PORT AUTHORITY NY NJ

AIR LAND RAIL SEA

Seaport Facility Security Guidelines

March 2025

Revision History

Revision No.	Description	Date
0	INITIAL PUBLICATION	March 2022
1	Revision 1	March 2025
2		
3		
4		
5		
6		
7		

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

Table of Contents

1. INTRODUCTION

This document is a guide to security standards that shall be followed by all tenants at Port Authority of New York and New Jersey (Port Authority) port facilities, regardless of status as a federally regulated facility subject to the requirements of the Maritime Transportation Security Act of 2002 (MTSA). Note that compliance with these security guidelines carries with it no guarantee of protection against acts of terrorism, other crimes, or of their consequences. While following these guidelines will help reduce risk, risk will not be eliminated. All tenants, and their service providers, employees, and visitors at the port facilities must take their own reasonable standards of care and responsibility associated with the use and application of information provided in this guideline.

There is no "one size fits all" security solution based on the location, type and size of a tenant's operation. As such, working with the Office of the Chief Security Officer (OCSO), Port Security Manager (PSM), the tenant will identify the appropriate level of security technology, infrastructure and procedures required.

1.1. Purpose

This document (hereinafter referred to as "Guidelines") serves as an instruction for the industry best practices that have been adopted and security guidelines that have been established by the Port Authority for the planning, design, construction, and maintenance of tenant spaces at its port facilities.

The Guidelines are intended to inform tenants and their security managers and contractors of considerations to be addressed in accordance with Port Authority security policies and the general threat environment. The Guidelines supplement standard building code requirements for all buildings and installations on Port Authority property. The Guidelines will be incorporated into new Port Authority lease agreements as well as renewals. A tenant may construct or alter its premises with measures that are in addition to the Guidelines, however, it must adhere to its minimum requirements. The Port Authority reserves the right to inspect a tenant's leasehold prior to, during and after construction or an alteration to ensure compliance with the Guidelines.

Tenants and planning developers shall refer to the Guidelines for fundamental requirements regarding security infrastructure, technologies, and protocols to be applied at Port Authority facilities. The intent is to maintain a culture and environment where security is always a central consideration in planning, design, construction, and operations.

The standards described in the Guidelines assume that the tenant's planning, design, construction, and operation will also be in full compliance with any applicable local, state, and federal regulations and guidance. The Guidelines may be updated from time to time in response to emerging threats and new technology. These Guidelines do not take precedence over security regulations or criteria required by the U.S. Coast Guard for port facilities subject to the requirements of the Maritime Transportation Security Act (MTSA) or U.S. Customs and Border Protection requirements, including the Minimum-Security Criteria for participants in the Customs-Trade Partnership Against Terrorism (CTPAT) program. In the event of any conflict between these Guidelines and the regulatory requirements, the Federal requirements will prevail.

1.2. Applicability

Requirements contained in these Guidelines shall apply in total to new construction. For alteration, renovation, and/or modification to existing premises, the applicability of these Guidelines shall be proportionate and commensurate with the nature of the alteration, renovation, and/or modification, as determined by the Port Authority. Such will also be the case for new leases and/or lease renewals of existing premises. All Tenant Alteration Applications (TAA) will be reviewed by the PSM. The PSM will establish applicable requirements for the TAAs on a case-by-case review and will ensure that all minimal security designs, technologies, and protocols are met by each tenant as needed. This approach applies regardless of whether the subject facility is subject to federal regulations or not. For the key elements of these Guidelines that tenants should consider when submitting TAAs, please see Appendix A for a useful overview of key requirements.

1.3. Threats to Safety and Security

The basic threats from terrorism can take the form of a physical attack using conventional weapons, vehicles, explosives, flammables, chemical, biological and radiological agents or the use of cyber methods to adversely impact public safety and critical infrastructure. Threats from natural hazards, such as wind and flood, also need to be considered in planning and operating all safety and security measures. Finally, general crime to include assault, larceny etc. will always pose a threat to safety and 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 by complying with these Guidelines.

1.4. Office of the Chief Security Officer, Port Security Manager (PSM)

The PSM is the primary contact at each Port Authority facility for compliance with security standards and policies. The PSM prepares and maintains the security program, approves tenant security programs and provides feedback on construction-related security plans. The PSM is charged with mitigating security risk to the facility, and its employees and patrons. The PSM oversees a variety of security equipment for access control, intrusion detection, surveillance, and physical protection. The PSM works in close collaboration with the Facility General Manager (GM) and staff, Facility Security Officers of United States Coast Guard (USCG)-regulated facilities, the Port Authority Police Department (PAPD), and local and federal law enforcement and emergency response agencies. The PSM or his/her designee will be responsible for conducting a site survey of all leaseholds prior to the start of negotiations for all new or renewed leases. These surveys are designed to determine any security measures which must be addressed prior to the execution of a new lease, or which must be in place throughout the tenancy. The PSM will also be involved in the TAA process from design through construction and will determine individual applicability of requirements listed within this document.

1.5. Planning and Design Review Process

The requirements for the review of proposed plans and design documents are described in the *Port Authority of New York and New Jersey Security Planning Guideline: Guideline for Security Classification, Planning and Design at Project Inception for Port Authority and Tenant Projects, September 2021.*

The process consists of the following steps:

- Determine the level of security measures required through the following:
    - Ensuring a security requirements overview is included in lease negotiations;
    - PSM site surveys in advance of new leases or lease renewals;
    - PSM identification of security-specific issues applicable to build out and use;
    - Meetings with the PSM to determine the Security Classification (Level 0,1, or 2) as per the *Guideline for Security Classification, Planning and Design at Project Inception for Port Authority and Tenant Projects.*
- Perform reviews of drawings, specifications, and security plans and ensure Federal Code and Regulation compliance, if applicable; and
- Work towards Approval or Conditional Approval by the second submittal of documentation.

2. GENERAL SECURITY REQUIREMENTS

The varied nature of functional activities in Port Authority facilities calls for a wide range of security, safety, and operational standards. Many of these standards are closely linked to the locations of restricted areas and secure areas within, and near, the facility.

The Guidelines are a quick reference guide to explain the security policies & procedures and describe the tenant's role and responsibilities. It is expected that the tenant will abide by the policies and procedures herein. Failure to do so may result in the tenant being found in violation of their lease and could delay or prevent the issuance of a Construction Permit or Permit to Occupy for TAA related work. Further, port tenants are expected to participate in the Port Authority's Tenant Security Work Group, and, at the direction of the Port Authority, may be expected to participate in the Port of New York and New Jersey's Security Information Exchange.

2.1. Introduction of Security at Planning/Design Inception

Physical and operational security requirements must be introduced into the facility 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 space, or leasing and operation of an existing premises that is being re-purposed may have similar requirements. For the latter category of projects, it is necessary to check with the PSM.

In the project's preliminary planning/conceptual design phase, the tenant's Design Team, Architect or Engineer of Record, shall include an experienced anti-terrorism / security professional for the specific facility. The aforementioned security professional shall demonstrate previous experience in completing protective design for projects of a similar scope and nature. Specific requirements for the anti-terrorism/security professional will be provided by the Port Authority's Security Operations and Planning Department and will reflect specific needs of the project and licensing requirements that are based on the location of the work.

Any threat related information that is generated in the planning, design and construction process shall be classified as Confidential Privileged Information (CPI). All individuals on the developer's planning and design team who will be involved in 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 (Handbook).

The developer shall be required to designate a Security Information Manager (SIM) to ensure that the 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 for port facilities and operations 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 facility 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 or Engineer of Record (EOR), 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. The PDN shall be transmitted as part of the "Phase I: Initial Design" submittal. The identified mitigations shall then be further developed in each later phase of the design all the way through to the construction phase and shall be subject to review by the Port Authority as a basis for the 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 using physical barriers or electronically based access control, (b) defining the physical level of performance of the facility structural building elements and finishes that are required to limit damage to property and occupants from threats, (c) or otherwise employ security technology and personnel to detect, deter and defend the facility from threats. PDN mitigation strategies can be documented through Concept of Operations where applicable. 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 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 facilities. PDN design mitigations strategies (design options) shall be followed throughout the design and construction of the project. This documentation must be submitted by the design builder/EOR as part of the substantial completion of the project, in order to support the Department of Homeland Security (DHS) Safety Act Applications by OCSO.

The Port Authority document "Security Planning Guideline: Guideline for Security Classification, Planning and Design at Project Inception for Port Authority and Tenant Projects" provides detailed explanations for these processes.

2.2. Cybersecurity

The tenant shall also have a Cybersecurity policy and plan that covers all tenant terminal computing resources and is complied with by all employees and contractors 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 Information Technology (IT) and Operational Technology (OT) networks, systems and applications operated on site by the tenant. Where relevant, the Cybersecurity Policy shall also set forth requirements for the tenant to access Port Authority networks as an external IT partner. 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.

For those tenant facilities subject to the Maritime Transportation Security Act of 2004 (MTSA), they must comply with the USCG requirements. All tenants must assess the effectiveness of these measures, which include the following actions:

• Develop network segmentation policies and controls to ensure that OT systems can continue to safely operate if an IT 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.

2.2.1. 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. Security System Logic and Design

To be effective, security systems need to be well planned and integrated in a manner that results in an error-free logic to ensure that they achieve their security objective. The following types of security related systems are a general approach to security system logic and design.

- Access Control Systems
- CCTV (Closed Circuit Video Cameras)
- Video Management & Surveillance Systems (VMSS)
- Public Address Systems
- Bollards
- Gates and Fences
- Engineering and Architectural Design
- New Security Technologies

During the planning and design phases of a project, the tenant will plan for security mitigations pursuant to the PDN and applicable regulatory requirements. In planning technology-based security solutions, planners need to also provide for expansion and evolution of systems and facilities. Allowing capacity for advanced design technologies alleviates much of the burden for additional costs in retrofitting infrastructure in the future. This “forward thinking baked in” approach to planning and project design also minimizes downtime, loss of space and services. Security project planning shall also incorporate back-up redundancy features, such as alternate power sources, to ensure that critical systems remain resilient during emergency events.

2.4. Crime Prevention through Environment Design (CPTED)

Crime Prevention through Environment Design (CPTED) is based on the idea that the effective design and proper use of the built environment may lead to a reduction in the incidence of crime and improve the safety and use of the premises. The goal of CPTED is to reduce the number of opportunities for crime to occur. This reduction may be achieved by employing physical design features that discourage crime, while at the same time encouraging legitimate use of the environment.

2.4.1. CPTED Guideline

CPTED was originally based on four main principles: Natural Surveillance, Territorial Reinforcement, Natural Access Control, and Image & Milieu. While subsequent versions of CPTED have modified these principles for specific uses, the principles listed below remain valid for seaport environments. All tenants are requested to support these concepts by:

- Incorporate natural surveillance design concepts into public space floor layout that complements easy natural public observation of the area, individuals, and their activities. Maximize the visibility of people, especially at building entrances. Also, ensure that there are adequate protective lighting schemes and keep interior landscaping to a minimum to maximize the ability to see and be seen.
- Do not place anything that could block or hinder security elements such as camera surveillance or impair physical security.
- Incorporate physical designs that reinforce territory by creating or extending a sphere of influence. This principle promotes psychological features that define ownership and distinguish private space from public space. A sense of territorial control will deter offenders and discourage unsafe activities.
- Employ design concepts that support natural access control. Limit access to critical areas and create a perception of risk to potential adversaries. Incorporate design or place signage that clearly indicate public routes and discourages access to private and restricted areas. Use these concepts in both exterior and interior applications.
- Ensure that site and facility maintenance areas indicate that the space is being used and regularly attended to. Image and milieu (maintenance) activities are often related to management and operations rather than the design of the facility but can illustrate to the public that these areas are not being neglected.

2.5. Access Control Systems (ACS)

Tenants with access to areas that are designated as “Restricted” under MTSA regulations shall, at a minimum, electronically monitor, record and control portals, doors, and access points for authorized personnel passing between the restricted and non-restricted areas. Restricted areas include but are not limited to:

1. Shore areas immediately adjacent to each vessel moored at the facility;
2. Areas containing sensitive security information, including cargo documentation;
3. Server rooms and technology rooms or cabinets;
4. Areas containing security and surveillance equipment and systems and their controls, and lighting system controls;
5. Areas of the facility containing critical infrastructure, including:
    - Water supplies;
    - Telecommunications;
    - Electrical system;
    - Access points for ventilation and air-conditioning systems; and
    - Access points to lift stations.
6. Manufacturing or processing areas and control rooms;

7. Areas designated for loading, unloading or storage of cargo and stores; and
8. Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

This is not a comprehensive list and may be updated by the PSM, PAPD or senior Port Authority management.

All portals, doors and access points which lead to restricted areas shall be electronically monitored and controlled and must be equipped with an appropriate level of door control and locking equipment. If the door also acts as an emergency exit, it shall be equipped with alarmed panic hardware operable from the inside only and otherwise kept secured at all times.

The following system criteria are required for an electronic ACS:

1. A written Standard Operating Plan;
2. Electronic card access readers to unlock door;
3. Monitored and audible alarm sounds when door is unlocked or opened without access card;
4. CCTV camera view of individual accessing the door with video resolution capable of facial recognition and automatically stored in video management system (VMS);
5. All elements of the ACS system shall have an Uninterrupted Power Supply (UPS) and battery backup that can sustain operations for a minimum of twelve (12) hours. An audible alarm must be operational when the UPS is activated and in use;
6. Generate traffic reports;
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. No single point of failure in the system;
10. Computer system controlled and local controller; and
11. Uninterrupted alarm monitoring.

Tenant planners shall coordinate with the Port Authority during the design phase, for direction on connectivity to Port Authority monitoring centers if appropriate. A tenant 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 all restricted areas.

2.6. Closed Circuit Television (CCTV)

Tenants may be required to plan for, install, maintain, and operate a comprehensive CCTV system, at the sole discretion of the Port Authority. CCTV surveillance shall provide continuous views of persons for tracking from the point of entry and throughout the tenant space. All

elements of the CCTV system shall have an UPS and battery backup that can sustain operations for a minimum of twelve (12) hours. An audible alarm must be operational when the UPS is activated and in use.

If a CCTV system is required, it shall be configured to reliably meet the following performance criteria:

1. Capability to configure and provide computer aided monitoring alerts to console operators when anomalies are noted;
2. Support programmable computer analytics and facial recognition software; and
3. 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 of integrating with the ACS if required at the sole discretion of the Port Authority.

The CCTV system must have a Video Management & Surveillance Systems (VMSS) configured to reliably meet the following performance criteria:

1. Compatibility with the existing Port Authority VMSS in accordance with Agency CCTV Standards and Verint VMS Supported IP Cameras to allow PAPD, OCSO and Facility Operations staff to view cameras in real-time;
2. Enable the display of live and recorded security camera video feeds at designated locations and support archiving video feeds on VMSS servers;
3. Enable the users to operate video streams, distribute the video, and store the video;
4. Ability to call up cameras, monitor and process images, and organize how images are stored, retrieved and integrated with third party applications;
5. 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;
6. Store all video for a minimum of 31 days for future retrieval;
7. Configure the distributed video recording server architecture and supporting software application to allow each of the master servers to operate in an independent mode, furnishing identical capabilities for live viewing, video recording and review functions to its connected review workstations;
8. Configure the Network Attached Video Storage solution to avoid any single point of failure and to operate independently of one another and support all integrated security systems; and
9. All elements covered herein for the VMSS shall have an UPS and battery backup that can sustain operations for a minimum of twelve (12) hours.

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 and
2. Equipment shall be furnished with the most current compatible version of firmware.

2.7. Public Address and Variable Message Systems

Depending on the type, size and configuration of a tenant space being constructed or altered, a Public Address (PA) and/or Variable Message System (VMS) may be required at the sole discretion of the Port Authority.

1. Systems must be sufficiently flexible to handle the various planned usages including emergency notifications;
2. Systems shall be configured by zones so that advisory messages and emergency announcements can be directed to specific areas where an emergency develops;
3. Emergency notifications shall take priority over all other messages. Standard wording of the distinct types of emergency messages shall be developed in advance in collaboration with the Port Authority;
4. Systems shall be integrated to enable alarm notifications to be precise, indicating location, type of danger and evacuation directions in calmly spoken live or recorded messages;
5. Systems shall provide sufficient sound volume and audible clarity of messages, a clear source of the message, proper routing of audio signals, appropriate equipment selection and acoustic design to avoid acoustic feedback and echo and to ensure that sound quality is maintained;
6. Systems shall have a minimum twelve (12) hour uninterrupted power source; and
7. The systems must be tied into the Port Authority facility Operations Control Center, at the direction of the Port Authority. Actual emergency messaging may come from PAPD as directed by an Incident Commander.

2.8. HVAC Systems

The design for HVAC systems must comply with the following:

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 access controlled, alarmed and monitored by CCTV (or by another type of unauthorized entry detection system).

3. The HVAC systems shall have a highly effective air filtration system and the ability to isolate airflow within the designated space. Filtration and air-cleaning systems may protect a building and its occupants from the effects of a chemical, biological, radiological (CBR) 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 spaces shall be for authorized personnel only and shall be enforced by employee background checks, official ID credentials, key card entry tied into ACS, and CCTV surveillance.
5. Video surveillance equipment shall be installed at all entry points and all entries shall be monitored and recorded.

2.9. Accommodation of Public Space for Police Screening

Depending on the type, size and configuration of a tenant space being constructed or altered, accommodation of space for use by PAPD may be required at the sole discretion of the Port Authority.

1. Design and construction of new or altered facilities, terminals, etc. shall incorporate space on the floors of entrances, exits and heavily trafficked areas that can be made available to PAPD to set up random screening operations for patrons, or deployment of screening technology.
2. Vehicular roadways entering or surrounding tenant spaces or Port Authority facilities shall incorporate strategic locations where PAPD can conduct random or targeted vehicle inspections.

2.10. Accommodation of New Security Technologies

Tenant designs, especially at entrance locations, shall be sufficiently flexible and adaptable to be capable of accommodating new, emerging, and next generation security technologies 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. SECURITY REQUIREMENTS FOR FACILITIES AND OTHER BUILDINGS IN PUBLIC AREAS

Facility public areas consist of the following: lobbies, passenger drop off and pick up, public frontage roadway, truck loading docks and any other area accessible to the public.

3.1. 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 facade which must be enforced by crash rated bollards which are specified in Section 3.2.
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 surrounding roadways and sidewalks.
4. Vehicle entrances and exits to public parking directly in front of facilities are not permitted.

3.2. Enforcement of Vehicle Standoff (Use of Bollards)

1. Standoff protection measures from vehicles must be provided adjacent to critical building assets.
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 facility.
3. The standoff distance between the bollard line and the facility façade is relied upon for protection and as such shall be maximized and equal or exceed the distance identified in the Protective Design Narrative.
4. 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.
5. 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.
6. Protective bollard dimensions and stainless-steel exterior sleeve are required to comply with Port Authority standards, which are based on ASTM International standards.

7. For bollards, the clear distance between the structural members shall not exceed 48” and the clear opening between the finished bollard covers shall be Americans with Disabilities Act (ADA) compatible.
8. ADA compliant curb cuts with tactile warning surface shall be provided between bollards per local codes and ordinances.
9. A minimum curb height of 6 inches must be provided at roadway frontages that accommodate ADA compliant kneeling buses.
10. 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.
11. Horizontal beam barriers shall have equivalent structural crash ratings as the standard bollard system. They may be operated manually, or power operated, with backup power provided.
12. Horizontal beam barriers shall be capable of being locked with access monitored by CCTV.

3.3. Building Entrances, Curtainwall and Facade Glazing

Security concerns must be addressed during planning and design of building facades.

1. The exterior curtain wall shall incorporate a blast debris mitigating system that shall provide a level of protection that is consistent with glazing systems designed to achieve a “high level” of protection as defined by the ISC Security Design Criteria for Federal Buildings, consistent with GSA Performance Condition 3b or better which provides a “High Level” of protection and “Low Hazard Level”.
2. Glazing panels themselves shall meet ASTM F2912 - 17 Standard Specification for Glazing and Glazing Systems Subject to Air Blast Loadings.
3. Building entrances and exits shall be designed with sufficient width to accommodate mass exodus during an emergency evacuation.

3.4. 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. 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.
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 inside the building 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 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. Hardening individual structural elements to resist blast effects so they do not fail and are repairable.

3.5. Vehicular Parking Lots and Garages

1. Vehicular parking lots and structures for public use shall be proven to have adequate standoff distance from facilities, and parking structures shall be designed to resist progressive collapse due to blast forces.
2. Vehicle height in parking structures shall be limited to 9’-6” vertical clearance.
3. Damage to the structure from the vehicle threat shall be limited to ASCE 59-11 “Heavy Damage” limits or better.
4. Maximum damage shall result in only localized collapse of no more than two adjacent structural columns that extend vertically through the structure but do not extend laterally.
5. Restricted parking areas close to the terminal must be access controlled, allowing vehicle access to only known persons or screened individuals who exhibit proper credentials.
6. 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.
7. Consult with the PSM to identify and determine physical and electronic security countermeasure requirements, including but not limited to crash-rated vehicle access barriers, vehicle screening technologies and CCTV coverage.

3.5.1. Trash and Recycling Receptacles in Public Areas

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

3.6. Perimeter Fencing

Certain areas surrounding buildings may require a perimeter fence to secure the area. The basic features of Port Authority perimeter security fences are as follows:

1. A continuous crash resistant concrete base is required where any type of vehicle may have access to the terrain where the fence line is constructed.
2. The minimum fence fabric height is 8’-0” above the top of concrete barrier or above finished grade
3. Chain link fabric is 1 ¾” x 1 ¾" with 0.192” OD wire, anti-climb with metal coated (galvanized) or polyvinyl chloride (PVC) coated.
4. In certain cases, the fence is topped with 3 lines of barbed wire, or concertina wire. The PSM, PAPD and Facility Operations Staff must be consulted before implementation.
5. To assist in surveillance and security patrol inspections, fences shall be configured as straight and uncomplicated as area conditions will allow to preserve long straight lines of sight and detection zones for visual observations from patrols, CCTV monitoring, and various fence system detection sensors.
6. Contact the PSM for the current Port Authority Security Fence design criteria when altering an existing security fence or constructing a new security fence.

3.7. Emergency Response Technologies

3.7.1. Gunshot Detection Systems

If required, Gunshot Detection Systems, which use acoustic and infrared sensors to detect the sound and the muzzle-flash of light associated with the discharge of a weapon, shall be installed in all public areas of facilities when appropriate. The systems use this technology to rapidly locate the source of gunshots within a terminal by triangulation on the origin of the shot while minimizing false alarms. It will be used by law enforcement to improve the speed of response to

the incident and provide the OCC with information that shall be used to alert, instruct, or advise the building occupants.

3.7.2. Emerging Emergency Response Technologies

Other emerging emergency response technologies under consideration include but are not limited to:

1. Chemical Sensor Detection
2. Biological Sensor Detection
3. Artificial/Machine Learning Systems
4. Video Analytic Systems
5. Other emerging technology to enhance public safety and physical security

4. PLANNING CONSIDERATIONS

Designing for the Future: The Guidelines may be modified or further amended, from time to time, as the Port Authority may reasonably require. As the amount of cargo activity and/or cruise passengers per year increases, and security equipment and technologies evolve, the facility needs to have the flexibility for change and the ability to adopt new security measures. Allowance for future modifications must be included in all tenant security planning.

5. INFORMATION SECURITY

The Handbook details the agency's information security policy for Port Authority Protected Information and systems. The Handbook is issued and controlled by the OCSO and provides requirements for the identification, handling, protection and storage of Port Authority Protected Information. To access the Handbook, click here.

6. ACRONYMS

ACS	Access Control System
CBR	Chemical, Biological, Radiological
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
CPD	Central Police Desk
CPI	Confidential Privileged Information
CPTED	Crime Prevention Through Environmental Design
EOR	Engineer of Record
ID	Identification
IED	Improvised Explosive Device
MTSA	Maritime Transportation Security Act
NDA	Non-Disclosure Agreement
NYPD	New York City Police Department
OCC	Operations Control Center
OCSO	Office of the Chief Security Officer
PA	Public Address
PANYNJ	The Port Authority of New York & New Jersey
PAPD	Port Authority Police Department
SIM	Security Information Manager
SIX	Port of New York and New Jersey Security Information Exchange
SOC	Security Operations Center
TSWG	Tenant Security Work Group
UPS	Uninterrupted Power Supply
USCG	United States Coast Guard
VMS	Variable Message Signs
VMSS	Video Management & Surveillance Systems
VSS	Video Surveillance System

7. REFERENCES

1. Maritime Transportation Security Act of 2002 (MTSA) (P.L. 107-295)
2. Port Authority of New York and New Jersey Information Security Handbook, April 2018
3. Port Authority of New York and New Jersey Security Planning Guidelines: Guidelines for Security Classification, Planning and Design at Project Inception for Port Authority and Tenant Projects, July 2024
4. Port Authority Technology Department – Technology Standards Overview
5. US Customs and Border Protection: Minimum Security Criteria – Marine Port Authority and Terminal Operators, November 2019

8. APPENDIX A

TENANT ALTERATION APPLICATION SECURITY CONSIDERATIONS

As noted in the **Seaport Facility Security Guidelines**, there is no "one size fits all" security solution based on the location, type and size of a tenant/contractor's operation. As such, working with the OCSO and the PSM, the tenant/contractor will identify the appropriate level of security technology, infrastructure and procedures required. A review of the Tenant Alteration Applications (TAA) will assist in ensuring that key security requirements for all projects are being met. Accordingly, when submitting a TAA relative to security requirements, please consider the information below.

Applicability

Requirements contained in this Appendix shall apply as a minimum to new construction, as applicable to the construction type. For alteration, renovation, and/or modification activities to existing premises, the applicability of the requirements shall be proportionate and commensurate with the nature of such alteration, renovation, and/or modification, as determined by the Port Authority. This will also be the case for new leases and/or lease renewals of existing premises. All TAA will be reviewed by the PSM and the PSM will establish applicable requirements for the TAAs on a case-by-case review. The PSM will ensure that all minimal security designs, technologies, and protocols are met by each tenant as needed.

Crime Prevention Through Environmental Design

Crime Prevention through Environment Design (CPTED) is based on the idea that the effective design and proper use of the built environment may lead to a reduction in the incidence of crime and improve the safety and use of the premises. The goal of CPTED is to reduce the number of opportunities for crime to occur. This reduction may be achieved by employing physical design features that discourage crime, while at the same time encourage legitimate use of the environment.

For more information on CPTED please refer to Section 2.3 of the **Seaport Facility Security Guidelines.**

Access Control Systems (ACS)

Tenants with access to areas that are designated as Restricted by the Maritime Transportation Security Act (MTSA) shall at a minimum, electronically monitor, record and control portals, doors, and access points for authorized personnel passing between the restricted and non-restricted areas, as required by current applicable law and regulations. In addition to any security measures

required under the MTSA and federal regulations, additional security measures may be required and updated by the PSM, PAPD or senior Port Authority management.

All portals, doors and access points which lead to restricted areas shall be electronically ACS monitored and controlled and must be equipped with an appropriate level door control and locking equipment. If the door also acts as an emergency exit, it shall be equipped with alarmed panic hardware operable from the inside only and otherwise kept secured at all times.

For more information on ACS please refer to Section 2.4 of the **Seaport Facility Security Guidelines.**

Closed Circuit Television (CCTV)

Tenants may be required to plan for, install, maintain, and operate a CCTV System at the sole discretion of the Port Authority. CCTV surveillance shall provide continuous views of persons for tracking from the point of entry and throughout the tenant space.

The CCTV system must have a Video Management & Surveillance Systems (VMSS), recording capabilities and be compatible with existing VMSS used at the facility. The tenant shall utilize only Internet Protocol (IP) cameras that have the capabilities to send and receive data via a computer network.

For more information on CCTV please refer to Section 2.5 of the **Seaport Facility Security Guidelines.**

Information Security

The Port Authority Information Security Handbook details the agency's information security policy for Port Authority Protected Information and systems.

If tenants come in contact with Port Authority Protected Information, it is expected that this information is handled with care as outlined in The Port Authority of New York and New Jersey Information Security Handbook.

All tenants, contractors, and vendors who require access to Port Authority Protected Information will be required to execute a Non-disclosure Agreement and may be subject to SWAC.

For more guidance on Information Security, please refer to Section 5 of the **Seaport Facility Security Guidelines.**