshot Detection System
GSR	Ground Surveillance Radar
HVAC	Heating, Ventilation and Air Conditioning
IED	Improvised Explosive Device
ISA	Initial Security Assessment
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Transportation Systems
JFK	John F. Kennedy International Airport
LEO	Law Enforcement Officer
LGA	LaGuardia Airport
LPR	License Plate Reader
OCSO	Office of the Chief Security Officer
PA	Public Address
PANYNJ	Port Authority of NY & NJ
PAPD	Port Authority Police Department
PARAS	Program for Applied Research in Airport Security
PDN	Protective Design Narrative
PIDS	Perimeter Intrusion Detection Systems
PIRF	Port Authority Project Initiation Report Form
PMO	Project Management Office
PoE	Power over Ethernet
PSIM	Physical Security Information Management
PSLS	Public Safety Life Safety
PSP	Project Security Plan
PTZ	Pan-Tilt-Zoom
PTZR	Pan-Tilt-Zoom-Rotate
SEOC	Security & Emergency Operations Center
SDK	Software Development Kit
SDS	Shooter Detection System (Brand of GDS)
SIDA	Security Identification Display Areas
SIM	Security Information Manager
SME	Subject Matter Experts
SOC	Security Operations Center
SOP	Standard Operating Procedure
SPC	Security Performance Criteria
SPM	Security Planning Manual
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
TDC	Travel Document Checker
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSO	Transportation Security Officer
UPS	Uninterrupted Power Source
VMD	Video Motion Detection
VMDT	Video Motion Detection Tracking
VMS	Variable Message Sign
VMS	Video Management System
VSS	Video Surveillance System
WTMD	Walk Through Metal Detector

12. REFERENCES

1. Security Planning Guideline: Guideline for Security Classification, Planning and Design at Project Inception for Port Authority and Tenant Projects https://paenet.panynj.gov/ocso/pdf/guideline-statement-security-planning-design.pdf
2. Port Authority Airport Planning Standards Version 3, September 2018 https://www.panynj.gov/content/dam/port-authority/pdfs/-available-engineering-documents/panynj-terminal-planning-guidelines.pdf
3. The Port Authority of New York and New Jersey Information Security Handbook, Revised April 2018 https://www.panynj.gov/content/dam/port-authority/pdfs/vendor-resources/Corporate-Information-Security-Handbook.pdf
4. Port Authority of New York & New Jersey Airport Contractor Security, Tool Management and Escort Responsibilities (Revised 6-19-2018) https://www.panynj.gov/airports/en/aviation-security/ecscort-rules-procedures.html
5. The Port Authority Of New York And New Jersey Airport Rules & Regulations, July 2022 https://www.panynj.gov/content/dam/airports/pdfs/Airport_Rules_Regs_7_27_22.pdf
6. Port Authority Wayfinding Manual, July 2020 https://wayfinding.panynj.gov/
7. Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attack (Published by US CDC, April 2003) https://www.cdc.gov/niosh/docs/2003-136/pdfs/2003-136.pdf
8. Port Authority of NY & NJ Standard Security Galvanized Steel Chain Link Fence Standard Drawings. https://enet.panynj.gov/ocso/pdf/standard-details-for-security-chain-link-fence.pdf
9. Recommended Security Guidelines for Airport Planning, Design, and Construction 157, PARAS 0004, February 2021. https://www.sskies.org/images/uploads/subpage/PARAS_0028.Recommended_Security_Guidelines_.FinalReport_.pdf
10. TSA Checkpoint Design Guide (CDG), June 2016 https://files.constantcontact.com/8c363cd8001/f070043f-495f-42bf-99b4-d1688c57e199.pdf
11. TSA issues new cybersecurity requirements for airport and aircraft operators, National Press Release Tuesday, March 7, 2023. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft
12. TSA Recommended Security Guidelines for Airport Planning, Design & Construction, June 2006 https://crp.trb.org/acrpwebresource2/tsa-recommended-security-guidelines-for-airport-planning-design-and-construction/