APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20005

APTA SS-ISS-RP-004-23
First Published: May 23, 2023

Transit Infrastructure Security Working Group

Security Considerations for Public Transit Passenger Stations and Stops

Abstract: This document proposes standards for enhancing the security of public transit stations and stops of all modes and the passengers who use them.

Keywords: assessment, balanced security, consequence, mitigation, passenger stations, risk, security posture, site planning, stops, threat, transit security, vulnerability

Summary: This document provides information to assist with the reduction of security risk for transit stations and stops. It discusses potential threats and vulnerabilities and various security mitigation measures that should be implemented to reduce security risk.

Scope and purpose: This recommended practice provides strategies to enhance the security of public transit stations and stops. It provides transit agencies with information regarding threats, vulnerabilities, consequences and assistance to identify potential mitigations and control strategies. The purpose of this document is to provide public transit operators with guidance in providing safe and secure public transportation of all modes.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **APTA Transit Infrastructure and Systems Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Lurae Stuart, *Chair*
Mark Uccardi, *Vice Chair*

Aldon Bordenave, *LA Metro*
Ryan Chelski, *Sound Transit*
Neil Crosier, *King County Metro*
Matthew R. Dimmick, *STV*
Dean Fajerski, *TSA*
Kevin Franklin, *BART*
Rick Gerhart
Erin Gorrie, *ADS System Safety*
Stephan Parker, *Transportation Research Board*
Rob Pascoe, *King County Metro*
Jacob Peltier, *Community Transit*
John Plante, *METRA*
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Charles Rappleyea, *WSP USA*
Harry Saporta, *WSP USA*
Jill Shaw, *DART*
Lurae Stuart, *WSP* USA
Kirsten Tilleman, *WSP USA*

Project team
Polly Hanson, *American Public Transportation Association*
Eric Halzel, *Eagle Hill Consulting*

Introduction

This introduction is not part of APTA SS-ISS-RP-004-23, "Security Considerations for Public Transit Passenger Stations and Stops."

Transit passenger stations and stops are key components to transit systems, as they are the first and last interface that passengers have with the transit system. They can serve a single transit line or provide service to multiple lines, systems or modes. Passenger stations and stops range from simple open-air stops along a public sidewalk or platforms with minimal amenities to more complex facilities with enclosed structures with waiting areas and a variety of passenger services. Passenger amenities may include seating, parking facilities, passenger drop-off areas (kiss and ride), restrooms, ticket sale windows or machines, food services, passenger information, and retail services. This recommended practice promotes measures, practices and strategies to reduce risk related to passenger stations and stops.

This document is intended to complement other documents or reports that address security for public transportation. It builds on and incorporates information described in the series of the APTA Security Standards Program documents. They should be reviewed and applied where applicable. APTA's Security Standards Program documents can be found on the APTA Standards website.

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Security and Design Considerations for Public Transit Passenger Stations and Stops

1. Passenger stations and stops overview

The first and final points of contact between the passenger and the transit system are the passenger stations or stops. They function as a central point to allow passengers to wait, board, disembark or transfer between modes of transportation and provide a safe and secure location to do so. If the location is perceived as unsafe or presents other hazards, ridership will be impacted and passengers may choose other methods to reach their destination. Station and stop features should have effective security measures as well as incorporate comfort and convenience enhancements to improve the passenger experience.

Information in this recommended practice is applicable to all modes of public transit passenger stations and stops. This document describes processes to identify issues, analyze and review various mitigation strategies, protect sensitive information, identify necessary training guidance, and promote maintenance to ensure operability of features as designed.

1.1 Stakeholder considerations

Security for transit stops and stations is one element of the security of the entire system. Security for the system must ensure that all elements are secured to reduce the risk to the system. Transit agencies should apply the recommendations based on their assessed risk.

1.2 Security risk assessment

Transit agencies should complete a current system-wide security risk assessment with recommendations to identify, evaluate and reduce risks to the system's people, assets, operations and infrastructure. Additional information about security risk assessments can be found in the APTA recommended practice "Security Risk Assessment Methodology for Public Transit" (APTA SS-SIS-S-017-21).

1.3 Benefits

Transit agency that apply this recommended practice to their transit operation will:

- recognize credible threats to their stations and stops;
- enhance the security and perception of safety by the reduction of station vulnerabilities; and
- reduce the risks related to stations and stops with application of appropriate mitigations and controls.

2. Passenger station and stop design

2.1 Station or stop environment

Transit stations and stops range from bus stops with only a sign along a public walkway and perhaps a bench for sitting to multimodal stations with passenger amenities, including vendor services for various passenger needs. Some stations are designed as designations in and of themselves where people go to enjoy amenities such as restaurants, movie theaters or retail store—even if they are not using the transit services. The first

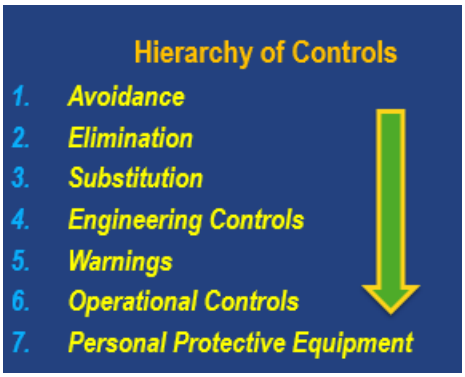
activity for providing security for the station or stop is to understand the scope of the stop or station, how it will be used and by whom, what assets are involved, and whether any external jurisdictions share responsibility for safety and security at the facility. These are all elements that should be explored or described when performing a stop or station security assessment. Much of this information would be found in a Concept of Operations, (ConOps), if one has been developed for the system or system elements. Having this information will inform not only what threats a stop or station might be vulnerable to, but also what level of protection might be needed.

2.2 Security design for new stops or stations

Security should be introduced early in the planning and design process to allow transit agencies to define security goals, objectives, strategies and operational requirements. During planning and design, transit agencies that include security considerations are able to impact the security of the eventual system or system elements to a greater degree. During design, agencies can implement the application of design principles that positively impact the security of the system.

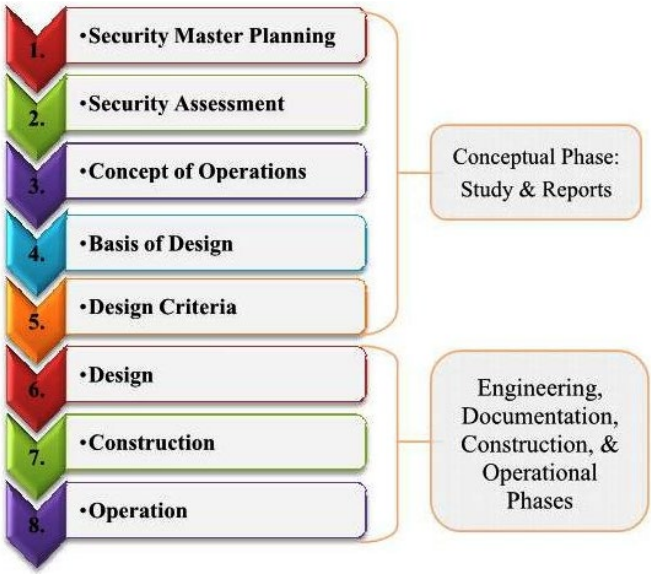
Two such principles that should be implemented in every design for a station or stop are Crime Prevention through Environmental Design (CPTED) and Prevention through Design (PtD). More information regarding CPTED can be found in Section 4.1.1 of this document, the APTA "CPTED for Transit Facilities" recommended practice, and the References section of this document. Prevention through Design (PtD) is a safety concept that follows the Hierarchy of Controls principle. Some controls are more effective than others when impacting the desired outcome. This design principle works as well in security as it does in safety. A design that avoids or eliminates a vulnerability is more effective than the application of a procedure or process. Procedures and processes are subject to human action and may not always be followed or implemented. The higher the control is located on the Hierarchy of Controls, the more effective it is. PtD is illustrated in **Figure 1**.

FIGURE 1
Prevention Through Design



Security for stops and stations should be part of a master security planning effort. Performing a security assessment on the system and system elements, including stops or stations, during preliminary design will identify specific threats and vulnerabilities that can then be addressed through the design and construction process. Other steps to designing in security include the development of design criteria, documenting the criteria that all project designs must follow to ensure they meet the program goals of the agency. **Figure 2** illustrates the project phases.

FIGURE 2
Project Security Implementation



It is critical to include review of the security design at each project phase. This provides verification that the agreed-upon security measures are incorporated in the design. Deviations or design changes should also be reviewed for impact to the security design elements. Prior to acceptance of the completed systems, include the security systems in the testing phase to validate and verify the operational effectiveness.

Introduction of security in the design phase makes operational and budgetary sense. Security systems or features retrofitted into structures or properties are more costly to implement and may provide less effective security protection.

2.3 Security for existing stops or stations

Transit systems implementing additional security for existing stops and stations will have to work with existing designs and may have additional challenges—and costs—to achieve a similar level of security. The same process of understanding the concept of operation for the stops and stations is critical. Performing a security risk assessment is essential to determine the threats facing the system elements, but also what vulnerabilities are inherent in the existing design and operation. Elements of CPTED and PtD still may be implemented in existing stops and stations but will require additional effort to achieve the same levels of benefit.

3. Threats, vulnerabilities and consequences related to stops and stations

Passenger stations and stops are fixed locations with open access, making them difficult to secure. They may be at grade, above or below grade, or designed with multiple levels. Understanding the types of threats and vulnerabilities common to stops and stations will assist transit agencies in determining the mitigations that may help to secure the stops and stations in their transit systems.

3.1 Threats to stops and stations

Threats, both criminal and terrorist, vary in their desired outcome. If the threat is theft of goods, then the perpetrator might be looking for dark, isolated areas where the theft can proceed undetected. If the goal is to

inflict mass casualties, then optimum locations are areas where large groups of people gather. Known threats to passenger stations and stops are described in **Table 1**.

TABLE 1
Threat Types and Descriptions

Threat Type	Types Within Category
Explosives	Improvised explosive device (IED), vehicle-borne improvised explosive device (VBIED), person-borne improvised explosive device (PBIED), improvised incendiary devices (IID)
Chemical	Toxic industrial chemicals and poisons
Active attacker	Use of standard firearms and other weapons
Standoff attack	Weapons from a distance, unmanned aircraft system (UAS)
Cyberattack	Viruses, worms, Trojan horses and ransomware
Sabotage	Intentional damage or destruction of systems
Hoax call/device	Intentional false alarm or threat that potentially disrupts operations
Crimes against persons	Assault, homicide, theft, vehicle ramming
Crimes against property	Robbery, arson, cargo theft, vandalism, burglary, fare evasion
Victimless crimes	Organized crime presence, using system to move contraband
Quality of life crimes	Vagrancy, trespass, panhandling, drug/alcohol abuse

Not all stations or stops will be the target for each of the listed threats. To utilize resources appropriately, agencies should focus on credible threats for their stations or stops. Credible threats for a specific agency's stops or stations should be determined during the security risk assessment. This information is usually resourced through local law enforcement or federal agencies, including the Transportation Security Administration (TSA). These resources are available for every transit agency to understand the credible threats for their areas of operation. Potential threats and targets, including relative threat level for stations or stops, are included in **Table 2**.

The potential threat rating is based on the combination of intent and capability to carry out the threat. A threat with a very high rating (red) is a significant and proven threat based upon demonstrated intent and demonstrated capability; whereas a threat with a low rating (green) is an acknowledgement that the general threat exists and should be monitored, as the intent and capability have not been proven. As previously noted, the threat level for an agency is dependent on available threat intelligence and history. See APTA's standard "Security Risk Assessment Methodology for Public Transit" for additional information on threat ratings.

TABLE 2

Station/Stop Threats, Targets and Relative Threat Level

Potential Threat	Delivery Method	Threat to Asset	Target/Affected Group
VBIED	• Small vehicle (<227 kg TNT) • Medium vehicle (<454 kg TNT) • Large vehicle (<1814 kg TNT) • Delivery truck (<4536 kg TNT)	🔴	• Passengers • Employees • Community members • Joint station tenants • Equipment • Station structure
Active attacker, assault	• Long range (sniper) • Close range • Edged blade	🔴	• Passengers • Employees • Community members • Joint station tenants • Equipment
Standoff attack	• Rocket-propelled grenade	🟢	• Passengers • Employees • Community members • Joint station tenants • Equipment • Station structure
Vehicle ramming	• Motor vehicle	🟡	• Passengers • Employees
Transport vehicle delivery	• Bus/train used as a VBIED	🟢	• Passengers • Employees • Community members • Joint station tenants • Equipment • Station structure
IED	• Suicide attack • Small object (<2.3 kg TNT) • Medium object (<23 kg TNT)	🔴	• Passengers • Employees • Community members • Joint station tenants • Equipment • Station structure
Chemical	• IED dispersion • Spilled broken containers • Aerosolized	🟡	• Passengers • Employees • Community members • Joint station tenants
Biological attack	• Release of viruses, bacteria or other toxins	🟢	• Passengers • Transport personnel • Community members • Joint tunnel/station tenants
Incendiary attack	• Incendiary device • Flammable materials	🟡	• Passengers • Employees • Community members • Joint station tenants • Equipment • Station structure

TABLE 2
Station/Stop Threats, Targets and Relative Threat Level

Potential Threat	Delivery Method	Threat to Asset	Target/Affected Group
Radiological event	• IED	🟢	• Passengers • Employees • Community members • Joint station tenants
Kidnapping	• Taking control of one or more employees or passengers	🟢	• Passengers • Employees • Community members • Joint station tenants
Cyber	• Disabling station functions through internet or network connections	🔴	• Passengers • Employees • Community members • Equipment
Crimes against persons (theft)	• Distraction • Surveillance	🔴	• Passengers • Employees
Crimes against persons (assaults)	• Weapons	🟡	• Passengers • Employees
Crimes against persons (intimidation)	• Large groups • Gang activity • Bullying	🔴	• Passengers • Employees
Crimes against persons (pickpocketing)	• Distraction • Surveillance	🔴	• Passengers
Crimes against property (vandalism)	• Paints, markers • Destructive Instruments	🔴	• Station assets • Station facilities
Other crimes on transport property (fare evasion)	• Persons • Large crowds	🔴	• Employees • System
Other crimes on transport property (loitering)	• Large groups • Persons • Cultural practices	🔴	• Stations • Passengers
Other crimes on transport property (alcohol/drug-related offenses)	• Persons	🔴	• Passengers • Employees
Other crimes on transport property (trespassing)	• Persons • Surveillance	🔴	• Passengers • Employees

🔴 High 🟡 Medium 🟢 Low

3.2 Vulnerability of stops and stations

A vulnerability is defined as any weakness, flaw or condition that allows and/or can be exploited for the successful realization of a potential threat against the transit system. As the threat environment is ever-

changing, vulnerabilities to different threats and attack methods may also change. Transit agencies should constantly review their threat and vulnerabilities to ensure that they are addressing current trends.

Vulnerability conditions can be classified into two different types: physical and procedural. A physical vulnerability condition is an actual physical deficiency, flaw, or absence of physical measures designed to deter, detect, delay and/or respond against a breach or unauthorized access to the stop or station. A procedural vulnerability condition relates to the existence, implementation, legality and oversight of policies and procedures that are designed to deter, detect, delay or respond against a breach or unauthorized access to the stop or station. Some potential types of vulnerabilities that might be found in a station or stop include:

- **Potential physical vulnerabilities:**
  - Lack of barriers/fencing
  - Lack of access control
  - Lack of adequate lighting
  - Lack of CCTV
  - Lack of hardened structures
  - Lack of fire-resistant materials
  - Lack of hostile vehicle mitigation (HVM)
  - Lack of intrusion detection systems
  - Lack of CBR detection system
  - Lack of emergency response equipment
  - Lack of CPTED implementation

- **Potential procedural vulnerabilities:**
  - Insufficient background checks for employees
  - Lack of security checkpoints
  - Lack of access control procedures
  - Lack of suspicious activity reporting procedures
  - Lack of security force
  - Lack of transportation police or security force presence
  - Unattended facilities or vehicles reporting
  - Lack of chain of custody procedures
  - Lack of liaison with external authorities
  - Lack of sufficient area sweeps
  - Lack of vehicle sweeps
  - Lack of procurement procedures
  - Predictable security patrols
  - Poor communication and information collaboration
  - Lack of oversight and audit procedures
  - Lack of maintenance procedures
  - Lack of equipment deficiency reporting
  - Lack of security staff performance management procedures
  - Lack of employee security awareness training and management
  - Lack of incident response procedures

The successful execution of a threat is dependent upon the presence of either a physical or a procedural vulnerability, or both. By identifying the physical and procedural conditions that contribute to a certain threat, it is possible to start developing mitigation strategies to address the vulnerability and therefore reduce the likelihood and/or consequences of a successful attack. In general, vulnerability conditions allow access to an asset in order to be attacked.

Some additional station and stop features or elements that might impact vulnerability are listed in Appendix A. This list can be used as a starting point to identify potential vulnerabilities in a transit agency's stations and stops. It is critical to understand that vulnerabilities are specific to a threat. Without a threat, there is no vulnerability.

3.3 Consequences

Along with threats and vulnerabilities, security risk assessments of passenger stations assess the consequences of a realized threat against an asset. Consequence is measured by the level of impact on primary areas of people, equipment and service and by the impact upon the secondary areas of finance and reputation. A summary of potential impacts of some specific threats to stations and stops is contained in **Table 3**. Actual consequences for a transit agency's stations and stops would be determined in the security risk assessment.

TABLE 3
Impacts of Realized Threats

Threat	IED	VBIED	Active shooter	CBR	IID	Sabotage	Cyber	Crime
Fire/smoke damage	✓	✓			✓			✓
Flooding damage					✓			✓
Structural damage	✓	✓			✓	✓		
Progressive collapse	✓	✓			✓			
Closure of facility	✓	✓	✓	✓	✓	✓		✓
Passenger station closed	✓	✓		✓	✓	✓		✓
Contamination	✓	✓		✓				
Extended public health issues	✓	✓		✓				
Mass casualties	✓	✓	✓	✓	✓			
Utility disruption or outage	✓	✓			✓	✓		
Cyber/network disruption	✓	✓			✓	✓	✓	
Loss of revenue	✓	✓						✓

4. Station and stop mitigations

The security risk assessment process identifies threats, vulnerabilities and consequences and proposes mitigation measures to reduce risk to people, operations and assets to an accepted level. There are a variety of mitigations that can be applied to stops and stations. Some mitigations are design related and physical in nature, and others are procedural or operational. The most effective mitigations are layered, using a combination of mitigations to provide the best protection. To ensure that a robust and effective security outcome is delivered, measures must be complementary and offer sufficient redundancy should one or another completely or partially fail. The mitigation measures offered within this section are not the full extent of risk treatment options but provide insight into protective security measures and the three security principles that are widely and successfully adopted for risk management within and outside of the transport environment.

4.1 Security principles

4.1.1 Crime Prevention Through Environmental Design

CPTED is a multidisciplinary approach to crime prevention and differs from traditional approaches by placing emphasis on human activities and how they become exposed to crime through environmental design. The National Crime Prevention Institute defines CPTED as a tool in creating safer environments:

> The proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, and an improvement in the quality of life.

CPTED offers a holistic approach based on sociology, psychology and ecology of crime, as well as environmental criminology, criminal justice and architecture. The CPTED principles are applied to a physical environment or structure to reduce opportunities for violence and crime in a community and have the result of making people feel safer. It is based on the principle that most criminals decide to commit crimes based on opportunity that is inherent in how human space is designed or being used.

CPTED differs from procedural and physical security by placing emphasis on natural strategies. Strategies are aimed at integrating and incorporating behavior management into the design of human activity and physical resources.

Applying CPTED strategies to a passenger station or stop environment can reduce the perception of the fear of crime at an agency's properties. Strategies include establishing territorial boundaries to establish a sense of ownership, reducing opportunities for crime by controlling access, and observing the behaviors of users of the space. Additional information about this topic is found in the APTA recommended practice "Crime Prevention Through Environmental Design (CPTED) for Transit Facilities" (APTA SS-SIS-RP-007-10). This recommended practice features a CPTED Considerations Survey to help decide which functional areas may be applicable to your transit agency and inform security planning.

4.1.2 Layered protection

Security measures at several different levels or "layers" throughout a system, and at each station or stop, provide greater redundancy and defense-in-depth protection for station/stops and the system. The concept of layered protection recommends placing the most critical or vulnerable assets in the center of concentric levels of increasingly stringent security measures. This allows multiple opportunities for thwarting or disrupting criminal and terrorist activities and is a key aspect of an effective security management strategy. The integration of CPTED supports the outcomes and efficiency of the layered security approach by causing threat actors to alter their behavior to suit the CPTED environment.

Layered protection is more applicable to an enclosed station environment where there might be other transit operations incorporated in the station structure. A station that has public and private space should have more protective measures to secure the private areas of the station.

Private or restricted spaces should have signs that give notice, identify boundaries and provide appropriate warnings to users, such as "No Trespassing," "Keep Out," "Restricted Area," etc. Where applicable, transit agencies should coordinate physical hardware installation for designated zones to reinforce boundary access controls to form layers of protection around an area.

Physical hardware, for example, may range from painted lines to locking doors, fencing and gates, or landscape and hardscape features. Begin designated zones, coupled with layers of protection at the boundaries of a station or stop, and continue overlapping layers of coverage ending within an interior location of a station or stop. See APTA recommended practice "Standard Security Program Considerations for Public Transit" for additional information about designation of zones.

4.1.3 Scalability

The selection of security measures within the system should be considered in the context of providing ongoing sufficiency and support scalability during periods of elevated threat. During the design/planning phase of a project, the selection of day-to-day "baseline measures" that offer full scalability during periods of elevated threat and then subsequent reduction of threat is important for the continuing efficiency of the transportation system.

4.2 Station or stop mitigations and controls

The effectiveness of layered security is assessed by the ability of the measure to offer deterrence, delay, detection, response and recovery qualities, with some control measures offering more than one quality. For instance, transit agency employee and security force presence offers deterrence, detection and response qualities. Similarly, some security measures, such as personnel screening, offer benefits to other parts of or the entire transit system, not just passenger stations and stops.

Table 4 indicates the attributes or properties that each control measure contributes to a layered security system for stations and stops. Deter, delay, detect and respond are risk-reduction strategies for enhanced station and stop security.

TABLE 4
Security Mitigation Measures for Stations and Stops

Physical Measures					
Security Measures	**Element Attribute**				
	Deter	**Delay**	**Detect**	**Respond**	**Recover**
Signage	Yes	No	No	No	No
Barriers/fencing (CPTED)	Yes	Yes	No	No	No
Access control	Yes	Yes	No	No	No
Proximity to local traffic (pedestrian and vehicle)	Yes	Partial	Partial	Partial	No
Open lines of sight (CPTED, absence of building or terrain cover)	Yes	No	Yes	No	No
Security lighting (CPTED, area lighting conditions)	Yes	No	Yes	No	No
Construction/building materials and design (CPTED)	Partial	Yes	No	No	No
Vehicle control and calming measures (CPTED)	Yes	Yes	Yes	No	No
Security buffer zones (CPTED)	Partial	Yes	No	Yes	No
Emergency telephones and blue-light stations	Yes	No	Yes	No	No
Designated fare zone (platform, station or stop)	Partial	Partial	No	No	No
Video surveillance system or CCTV	Yes	No	Yes	Yes	No
Intrusion detection systems	Yes	No	Yes	Yes	Partial
Identity cards	Partial	No	Yes	No	No
Security checkpoints	Yes	Yes	Yes	Yes	No
Law enforcement or uniformed security patrols	Yes	Yes	Yes	Yes	Yes
Covert security patrols	Partial	Yes	Yes	Yes	No

TABLE 4

Security Mitigation Measures for Stations and Stops

Procedural and Protocol Measures					
Security Measures	**Element Attribute**				
	Deter	**Delay**	**Detect**	**Respond**	**Recover**
Employee security awareness program	Yes	Yes	Yes	Yes	Yes
Background checks and vetting	Yes	No	Yes	No	No
Public security awareness program	Yes	No	Yes	No	No
Employee termination procedure	No	No	No	Yes	No
Staff training	Yes	Yes	Yes	Yes	Yes
Access control management	Yes	Yes	Partial	No	No
Lock-key management practices	No	Yes	No	No	No
Housekeeping	No	Partial	Yes	Partial	No
Evacuation plans	No	No	No	Yes	No
Chemical, biological, radiological (CBR) detection system	No	No	Yes	Yes	Partial
Emergency management planning	No	No	No	Yes	Partial
Emergency response equipment	No	No	No	Yes	Yes
Business continuity management	No	No	No	Yes	Yes
Liaison with external authorities	Partial	No	No	Yes	Partial
Emergency drills and exercises	No	No	No	Yes	Yes
Communication and information collaboration	Yes	No	No	No	Yes
Prior publicized responses to security incidents	Yes	No	No	No	No
Security access procedures	Yes	Yes	Partial	No	No
Security checkpoints	Yes	Yes	Yes	Yes	No
Incident response	No	Yes	Yes	Yes	Yes
Incident response plan	No	No	No	Yes	Partial
Emergency response equipment	No	No	No	Yes	No
CBR detection system	No	No	Yes	Yes	No
Surveillance capability	Yes	No	Yes	No	No
Security inspection and search	Yes	No	Yes	No	No
Suspicious activity reporting	No	No	Yes	Yes	No
Oversight and audit	Partial	Partial	Partial	Partial	Partial
Maintenance	Partial	Partial	Partial	No	Partial

4.3 Physical security mitigations

Each stop or station should be assessed for possible mitigations to reduce the security risk to people, operations and assets. This section contains a brief overview of mitigations that have benefits against the key security functions of deterring, delaying, detecting or responding to an event at a station or stop.

4.3.1 Physical mitigations

Signage

Deter	Delay	Detect	Respond	Recover
Yes	No	No	No	No

Signage can direct the public away from non-public spaces and warn against unauthorized entry.

Barriers/fencing

Deter	Delay	Detect	Respond	Recover
Yes	Yes	No	No	No

Barriers or fences are physical measures that provide visible barriers, deter unauthorized access, and serve to demarcate and secure physical areas. The protection level that a barrier or fence may offer is dependent upon height, construction, the material used, and any additional security feature used to increase its performance or effectiveness, such as barbed tape topping or electronic intruder detection equipment. The design of a barrier or fence should be commensurate with the risk from unauthorized intrusion. Determination of the type of barrier should also include whether the material is resistant to cutting, whether it limits someone from crawling or burrowing beneath, and the requirement for visibility from and to both sides of the fence/barrier. Barriers and fencing should be implemented in stations that have spaces that should not be accessed by passengers or the public, such as entrances to the guideway.

Access control

Deter	Delay	Detect	Respond	Recover
Yes	Yes	Partial	No	No

Physical access controls are measures that limit unauthorized access to restricted areas and assets such as facilities, rooms, information and people. Access control measures range from manual systems requiring a key or guard at a gate/door, to an automated electro-mechanical system linked to a control unit that upon verifying a cardholders credentials (identity card) provides automatic release and entry. Despite the automated nature of an electro-mechanical system, a degree of human intervention/oversight is always required. Access control measures should be implemented for stations with non-public spaces.

Security lighting

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	No	No

Security lighting supports surveillance of key areas and assets, deterring unauthorized entry to an area while aiding in detection. The positioning and usage of both regular and security lighting is part of the application of CPTED by reducing dark areas. The standard of lighting is an important consideration; lighting to a certain level of vertical lux (lighting quality and radiance) is necessary to support CCTV and human surveillance of key areas and assets. The application of good lighting applies to all stations and stops. See the APTA recommended practice “Security Lighting for Passenger Transit Facilities.”

Emergency telephones and blue-light stations

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	No	No

Emergency telephones and blue-light stations enhance the perception of safety at stations or stops. Emergency telephones can also to detect and enable response to a security incident. The following strategies should be incorporated when utilizing emergency telephones:

- Incorporate them into the agency's existing emergency phone network.
- Include all station platforms, elevator waiting areas, stairwell entries, parking structures, park-n-rides, pedestrian tunnels and pedestrian bridges that are indicated by the security risk assessment.
- Connect automatically to a dispatch center, local first responder or agency operations center.

Construction/building materials and design: Hardened/blast-rated structures

Deter	Delay	Detect	Respond	Recover
Yes	Yes	Partial	No	No

Blast-rated structures provide varying degrees of protection against explosive blast effects. The protection offered is dependent upon the materials used in construction and design. Blast-rated building materials with architectural design allow for the deflection, dissipation or shaping of the explosive blast to reduce the consequence of an explosive detonation while offering a degree of deterrence to a threat event. This mitigation is appropriate for structures that are assessed with a high likelihood of a blast event.

Construction/building materials and design: Fire-resistant materials

Deter	Delay	Detect	Respond	Recover
No	Yes	No	No	Yes

Fire-resistant materials reduce the impact of accidental fire events and incendiary and improvised explosive attacks. Fire resistant material provides heat protection and limits the amount of combustible material. Fire resistance can be inherent in a product material or physically applied to assets (spray or paint) and dependent upon the properties can delay and offer recovery to/from fire and explosive detonation events. This mitigation should be applied to all stop and station furnishings, shelters and station infrastructure.

Vehicle control and calming measures

Deter	Delay	Detect	Respond	Recover
Yes	Yes	Yes	No	No

Hostile vehicle mitigation (HVM) is the placement of bollards, hardened barriers and road calming measures. HVM is consistent with the application of CPTED through the physical control of vehicles by shaping the environment to change human behavior. HVM measures may include:

- raised curbs;
- solid steel bollards;
- concrete barriers or planters;
- pop-up vehicle barriers;
- other vehicle gates; and
- serpentine road calming measures.

The level of protection that a barrier provides against a hostile vehicle is rated against the size/weight, type and speed of the vehicle. The proximity between a vehicle and a structure/building/facility has a proportionate effect on the amount of physical damage that may result from an explosive blast detonated from a vehicle.

Security checkpoints

Deter	Delay	Detect	Respond	Recover
Yes	Yes	Yes	Yes	No

Security checkpoints may be either permanent or temporary/random; they are staffed by security personnel and/or transport police officers throughout the public transportation system to provide a visible human security presence and deterrence and to verify bona fides and access authority. Temporary and random security checkpoints are a useful tool to monitor and mitigate certain human behaviors while offering a deterrence, delay, detection and response capability to any event. Security checkpoints may be indicated based on risk to a station. Security checkpoints are not a mitigation for open stops or platforms.

Emergency response equipment

Deter	Delay	Detect	Respond	Recover
No	No	No	Yes	Yes

Emergency response equipment is crucial during or in response to an emergency or security incident and aids in reducing the consequences of such an event. Emergency response equipment such as fire extinguishers, first aid kits, gas masks/breathing apparatus, flashlights, and emergency response tools—together with trained personnel—provide a ready response and recovery capability. This should be implemented for every enclosed station environment. For open stops and platforms, emergency response equipment should be available for a response to an incident.

Intrusion detection systems

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	Yes	Partial

Intrusion detection systems are technological systems that detect unauthorized access throughout the system. An intrusion system can be integrated with the CCTV and access control systems, as well as used along perimeter fencing and barriers, to indicate a breach or intrusion into the system. This physical measure deters, detects and responds to security events while offering a partial degree of recovery in reestablishing integrity of a site or area. This mitigation should be considered for all enclosed stations, especially if critical operating functions are included within the station facility.

Video surveillance system (VSS) or closed-circuit television (CCTV)

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	Yes	No

A VSS or CCTV system is composed of cameras, communication feeds, servers, control consoles and video monitors. These systems can offer a range of analytical capabilities from simple to highly complex with varying degrees of scalability. VSS/CCTV systems aid in the deterrence and detection of security threats. A VSS/CCTV system can provide video evidence of occurrences throughout a transport system, aiding in response and detection of threat targeting and reconnaissance activities assisting post-event investigations. If utilized, it is critical that procedures and protocols are implemented to ensure that VSS/CCTV capabilities are utilized fully. VSS/CCTV offers deterrence, detection and response elements. This mitigation should be

implemented in all stations and considered for high-volume stops. Guidance on locations of VSS/CCTV in a station environment is provided in **Table 5**. In addition to those locations listed in **Table 5**, other locations as identified by a transit agency's threat and risk assessment should be considered.

TABLE 5
Station/Stop VSS/CCTV Placement Locations

Property boundaries and approaches	Choke points
ROW approaches to station	Elevators and areas of rescue
Pathways/walkways/pedestrian tunnels or bridges	Stairs/escalators
Entry and exit doorways	Fare gates
Station platform edges	Ticket vending machines (TVMs)
Stop street curb edges	Ticket selling windows
Critical assets contained in the station	Emergency telephone or blue light stations
Entrances to non-public areas in the station	Off-hours waiting areas (OWAs) on station platforms
Fare zones	Parking associated with kiss-and-ride

Chemical, biological, radiological (CBR) detection system

Deter	Delay	Detect	Respond	Recover
No	No	Yes	Yes	Partial

CBR detection technology or sensors can be installed or portably used by security and/or transport police to detect the presence of chemical, biological and radiological elements. CBR detection systems are used primarily to determine and aid in the detection and response of a chemical, biological or radiological event, whether intentional or accidental. This mitigation should be implemented only if the threat environment indicates that this is a credible threat to the station.

4.3.2 Procedural and protocol mitigations

Employee security awareness program

Deter	Delay	Detect	Respond	Recover
Yes	Yes	Yes	Yes	Yes

An employee security awareness program provides for training and procedures in security covering the instruction, training, management, adherence and development of a corporate security culture. An employee awareness program aids in providing a motivated and capable resource providing deterrence, delay, detection, response and recovery from a security event. This program protects the entire system, including stops and stations, and should be implemented by every transit system.

Public security awareness program

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	No	No

Public security awareness programs play an important part in crime prevention and security at stations and stops. These programs inform transit customers to recognize potential threats and the steps to report suspicious activity or items to a transit vehicle operator or station staff member. They also educate customers in measures to deprive criminals of opportunities to commit crimes; improving situational awareness for their personal safety.

Liaison with external authorities

Deter	Delay	Detect	Respond	Recover
Partial	No	No	Yes	Partial

Liaison with external authorities provides the information collaboration and communication processes for conveyance of intelligence, security threats, risk information, changes to operational status and deviations from the status quo. Fostering relationships with external stakeholders contributes to the integrity of the public transport system by building internal and external capability, including the following:

- Department of Homeland Security (DHS)
- Transportation Security Administration (TSA)
- Federal Transit Administration
- state and local law enforcement
- other transit systems

Every transit agency should document and be in communication with the external authority agencies to determine threats and coordinate response activities.

Without disclosing security-sensitive information, it is beneficial to share a familiarization program with all local first responders that cover a brief overview of the agency's physical security mitigations for awareness. Agencies may also offer site tours for first responders to review the mitigations in person.

Background checks and vetting

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	No	No

Background checks of employees provide the vetting and due diligence that provides information to aid determination of employee and contractor suitability for employment on grounds of professional competence, character and security risk. The type of background investigation depends on the position's security requirements. Background checks include, among others, verification of identity, analysis of criminal record, employment history, education and other activities. For enclosed station facilities, especially where other critical functions are part of the station environment, employees accessing those facilities should be vetted prior to allowing access.

Access control management

Deter	Delay	Detect	Respond	Recover
Yes	Yes	Yes	No	No

Access control procedures provide the protocol and process for the management of human behavior to control the access and egress of people and vehicle into and out of a facility or area. Procedures defining access arrangements may vary significantly from site to site and from the areas within, dependent upon criticality of assets, risk and role/function and purpose of people accessing a defined area.

Security inspection and search

Deter	Delay	Detect	Respond	Recover
Yes	No	Yes	No	No

The procedures relating to inspections and search of station areas and equipment provide instruction toward achieving and maintaining the security integrity of the station. Security inspection and search procedures provide assurance in response to and recovery from an event. Incorporating inspection and search activities into day-to-day operational duties is important in maintaining the required standard of security performance while allowing potential threats and hazards to be detected early.

Suspicious activity reporting

Deter	Delay	Detect	Respond	Recover
No	No	Yes	Yes	No

Suspicious activity reporting procedures provide instruction and process on the reporting of people, objects and circumstances deemed to be out of the ordinary and suspicious. The determination and reporting of suspicious events can be qualified by certain staff through analysis of the situation against a number of predetermined elements. There are many quick analysis tools used to determine the nature of unattended items in public areas; an example of a proven method of analysis is the HOT Principle (Hidden, Obviously suspicious, not Typical for the area) that is widely used throughout transport systems internationally.

Communication and information collaboration

Deter	Delay	Detect	Respond	Recover
Yes	No	No	No	Yes

Communication and information collaboration procedures and protocols relate to the internal communication and information flow of the regulator. These procedures define who, what, where, when, why and how security information is communicated across the public transportation network and the users of the public transportation system. These procedures deter and recover to/from security risks.

Oversight and audit

Deter	Delay	Detect	Respond	Recover
Partial	Partial	Partial	Partial	Partial

Security oversight and audit procedures and activities relate to the assurance process and methodology used to review, assess, audit, test, evaluate, document, report and resolve the implementation and performance of the security system and its elements. While audit and oversight activities do not deter, delay, detect, respond to and recover from a security event, the conduct of activities provides a quality assurance that is integral to risk management and continual improvement by enhancing all five elements. This is critical mitigation that applies to all transit agencies and should be implemented to reduce risk to all system elements, including stations and stops.

Maintenance

Deter	Delay	Detect	Respond	Recover
Partial	Partial	Partial	No	Partial

Similar to oversight and audit activities, the program and conduct of station and stop maintenance provides assurance to ensure system and security operates in accordance with required standards. Inspecting, maintaining, rectifying and documenting equipment and facilities for anomalies or issues maintains the integrity of the physical security risk mitigation measures in place. These procedures also incorporate the reporting of equipment deficiency to provide aspects of deterrence, delay, detection and recovery.

Incident response

Deter	Delay	Detect	Respond	Recover
No	Yes	Yes	Yes	Yes

Incident response procedures provide instruction on the processes for communicating about, reacting to and responding to a security risk event. The application of procedures provides a delay, detection, response to and recovery from a security risk and complements the Emergency Response Plan and procedures.

Emergency Response Plan

Deter	Delay	Detect	Respond	Recover
No	No	No	Yes	Partial

An Emergency Response Plan and procedures provide guidance and instruction for the response to and may also include recovery aspects to events deemed emergency. An Emergency Response Plan will include how an organization will respond to both safety and security events and is deemed a crucial element to the resilience of a transport system. Legislation and regulatory bodies may mandate the contents of a plan.

Related APTA standards

APTA SS-ISS-WP-001-20, "Cleaning and Disinfecting Transit Vehicles and Facilities During a Contagious Virus Pandemic"
APTA SS-SIS-RP-007-10, "Crime Prevention Through Environmental Design (CPTED) for Transit Facilities"
APTA SS-SIS-RP-001-10, "Security Lighting for Transit Passenger Facilities"
APTA SS-SIS-RP-003-10, "Fencing Systems to Control Access to Transit Facilities"
APTA-SS-SIS-RP-004-10, "Chain Link, Mesh, or Woven Metal Fencing Systems to Control Access"
APTA-SS-SIS-RP-005-10, "Gates to Control Access to Revenue and Nonrevenue Transit Facilities"
APTA-SS-SIS-RP-006-10, "Ornamental Fencing Systems to Control Access at Transit Facilities"
APTA-SS-SIS-RP-007-10, "Bus Stop Design and Placement Security Considerations"
APTA SS-SIS-S-010-13, "Security Considerations for Public Transit"
APTA SS-SIS-RP-011-13, "Security Planning for Public Transit"
APTA SS-SIS-RP-012-13, "Security Operations for Public Transit"
APTA SS-SIS-RP-013-13, "Physical Security for Public Transit"
APTA SS-SIS-WP-014-13, "Trash and Recycling Receptacles for Transit Facilities"
APTA-SS-SIS-RP-015-13, "Equipment and Technology"
APTA SS-SIS-RP-016-15, "Tunnel Security for Public Transit"
APTA SS-SIS-RP-017-21, "Security Risk Assessment Methodology for Public Transit"
APTA-SS-SRM-RP-001-09, "Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)"
APTA-SS-SRM-WP-002-10, "Random Inspections of Carry-On Items in Transit Systems"
APTA-SS-SRM-RP-005-12, "Security Awareness Training"
APTA-SS-SRM-RP-006-11, "Random Counterterrorism Measures on Transit Systems"
APTA-SS-SRM-RP-007-12, "Recognizing and Responding to Unattended Packages, Objects and Baggage"
APTA-SS-SRM-RP-009-09, "Identifying Suspicious Behavior in Mass Transit"
APTA-SS-SRM-RP-012-09, "Conducting Revenue Vehicle Security Inspections"

References

The Atlantic, "Broken Windows: The police and neighborhood safety," J.Q. Wilson and G.L. Kelling, March 1982. http://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/5/

Atlas, R.I., "21st Century Security and CPTED: Designing for critical infrastructure protection and crime prevention," 2nd Ed., CRC Press: Taylor & Francis Group. Boca Raton, Florida, 2013.

American Association of State Highway and Transportation Officials (AASHTO), "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection."

ASIS International, "A Comprehensive Glossary of Terms for the Security Industry. https://www.asisonline.org/globalassets/professional-development/careers/career-resources/wis---glossary-of-terms-for-the-security-industry..pdf

Congressional Research Service, "CRS Report for Congress. Passenger Rail Security: Overview of Issues," Order Code: RL32625, October 2004. http://www.hsdl.org/?view&did=450362

Department of Defense (DoD), Unified Facilities Criteria (UFC), DoD Minimum Antiterrorism Standards for Buildings, UFC 4-010-01, August 2020. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-01

Department of Defense (DoD), Unified Facilities Criteria (UFC), Design of Buildings to Resist Progressive Collapse, UFC 4-023-03, November 2016. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-023-03

Department of Homeland Security (DHS), National Terrorism Advisory System (NTAS). www.dhs.gov/files/programs/ntas.shtm

DHS. Building and Infrastructure Protection Series (BIPS 02), Integrated Rapid Visual Screening (IRVS) of Mass Transit Stations, 2011.

DHS/Federal Emergency Management Agency (FEMA), Homeland Security Exercise and Evaluation Program (HSEEP). https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

DHS/Transportation Security Administration (TSA), Sensitive Security Information Program, SSI Training for Surface Transportation Stakeholders.

Federal Emergency Management Agency (FEMA), Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks, FEMA 430, 2007. https://www.fema.gov/sites/default/files/2020-08/fema430.pdf

Federal Transit Administration (FTA), "The Public Transportation System Security and Emergency Preparedness Planning Guide," 2003.

FTA, "An Introduction to All-Hazards Preparedness for Transit Agencies," 2010. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/All_hazards.pdf

FTA, "Public Transportation System Security and Emergency Preparedness Planning Guide," 2003. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf

FTA, "Sensitive Security Information (SSI): Designation, Markings and Control, Resource Document for Transit Agencies," 2009.

FTA, "Traveler Information Systems and Wayfinding Technologies in Transit Systems," May 2011. https://www.transit.dot.gov/research-innovation/mmtps-final-evaluation-report

Mineta Transportation Institute, "Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation," Report 11-20, B.M. Jenkins and J. Trella, April 2012. https://transweb.sjsu.edu/research/Carnage-Interrupted-Analysis-Fifteen-Terrorist-Plots-against-Public-Surface-Transportation

National Transit Institute (NTI), Terrorist Activity Recognition and Reaction.

State Government of Victoria (Australia), Department of Transport, "Security Risk Assessment for Transit Operations," 2012.

Rand Corporation, "Homeland Security: Securing America's Passenger Rail," pg. 10–12, 2007.

Department of Homeland Security, Transportation Security Administration, "Sensitive Security Information Stakeholder Best Practices Quick Reference Guide."

Transportation Security Administration (TSA)/FTA, "Security and Emergency Management Action Items for Transit Agencies." https://www.hsdl.org/?view&did=773635

Transit Cooperative Research Program (TCRP), "Guidelines for Providing Access to Public Transportation Stations," TCRP Report 153, 2012. http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_rpt_153.pdf

Definitions

access control: An aspect of security that uses physical security equipment/technology entry control systems and specialized procedures to manage and monitor movement into, out of or within a specific protected area. Access to various areas may be limited by need to know, place, time or a combination of all.

clear zone: An area clear of visual obstructions and landscape material that could conceal a threat or perpetrators, for example the space immediately adjacent to and around an inhabited building without obstructions large enough to conceal explosives 6 in. or greater in height.

consequence: The level, duration and nature of loss from an unfavorable event.

Crime Prevention Through Environmental Design: A crime-prevention philosophy based on the theory that proper design and effective use of the built environment can lead to a reduction in the fear and incidence of stranger-on-stranger crime, as well as improve the quality of life.

delay: A measure to impede an adversary during an attempted entry or attack, or to slow the progress of security event so as to allow a response.

detect: The act of discovering a suspicious activity or an attempt (successful or unsuccessful) to breach a secured perimeter (such as scaling a fence, opening a locked window or entering an area without authorization).

deter: A measure to discourage or prevent a potential threat from occurring by instilling doubt that an attack is likely to be successful.

entry control: The control of people, vehicles and materials through entrances and exits of a protected area using equipment and/or technology that channels, restricts or controls entry to an area, space or location.

first responders: Local police, fire and emergency medical personnel who first arrive at the scene of an incident and take action to save lives, protect property and meet basic human needs.

layered defense: Cumulative successive obstacles that must be penetrated by an adversary to reach the intended target, thus providing additional warning and response time for security forces (aka defense in depth or layers of protection).

progressive collapse: The spread of an initial local failure from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it.

risk: The likelihood of the occurrence of an unfavorable event that leads to catastrophic losses (fatalities, injuries, damage or business interruption). The three factors of risk are threat, vulnerability, and consequence. Also described as $R = T \times V \times C$.

recovery: The ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption or security event.

resourcefulness: The ability to skillfully prepare for, respond to and manage a crisis or disruption as it unfolds.

resilience: The ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.

response: Employees, guards or law enforcement representatives who deploy to investigate a detected event to prevent or mitigate an attack or security event.

robustness: The ability to maintain critical operations and functions in the face of crisis.

standoff distance: The distance between an asset or building or portion thereof (target) and the potential location of an explosive device (threat).

target: An object, background or reflector at which something (i.e., a threat) is aimed.

threat: A natural or human-made occurrence that harms or indicates the potential to harm life, information, operations, the environment and/or property; or any indication, circumstance or event with the potential to cause loss of or damage to an asset.

transit domain awareness: The awareness and understanding of activities within or associated with the transit domain that could impact the security, safety, economy or environment of an agency. It is a key component of an active, layer-protected and balanced security program that is supported by other agency plans and activities.

ventilation: A system or means of circulating fresh air by natural or mechanical means.

vulnerability: A physical feature or operational attribute that renders a station or stop open to exploitation or susceptible to a given hazard or threat. Vulnerabilities may be associated with physical, cyber or human factors.

Abbreviations and acronyms

AASHTO	American Association of State Highway and Transportation Officials
ACS	access control system
CBR	chemical, biological or radiological
CCTV	closed-circuit television (see VSS)
CFR	Code of Federal Regulation
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security
ESS	electronic security system
FEMA	Federal Emergency Management Agency
FTA	Federal Transit Administration
HVAC	heating, ventilation and air conditioning
HVM	hostile vehicle mitigation
IDS	intrusion detection system
IED	improvised explosive device
IID	improvised incendiary device
P3	plans, policies and procedures
PtD	Prevention through Design
SSI	Sensitive Security Information

TSA Transportation Security Administration
VBIED vehicle-borne improvised explosive device
VSS video surveillance system

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Oct. 18, 2021	Jan. 7, 2022	Jan. 24, 2022	June 3, 2022	May 23, 2023
First revision	—	—	—	—	—

Appendix A: Vulnerabilities

Potential vulnerabilities of stations and stops that should be considered are described in the following sections:

Site location

Passenger stations that share infrastructure or systems have potential for both physical and procedural vulnerabilities that should be identified and addressed. These include the following:

- **Proximity to other structures.** Stations with minimal separation or that are connected to adjacent buildings need to consider both the function and physical security of the proximate facilities. The adjacency can add to the vulnerabilities of the station, especially if there are shared facilities such as loading docks or utilities. The risk assessment should consider adjacent facilities in the analysis.
- **Parking areas.** Adjacent parking to a station reduces standoff distance and may limit the structure's resilience to blast. They also can provide locations for staging of threat activity.
- **Standoff distance.** Vehicle access to non-public or restricted areas of a passenger station may allow threats to be introduced to the station structure. These include the proximity of kiss-and-ride drop-off zones, taxi stands or other noncontrolled vehicle access.
- **Lighting.** Insufficient lighting may inhibit natural or mechanical surveillance and attract unwanted activities at a station or stop. Insufficient lighting also contributes to the perception that the stop or station may be unsafe.
- **Station or stop orientation.** Where a station or stop is located may interfere or limit the application of security controls or mitigations.
- **Vegetation or landscaping.** Overgrown vegetation, shrubs, and tree canopies may inhibit natural and mechanical surveillance and can also contribute to low lighting, shadows and a feeling of vulnerability.
- **Vehicle interface.** Direct vehicle approach paths can provide for direct collision of a threat vehicle with the stop or station.
- **Access and egress.** Access and egress to enclosed stations must balance the emergency evacuation needs with the need to balance threat access to the station.

Structural and architectural

Some structural and architectural designs lead to an increased risk to occupants and should be evaluated as part of the security assessment. These include the following:

- **Structural design.** Older stations may not be designed, built or retrofitted to withstand progressive collapse caused by an explosion or may not enable occupants to evacuate the structure. Bus shelters may also be vulnerable to vandalism or sabotage that could lead to the shelter's collapse and passenger injury.
- **Stairwells, stairways, loading docks.** External building stairs and loading docks may offer access to the station and its critical infrastructure.
- **Access control.** Uncontrolled or unrestricted access to non-public, restricted areas of stations may allow for sabotage, vandalism, vagrancy or other criminal activities.
- **Proximity of ancillary equipment.** Trash equipment, fuel tanks or other such equipment positioned adjacent to the station may provide for unauthorized entry.
- **Pinch points.** Station entrances and exits, fare gates, internal concourses and hallways funnel people into close proximity, which can make them vulnerable to attack.
- **Building materials and furnishings.** Enclosed stations may incorporate materials or furnishings that can contribute to injury and death by fragmenting, falling or becoming airborne in an explosion.

- **Deliveries.** Packages, envelopes and other vendor shipments delivered to a station may contain potentially hazardous material.
- **Trash and recycling receptacles, newspaper/magazine stands, and vending machines.** These could be used to hide harmful devices.

Utilities and communication systems

These systems may be themselves vulnerable or introduce vulnerabilities into the station. These include the following:

- **Crawl spaces, utility tunnels, pipelines, conduit banks, etc.** Building services openings or conduits may provide vulnerability for unauthorized access to internal areas of stations.
- **HVAC.** Access to HVAC intakes may allow the introduction of toxic substances into the station.

Plans, policies and procedures

Plans, policies and procedures (P3) or the lack thereof, may introduce vulnerabilities to a station or stop. Examples of potential procedural vulnerabilities are listed below:

- **Sensitive building information.** The disclosure of security plans, procedures or operations; building vulnerabilities; or critical infrastructure information may increase a passenger station's security risk. This could come from a casual view, an overheard conversation, an internet posting or a social media site.
- **Tenants.** Businesses that lease space from owners/operators may be an adversary's target. The targeting of a lease tenant could result in collateral damage to the building it occupies or injure its occupants. Additionally, lease tenants who are unaware of or do not abide by passenger station security P3 may unintentionally introduce threats and increase risk to facilities.
- **Unoccupied areas.** Infrequent or unoccupied visited spaces such as storage areas or tenant spaces may introduce risks.
- **Security and emergency planning.** Outdated or nonexistent P3 expose passenger stations to increase vulnerability in their ability to respond appropriately to or recover from an attack.

Cyber

Information technology systems operate core building networks, systems and functions. These systems are vulnerable to insider, covert and other forms of attacks. Information technology risks should be continually monitored and evaluated for vulnerabilities. Unprotected IT systems and networks may expose operations and communication systems to a range of adversarial attacks against a system.

Other

Passenger stations lacking regular general housekeeping, proper maintenance and timely repairs imply unsafe conditions and an unsecure environment for passenger station operations, infrastructure and the people served—inviting crime. Good housekeeping should be continually monitored and evaluated for risk.

Appendix B: Mitigations

Table 6 summarizes some mitigation measures transit agencies can use to strengthen the safety and security of passengers and assets at stations and stops.

TABLE 6
Summary of Mitigation Measures for Transit Stations and Stops

Measure	Description
Access control system (ACS)	• Install at the entry point of a protected/restricted area to control access to space or area. • Incorporate access control (hardware) systems and specialized procedures to manage and monitor movement into, out of or within a specific protected area. e.g., entering and/or departing passenger stations. • Include policies and procedures to identify system processes and training, as well as system operations and maintenance requirements. • ACS should augment physical security equipment/technology entry control and operational measures.
Anti-vehicle barrier (AVB)	• Use to obstruct and prevent the movement of vehicles within a specific protected area, such as entering and/or departing passenger station portals. Examples of AVBs include Jersey-style concrete barriers, bollards, mobile barrier devices, etc. • Incorporate policies and procedures to identify system processes, training, and operations and maintenance requirements. • See APTA recommended practice “Anti-Vehicle Barriers for Public Transit” (APTA SS-SIS-RP-009-12).
Barriers	• Use to restrict trespass, control entry and identify boundaries. • Install barriers along perimeter boundaries to prohibit trespass and/or control entry to a passenger station’s critical infrastructure. Barriers may include fencing and gates, doors, panels, etc. • Float maritime barriers or submersed interwoven metal cable to form subsurface protective barricade in the form of a net. • See “Fencing Systems to Control Access to Transit Facilities” (APTA SS-SIS-RP-003-10), “Chain-Link, Mesh or Woven Metal Fencing Systems to Control Access” (APTA-SS-IS-RP-0004-10), “Gates to Control Access to Revenue and Nonrevenue Transit Facilities” (APTA-SS-IS-RP-0005-10); and “Ornamental Fencing Systems to Control Access to Transit Facilities” (APTA-SS-IS-RP-006-10).
Bracing support	• Use support bracing or braided wire securely fastened to the structure to prevent mounted utilities, fixtures and ceiling or other overhead features from falling or becoming a missile hazard during a blast or seismic event. • Follow the appropriate standards and codes of the authority having jurisdiction.
Clear zone	• Designate the area adjacent to and near the building that is clear of visual obstructions and landscape material that could conceal a threat or adversary, e.g., an area that would not obstruct the view of or allow an object to be concealed. • See APTA recommended practice “Physical Security for Public Transit” (APTA SS-SIS-RP-013-13).
Crime Prevention Through Environmental Design (CPTED)	• Incorporate the principles of natural, mechanical and organizational concepts to implement access control, surveillance and territoriality into transit designs at passenger stations and stops. • Include sustained activity support and planned maintenance to enhance the sense of safety and security. • See “Crime Prevention Through Environmental Design for Transit Facilities” (APTA SS-SIS-RP-007-10) and “Bus Stop Design and Placement Security Considerations” (APTA SS-SIS-RP-008-10).

TABLE 6

Summary of Mitigation Measures for Transit Stations and Stops

Measure	Description
Designated zones	• Use to prevent public access to restricted areas (designated zones). • Encourages openness and unrestricted passage to areas (designated zones) where the traveling public is authorized. • Incorporate with appropriate signage. • See “Security Program Considerations for Public Transit” (APTA SS-SIS-S-010-13).
Electronic security systems (ESS)	• See “Access control systems” above. Integrate ACS with IDS and VSS to enable complete assessment. • Use intrusion detection systems to detect intrusion into a protected or restricted area. Position sensors as far as possible from tunnel infrastructure being protected to allow for maximum response time. Integrate IDS with ACS and VSS to enable complete assessment of alarm. • Include maritime fiber-optic intrusion detection cable interwoven into a submersed and interwoven metal cable forming a subsurface protective barricade. Connect cabling to a central control center were intrusion can be assessed and a response can be dispatched. • Use video surveillance systems to assess—and record where capable—the areas of an activated IDS or ACS. • Coordinate VSS requirements with lighting. Integrate VSS with ACS and IDS to enable complete assessment. • Use heat/water sensors to detect the presence of heat/water and assess water levels in operational spaces, ancillary rooms and other critical assets. • Integrate with VSS and IDS to assess critical asset areas.
Emergency egress	• Use to aid evacuation of a space/building/facility or as an entry point for first responders. • Where required by fire and/or building code install emergency egress stairways. • Include appropriate signage and wayfinding; provide emergency lighting and communications to and within egress area; over-pressurize and separately vent the vestibule area; and implement ESS to monitor.
Emergency power	• Provide backup power to critical passenger station systems. • Where required by applicable code or the authority having jurisdiction, design and install emergency power to critical passenger station systems.
Emergency telephone	• Use to communicate emergency information from one location to another, e.g., station platform to Security or Operations Control Center. • Design and install as wall pack unit or as a standalone pedestal. • Options include video camera, microphone/speaker, blue light, and (short-term) solar power or battery backup. • See “Equipment and Technology for Public Transit” (APTA SS-SIS-RP-15-13).
Entry control	• Use to control entry into, out of, or within a specific protected area, such as entering and/or departing passenger stations. • Incorporates barriers, lighting, fencing, policies and procedures, etc., as well as electronic security systems (see “Electronic security systems” above) to augment management of people and vehicles within a specific protected area, e.g., entering and/or departing passenger stations. • Design entry control measures to augment access control policies and procedures.
Fire detection systems	• Use to detect smoke, sense heat, and then report the event(s) to an operations, command or communications center. • Check local building and fire codes with the authority having jurisdiction to determine if and what type(s) of detection systems are required based on structure type, length, etc. • Where permitted by code, fully integrate fire detection, fire suppression and ventilation control systems.

TABLE 6

Summary of Mitigation Measures for Transit Stations and Stops

Measure	Description
Fire suppression systems	• Use to suppress or deluge smoke and/or fire event. • Include systems that disperse water to deluge or an agent to extinguish fire; stand pipe connections to pump water/agent to the event site. • Design and install where permitted by building and/or fire code, integrate fire detection, fire suppression and ventilation controls systems.
Layered protection	• Provide a succession of ever more challenging obstacles that an adversary must overcome while approaching the target. • Layers are governed by the physical boundaries of the property. For example, the first layer of protection consists of barriers positioned at the property line or sidewalk. The second layer extends from the perimeter of the site inward to the exterior face of the passenger station building. This layer provides a building with standoff distance from vehicle threats. The third layer consists of interior building areas. • For structures without standoff distance, begin the first layer of defense at the structure's façade with continuing layers designated within the structure. • See " Security Program Considerations for Public Transit" (APTA SS-SIS-S-010-13) and "Equipment and Technology for Public Transit" (APTA SS-SIS-RP-15-13).
Patrols	• Assign static, direct and random patrols of property and for responce to calls for service. • Arrange and use mutual aid agreements with authority having jurisdiction to dispatch patrols upon request.
Policies and procedures	• Use to guide daily nonemergency operations of the structure and for responses to emergency operations. • Should include concept of operations, event-specific response(s), training, maintenance, and all-hazard responses, e.g., National Terrorism Advisory System (NTAS), Security and Emergency Actions List for Transit Agencies, etc. • See "Security Planning for Public Transit" (APTA SS-SIS-RP-011-13).
Progressive collapse	• Conduct a progressive collapse study to evaluate the durability and survivability of a structure or its critical components. • Design and implement structural hardening measures to reinforce structural integrity of buildings as required. • Evaluate mitigation measures to reduce the risk of progressive collapse before structural hardening is implemented.
Security and emergency lighting	• Provide artificial lighting to non-lighted areas; considered a deterrent. • Implement continuous, standby or mobile lighting as operations require; consider energy-efficient lighting sources; coordinate lighting with VSS. • Integrate with motion sensor technologies to turn on when activated, and install with timing clocks or photocell sensors to operate only during specific hours. • Illumination at entries may be necessary to ease transition from lighted to increasingly dark areas when entering and/or departing an area, space or location. • As required by the authority having jurisdiction, install approved emergency lighting type(s) approved for use by an agency. • See "Security Lighting for Revenue Transit Passenger Facilities" (APTA SS-SIS-RP-001-10) and "Security Lighting for Non-Revenue Transit Passenger Facilities" (APTA SS-SIS-RP-002-10).
Sensitive Security Information (SSI)	• Designate, mark, store and dispose of documents, plans, drawings, etc., with the SSI header and footer if it is determined that they contain or list information about any of the following: security programs, vulnerability assessments, contingency plans or threat information held by the federal government, and other information as determined in writing by the Transportation Security Administration administrator. See 49 CFR, Parts 15 and 1520. • Follow federal, state or agency regulations where applicable.

TABLE 6

Summary of Mitigation Measures for Transit Stations and Stops

Measure	Description
Signals and communications	• Used to send/receive messages, information, data or other communications into, within, or from a passenger station. • Hardware medium may include antenna, cable, fiber or other wireless device(s).
Signage	• Informs, provides notice or gives warning. • Post signage at appropriate locations to identify property boundaries and inform potential adversaries about trespass prohibitions, surveillance activities, and the fact that other measures may be in place. • Anchor buoys or other floating devices to signal maritime traffic of restricted waterway area. • Coordinate signage with wayfinding.
Standoff distance	• Reduce blast overpressures and damage. • Time and distance reduces blast overpressure. The farther the threat is from the target, the lower the blast overpressure should be when reaching it. • See “Physical Security for Public Transit” (APTA SS-SIS-RP-013-13).
Trash receptacles	• Position trash and recycling receptacles away from platforms and other places where people gather. If required for a platform, use a blast-resistant receptacle. Analyze placement location to avoid overhead beams, structures or fixtures. • See “Trash and Recycling Receptacles for Transit Facilities” (APTA SS-SIS-WP-014-13).
Walkways	• Guide circulation of people through passenger stations to their destinations. • Design and install where required by building and/or fire code. Apply Americans for Disability Act requirements where mandated by law. • See “Crime Prevention Through Environmental Design for Transit Facilities” (APTA SS-SIS-RP-007-10) and “Bus Stop Design and Placement Security Considerations” (APTA SS-SIS-RP-008-10).