APTA STANDARDS DEVELOPMENT PROGRAM
APTA STANDARD
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-SIS-S-010-13
Approved March 26, 2013
Infrastructure Security Working Group

Security Program Considerations for Public Transit

Abstract: This *APTA Standard* proposes security program consideration practices for transit passenger facilities to enhance the security of people, operations, assets and infrastructure.

Keywords: assessment, balanced security, blast, clear zone, considerations, design considerations, layers of protection, security program, site survey, standoff distance,

Summary: This *APTA Standard* provides basic security program considerations strategy background information. It offers an overview and descriptions of the applicability of the four pillars of security. It also includes discussions about: basic security principles, designation of zones, and layers of protection and how they may be integrated with other security standards and best practices used by transit agencies to enhance their security program(s).

Scope and purpose: This *APTA Standard* is the lead document in a series of infrastructure security *Recommended Practices* and white paper documents prepared for use by the transit industry. Other infrastructure security specific program topics developed for this series will address components of the four pillars of security—planning, operations, physical security, and equipment and technology—that will also be provided to the transit industry for consideration and use.

This *Standard* represents a common viewpoint of those parties concerned with its provisions, namely, transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any standards, practices or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of a transit system's operations. In those cases, the government regulations take precedence over this standard. APTA recognizes that for certain applications, the standards or practices, as implemented by individual transit agencies, may be either more or less restrictive than those given in this document.

APTA Standards
Development Program
Lead the Way

Participants

The American Public Transportation Association greatly appreciates the contributions of **Bill Pitard**, who provided the primary effort in the drafting of this *Standard*.

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

Sean Ryan, MNR, *Chair*
Randy Clarke, MBTA, *Vice Chair*

Bill Pitard, STV, Inc.
Gabriela Amezcua, *CTA*
John Plante, *CTA*
Brian Taylor, *Halifax*
Charles Rappleyea, *CATS*
Rick Gerhart, *FTA*
Chris McKay, *TSA*
Jevon D'Souza, *TSA*
David Hahn, *APTA*
Allen Smith, *SPAWAR*
Mark Mahaffey, *VTA*
Brad Baker, *MBTA*
Eric Hartman, *OCTA*
Harry Saporta, *TriMet*
Melanie Maxwell, *Parsons Brinckerhoff*
Gardner Tabon, *RPTA*

Ken Cummins, Sound Transit
Robert Barrow, NYC Transit

Contents

Security Program Considerations for Public Transit

1. Introduction

Public transit operates in inherently open environments. It provides ease of access and gathers volumes of people in confined spaces to provide passengers with efficient and convenient transportation through regions and their communities. These unique attributes make public transportation vulnerable to adversarial targeting and risks. For these reasons, a sound understanding of security program considerations and implementation of transit domain awareness (TDA) are necessary to assist agencies to implement approaches to effectively manage the risks of their environments.

While transit security programs may be implemented or operated using different types of strategies, measures or solutions, a "Security 101" philosophy of a basic level of appropriate strategies should be understood to reduce risk and enhance the posture of all transit properties.

This Recommended Practice is part of a series of related RP's. Several Recommended Practice documents were organized into series that link together related security information and topics. In each series of documents, a lead document establishes the general topic for series followed by other related document(s). For example, there are five documents in the RP's series titled "Security Considerations." The RP "Security Program Considerations" is the lead document in the series followed by "Security Operations," Security Planning," Physical Security," and Equipment and Technology" documents.

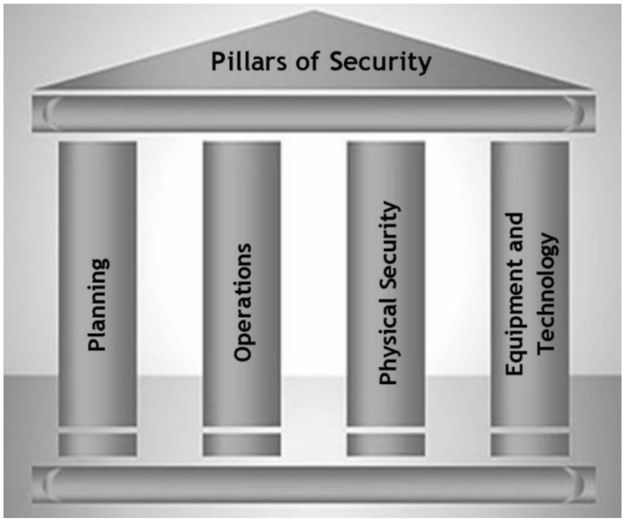
Additionally, other document series prepared for transit agencies to use within their security program include: four RP's about fencing and gates and two RP's concerning "security lighting." See "References" below for links to APTA Security Standards Document series.

2. Security program considerations overview

This is the lead document that organizes security program consideration derivative topics into four basic security pillars (**Figure 1**). Each pillar is structured to identify security program considerations and strategies that when used alone or interconnected are crucial to the mitigation of risks to transit assets. The pillars that should be considered are physical security, operations, planning, and equipment and technology, which are described below. To attain a balanced approach to security, no pillar should stand alone. Collectively, they exist by incorporating several components of the four pillars together into a system that provides a uniform approach to application of a security solution. When effectively applied, these components provide an agency with guidance or direction to mitigate risk and operate a balanced and effective security program.

FIGURE 1

Pillars of Security



Examples of similarly structured *Recommended Practice* documents that describe a broad scope of infrastructure security and derivative topics are described in **Table 1**. Other Security Standards Program documents from the Security Risk Management, Emergency Management, Enterprise Cyber Security, and Control and Communications Cyber Security working groups are also listed as resources to aid in the development of a balanced security program. They should be used where applicable by accessing www.aptastandards.com/Documents/PublishedStandards/Security/tabid/329/language/en-US/Default.aspx.

TABLE 1

APTA Infrastructure Security Standards Program Documents

APTA Number	Document Title
APTA SS-SIS-RP-001-10	"Security Lighting for Transit Passenger Facilities"
APTA SS-SIS-RP-002-10	"Security Lighting for Nonrevenue 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 to Transit Facilities"
APTA SS-SIS-RP-005-10	"Gates to Control Access to Transit Facilities"
APTA SS-SIS-RP-006-10	"Ornamental Fencing Systems to Control Access to Transit Facilities"
APTA SS-SIS-RP-007-10	"Crime Prevention Through Environmental Design for Transit Facilities"
APTA SS-SIS-RP-008-10	"Bus Stops Design and Placement Security Considerations"
APTA SS-SIS-RP-009-12	"Anti-Vehicle Barriers for Public Transit"

2.1 Stakeholder considerations

Transit agency understanding and buy-in to security program considerations are imperative to their continual evolution within the environments where they must operate. To the extent possible, the application of any or all of the topics of this document will assist agencies to improve their security program requirements and enhance their safe operations.

2.2 Benefits

A security program that includes security program considerations provides an agency's people, operations, assets and infrastructure the following benefits:

- Fosters a sense of security awareness.
- Creates pride of ownership by transit users and employees.
- Manages area access for authorized users.
- Controls access to non-public areas.

3. Security risk assessment

Transit agencies should complete a systemwide security risk assessment to determine exposure to their systems' people, assets, operations and infrastructure. A risk-based approach that factors threat, vulnerability and consequence should be used to assess transit systems.

> **NOTE:** Department of Homeland Security (DHS), National Infrastructure Protection Plan. Risk Methodology Factors. R(f) = T × R × C. www.dhs.gov/nipp.

The findings should be used to select security measures that mitigate risk to and enhance the protection of people, assets, operations and infrastructure. For more information regarding various security risk assessment methodologies, see:

- National Infrastructure Protection Plan (Department of Homeland Security [DHS])
- FEMA 452 - Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks (Federal Emergency Management Agency [FEMA])
- A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (American Association of State Highway and Transportation Officials [AASHTO])
- Public Transportation System Security and Emergency Preparedness Planning Guide (Federal Transit Administration [FTA])
- Security Vulnerability Assessment Methodology for Petroleum and Petrochemical Industries, (National Petrochemical & Refiners Association [NPRA])
- *Risk Analysis and Security Countermeasure Selection*, by T. L. Norman (CRC Press, Boca Raton, FL, 2010)

4. Security program considerations

4.1 Pillars of security

Security is dynamic and complex in the transit environment. Where requirements, standards, policies, practices and other important details may become overwhelming, it may be valuable for transit agencies to periodically relate tasking back to four essential pillars of security—planning, operations, physical security, and equipment and technologies—to maintain a persistent effort and focused approach to their security program. Security pillars could be implemented as standalone elements of a security program or combined with other pillars to provide an integrated and balanced approach to mitigating risk. Possible applications with examples of each security pillar are described below.

4.1.1 Planning

The planning pillar identifies processes for developing proactive and reactive plans to respond to potential events or incidents. Where the findings of a security risk assessment will identify risks and vulnerabilities to a system, they may also guide an agency to develop effective response plans and coordinate activities among stakeholders and their local, state, tribal and federal partners. These could include emergency plans, continuity of operations plans (COOPs) and Security and Emergency Preparedness Plans (SEPPs).

Also, through the design process, a crime prevention through environmental design (CPTED) survey can identify exposures and potential solutions to improving the operator's and ridership's perception of security of the built-environment. Visit APTAStandards.com to access the *Recommended Practices* and various plans, which include the COOP, SEPP and CPTED.

4.1.2 Operations

The operations pillar may provide signage and wayfinding guidance, as well as providing written guidance to staff and employees that delineates specific security program information and functions. Such guidance may include protocols or policies for agency staff and employees to take during certain events or incidents; staffing requirements, and identification of posts or positions that should be filled; a description of the contents of an agency's security awareness training program; and guidance for implementing security outreach for operator and ridership transit domain awareness.

4.1.3 Physical security

The elements of the physical security pillar are often a tangle of features. They include fencing and gates, lighting, lock and key control, anti-vehicle barriers, exterior doors, industrial doors, windows, HVAC, mailrooms, utility openings and other culverts, perimeter roads, and other active or passive systems that help to manage entry to an agency's properties.

4.1.4 Equipment and technology

This pillar involves the basic elements of equipment and technology solutions to reduce risk. For example, hardware (automated gates, electronic security systems [ESS) inclusive of: video surveillance systems (VSS) (formerly known as: closed circuit television systems (CCTV)), access control systems (ACS), intrusion detection system (IDS)), servers, LAN, WAN, etc.) and software applications to manage authorized access to specific areas, while deterring, detecting, delaying, and responding to unauthorized access to an agency's property. These elements should be coupled with other domain awareness equipment and technology to provide pinpoint or wide area surveillance and to integrate with systems that communicate internally to staff and employees and externally to first responders, operators and the ridership. This pillar also includes features designed to protect these management systems from intrusion, hacking or access denial (cited).

4.2 Basic security principles

Any application of security for transit agencies must include the basic security principles of deter, detect, delay and response to enhance the protection of people, assets, operations and facilities, thereby reducing risk (**Figure 2**). The development and implementation of these principles lead to layers of protection, coupled with designated zones that provide controls and obstacles that an adversary must overcome to gain access. Thus, the more critical the asset, operation or facility, the more complex and integrated the basic security principles, coupled with layers of protection, must be. The findings of an agency's security risk assessment will guide the implementation of the basic security principles.

FIGURE 2
Basic Security Principles

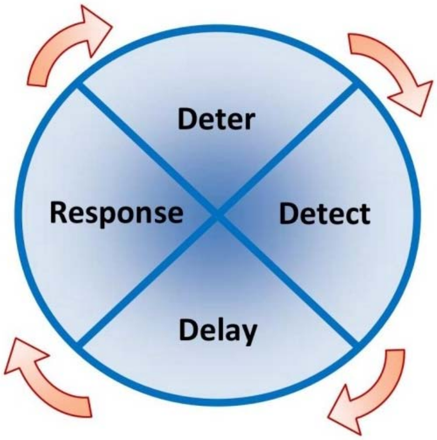
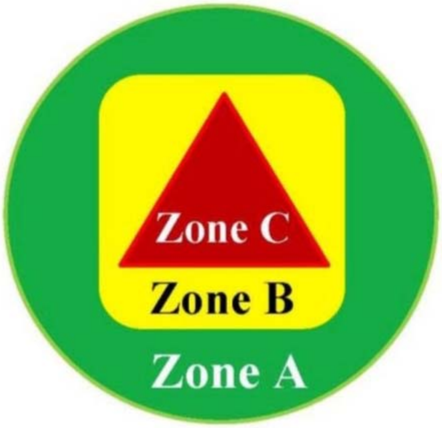


FIGURE 3
Designation of Zones



4.3 Designation of zones

The designation of zones encourages openness and unrestricted passage to areas (zones) where the traveling public is authorized, while preventing public access to restricted areas (zones). It is also used to control areas that require layers of protection depending on the nature, sensitivity or importance of the security interest. Beginning with identification of the outermost perimeter area, and then by determining other additional interior areas requiring greater protection, zones are identified, designated and established. There are no limits to the number of zones that may be designated. Multiple zones serve the purpose of deter and delay by discouraging or controlling penetration and slowing the path of travel to a target. The designation of zones also provides response forces time to deploy to the site to investigate and/or interdict.

Each zone should be identified by a separate designator (e.g., Zone A, Zone B, or Zone 1, Zone 2, etc.) and have security measures designed in layers that would deter, detect and/or delay an adversary's ability to penetrate from one zone into another zone or zones.

Figure 3 illustrates three designated zones of protection. While the shapes are only for illustrative purposes, Zone A shows an outermost (exterior) zone, while Zone B encompasses the middle zone, and Zone C includes the innermost (interior) zone. Under this concept, an adversary would encounter and be required to overcome an increasingly difficult series of security measures and subsystems in order to move from Zone A through Zone B and into Zone C. **Table 2** describes examples of people, operations, assets and infrastructure that may be located within the designated zones.

4.3.1 Guidance for designation of areas

Typically, the most critical people, assets, operations and facilities are surrounded by the most layers of protection. As general guidance for maximum effectiveness:

- People, operations, assets and infrastructure within Zone C should be surrounded or buffered by Zone B or Zone A.
- People, operations, assets and infrastructure within Zone B should be surrounded or buffered by Zone A.
- People, operations, assets and infrastructure within Zone A may not require being surrounded or buffered by another zone but should be afforded the protection of the Zone A boundary.

- Refrain from designating and placing Zone A people, operations, assets and infrastructure within Zone B or Zone C.
- Refrain from designating and placing Zone A or Zone B people, operations, assets and infrastructure within Zone C.

TABLE 2
Examples of Facilities or Assets with Designated Zones

Zone A	Zone B	Zone C
• Public access areas • Lobby and retail space • Parking lots • Restrooms • Pedestrian concourses • Administrative areas	• Fire systems • Electrical vaults • Water services • Other utility services • HVAC systems	• Operations center • Control center • Emergency power system • Emergency power fuel • Mail room/center

4.4 Layers of protection

To provide a layered protection approach to people, operations, assets and infrastructure, designated zones, coupled with the basic principles of security, should be established. This means that for authorized users, designate each zone with layers of protection using at least basic security principles to require an individual to overcome every additional challenge until the intended authorized zone (location) is reached. For example, access control badge, doors, alarms, etc. For adversaries, however, each designated zone would be designed with layers of protection, using basic security principles that require additional and more challenging efforts to overcome. When security measures are applied in unison with other measures, the combination of measures offers some increased level of protection for people, operations, assets and infrastructure. Security measures associated with a specific basic security principle or principles are described in **Table 3**.

TABLE 3
Security Measures Associated with Basic Security Principles

	Policies and Procedures	Barriers	ID Checks	Standoff Distance
Deter	Posted signs	Surveillance systems	Inspections/screening	Clear zone
	Fencing	Escorts	Employee awareness	Lighting
	Landscape	Uniformed personnel	Area designation	
Detect	Sensors	Emergency phones	Data collection and intelligence	Lighting
	Monitors and alarms	Explosive detection	Employee awareness	Intrusion detection
	Law enforcement	Area designation	Panic alarms	Contract security
	Clear zone	Surveillance monitoring		
Delay	Bolts, fasteners	Fencing	Public announcement systems	Standoff distance
	Flush surfaces	Barriers	Employee awareness	Access controls
	Alarms	Area designation		

TABLE 3
Security Measures Associated with Basic Security Principles

Response	Law enforcement	Contract security	Employee	

5. Training considerations

There are no specific training elements associated with the information contained in this document. However, the cited references provide information about the elements contained herein. Specific training considerations will be addressed where applicable in derivative series documents.

6. Maintenance considerations

There are no specific maintenance requirements associated with this document. However, where maintenance is applicable to an *APTA Standard, Recommended Practice*, or other document, it will be addressed in derivative series or other documents.

References

American Association of State Highway and Transportation Officials (AASHTO), "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection." http://highwaytransport.transportation.org/Documents/NCHRP_B.pdf

American Public Transportation Association (APTA), "Securing Control and Communications Systems in Transit Environments Part 1." www.aptastandards.com/Documents/PublishedStandards/Security/tabid/329/language/en-US/Default.aspx

ASIS International, "International Glossary of Security Terms." www.asisonline.org/library/glossary/index.xml

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

DHS, National Infrastructure Protection Plan. www.dhs.gov/nipp

Federal Emergency Management Agency (FEMA), FEMA 452 - Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks.www.fema.gov/plan/prevent/rms/rmsp452.shtm

Federal Transit Administration (FTA), "An Introduction to All-Hazards Preparedness for Transit Agencies," (2010). http://www.fta.dot.gov/documents/SMPM_Instruction_Manual.pdf

FTA, "Public Transportation System Security and Emergency Preparedness Planning Guide" (2003). http://transit-safety.volpe.dot.gov/publications/security/PlanningGuide.pdf

FTA, Office of Research Demonstration and Innovation, "Transit Security Design Considerations," November 2004. www.cedengineering.com/upload/Transit%20Infrastructure%20Security.pdf

National Petrochemical & Refiners Association (NPRA), "Security Vulnerability Assessment Methodology for Petroleum and Petrochemical Industries, 2nd Ed." www.npra.org/docs/publications/newsletters/sva_2nd_edition.pdf

Norman, Thomas L., CPP, PSP, CSC, *Integrated Security System Design: Concepts, Design, and Implementation* (Butterworth-Heinemann, Burlington, MA, 2007).

Norman, Thomas L., CPP, PSP, CSC, *Risk Analysis and Security Countermeasure Selection,* (CRC Press, Boca Raton, FL, 2010).

Definitions

delay: To impede penetration into a protected area.

detect: The act of discovering 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: To make a target inaccessible or difficult to defeat through the use of small hand tools (e.g., hammer, drills, electric power tools, etc.) or by using a specific tactic to bypass a security system.

response: Employees, guards or law enforcement representatives who deploy to investigate a detection event or interdict an intruder or trespasser.

security risk assessment: A formal, methodical process used to evaluate risk (both terrorism and crime) to a transit system.

transit domain awareness (TDA): 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.

Abbreviations and acronyms

AASHTO	American Association of State Highway and Transportation Officials
ACS	access control system
APTA	American Public Transportation Association
CCTV	closed-circuit television system
COOP	continuity of operations
CPTED	crime prevention through environmental design
ESS	electronic security systems
FTA	Federal Transit Administration
HVAC	heating, ventilation, and air conditioning
IDS	intrusion detection system
LAN	local area network
NPRA	National Petrochemical & Refiners Association
SEPP	Security and Emergency Preparedness Plan
TDA	transit domain awareness
WAN	wide area network