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

APTA SS-SIS-RP-013-13
Approved March 26, 2013
Infrastructure Security Working Group

Physical Security for Public Transit

Abstract: This *Recommended Practice* proposes physical security practices for transit passenger facilities to enhance the security of people, operations, assets and infrastructure.

Keywords: anti-vehicle barriers; ballistic; blast; culverts; doors; fencing; glass; heating, ventilation, and air conditioning (HVAC); hinges; key and lock control; lighting; mailroom; perimeter roads; physical security; risk assessment; security; windows

Summary: This *Recommended Practice* provides basic physical security strategy background information. It offers an overview and descriptions of the applicability of the physical security pillar. Elements of this pillar often include target-hardening elements such as security lighting, fencing and gates, security risk, exterior doors, industrial doors, windows and glazing, HVAC, mail rooms, utility openings and culverts, perimeter roads, lock and key control, standoff distance, and clear zones. The elements of this pillar may be integrated with other security standards and best practices used by transit agencies to enhance their security program(s).

Scope and purpose: This *Recommended Practice* is a derivative document of the security program considerations series of infrastructure security recommended practices and other documents prepared for transit passenger facilities. Other infrastructure security specific program topics developed for this series will address the remaining components of the four pillars of security—planning, operations, equipment and technology—and will also be provided to the transit industry for consideration and use.

Participants

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

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

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

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

Contents

1. Introduction 1

2. Physical security pillar overview 2
2.1 Stakeholder considerations 2
2.2 Benefits 2
2.3 Applicability 3

3. Security risk assessment 3

4. Physical security 3
4.1 Security lighting series 3
4.2 Fencing and gate series 3
4.3 Exterior doors 3
4.4 Industrial doors 5
4.5 Windows 6
4.6 HVAC control systems 7
4.7 Mail facility 8
4.8 Utility openings 8
4.9 Perimeter roads 9
4.10 Key and lock control 9
4.11 Distances 10

5. Training considerations 10

6. Maintenance considerations 10

References 11

Definitions 12

Abbreviations and acronyms 12

Physical Security 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 threats. For these reasons, a sound understanding of the elements of the physical security pillar is necessary to assist agencies to implement approaches to effectively manage the risks of their environments.

While transit security programs may implement or operate using different types of strategies, measures or solutions, a "Security 101" philosophy or a basic level of appropriate strategies should be understood to reduce risk and enhance the posture of all transit properties. The "Security Program Considerations" series of infrastructure security *Recommended Practices* (RP) prepared for transit passenger facilities provide such information (see **Table 1**).

This Recommended Practice is part of a series of related RP's. Several Recommended Practice documents were organized into series that link together related infrastructure 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.

TABLE 1
APTA 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-001-12	"Anti-Vehicle Barriers for Public Transit"
APTA SS-SIS-RP-XX-12	"Security Program Considerations for Public Transit"

TABLE 1
APTA Security Standards Program Documents

APTA Number	Document Title
APTA SEM-SS-RP-008-09	"Safe Mail and Package Handling"

2. Physical security pillar overview

Adversaries target people, operations, assets and/or infrastructure in the transit environment. To reduce the risk from these threats, the efficient design and effective placement of physical security elements should be considered.

The physical security pillar elements are not stand-alone programs. They exist by incorporating some or all elements of any one or several pillars together into a system that provides a uniform approach to applying a security solution. When effectively applied, these elements provide an agency with guidance or direction to mitigate risk and operate a balanced and effective security program. The physical security measures described herein are categorized as either "assets that should be protected" or assets that protect" and are listed accordingly in **Table 2**.

TABLE 2
Categorizing Transit Assets

Assets That Should Be Protected	Assets That Provide Protection
Glass and windows HVAC	Security lighting Fencing and gates Exterior, ballistic rated and industrial doors Mail facilities Utility openings Perimeter roads Key and lock control Standoff distance Clear zone

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 are also listed as resources herein to aid the development of a balanced security program and should be used where applicable by accessing APTA's Security Standards and Recommended Practices page at www.aptastandards.com/Documents/PublishedStandards/Security/tabid/329/language/en-US/Default.aspx.

2.1 Stakeholder considerations

As one component of a comprehensive security program, the physical security pillar must be fully understood by Transit Agencies before being implemented. The functionality of elements within this pillar will be determined by the agencies security risk assessment. To the extent that it is possible, transit agencies should consider implementing all elements of this recommended practice.

2.2 Benefits

An agency's security program that includes physical security provides its people, operations, assets and infrastructure the following benefits:

- Manages access to authorized areas

- Controls access to non-public areas
- Fosters a sense of physical security
- Creates a sense of ownership by transit users and employees
- Enhances the safety and security experience of its ridership within the transit environment

2.3 Applicability

While used to protect people, operations, assets and/or infrastructure from risk, the measures described herein are neither exhaustive nor mandatory. However, they do provide a transit agency several options or alternatives for their application based on the level of risk determined by various factors. For example, security risk assessment or survey results, municipal codes or ordinances, the environment and man-made or natural hazards, regulatory constraints and or requirements, resources, capabilities, etc., must all be investigated to identify their appropriate applicability to reducing the risk environment.

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. 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. Physical security

4.1 Security lighting series

This *Recommended Practice* series provides guidance on "Security Lighting for Transit Facilities" and "Security Lighting for Non-Revenue Transit Facilities." See APTA Recommended Practices (**Table 1**).

4.2 Fencing and gate series

This *Recommended Practice* series provides guidance on Fencing Systems, Chain Link, Mesh, or Woven Metal Fencing System, and Gate Systems. It does not include virtual or other technology-driven fencing systems. See APTA Recommended Practices (**Table 1**).

4.3 Exterior doors

Manufactured in single- or double-leaf configurations, commercial security hollow metal exterior doors (exterior doors) typically serve as a facility's general public entrance and exit doors or as service entrances for facility operations personnel. A facility's doors also serve double-duty by providing an emergency egress function. Regardless of purpose, door systems generally include the door, door face, hinges, frame, locks, anchorage to the structure, and in some instances louvers and glazing.

Facility exterior doors are often the weakest part of the structure because of their service requirements and functional components. The number of exterior doors should be kept to a minimum to reduce the number of vulnerabilities to a facility's envelope. As part of a balanced design approach, exterior doors must provide a level of protection that is equal to or greater than the level of protection provided by a facility's associated walls, floors and ceilings to be effective. Door systems must withstand a certain amount of pressure from direct force, prying, frame spreading, explosion, vandalism, firearm attacks, etc., for a specific time (e.g., 5, 15 or 60 minutes) while under attack of basic hand tools.

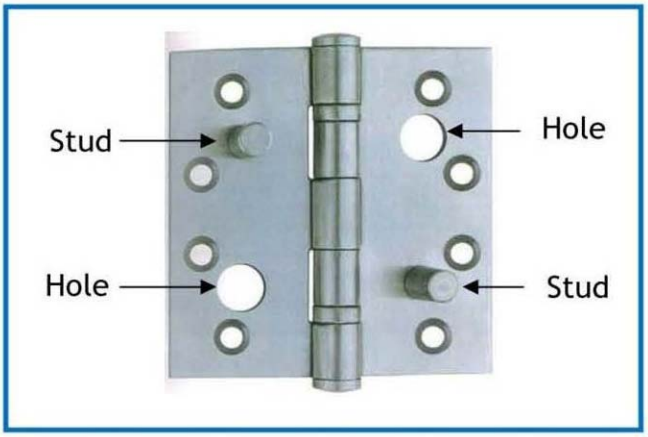
Depending on their specific function, exterior doors may be embedded with well-connected glazing and louvers. The appropriate fire-resistant classification should be identified and included in the design as required by fire-life-safety codes. Additional door system features, such as intrusion detection systems (IDS), video surveillance systems (VSS) (formerly known as closed-circuit television systems) and/or access control systems (ACS) should be designed without unintentional exposures to the door system. Similarly, interior doors protecting high-value or critical assets should prescribe to similar designs. Further information can be found in the equipment and technology section of the APTA Security Considerations Standard.

In coordination with IDS, all exterior doors should be clearly marked with numbers corresponding to an appropriate alarm zone to assist responding police and security with rapid identification of potential adversaries. Front and rear facility doors should be marked with the facility's address, on or above the doors. Peepholes should be designed into exterior doors to enhance surveillance of the facility's exterior without leaving it. To ensure that all doors are illuminated during hours of darkness, they should well lit by security lighting.

The installation of exterior doors with solid wooden cores and/or the addition of a steel plate attached over the face of a door can increase delay and penetration times through the opening. However, the increased weight and wear on the other door system components should be accounted for in the design.

Exterior doors should be securely anchored to a structure using a metal frame that is grouted with cement. Grouting supports the door system's supporting structure and provides protection against spreading of the doorframe to penetrate the opening. Exterior doors should also be mounted to open outward—that is, away from an interior space. Under blast conditions, outward opening doors will seat in their frames from the force of the detonation. This prevents exterior doors from entering the facility as a flying hazard during an explosive event. Unless prohibited by local jurisdiction, fire-life-safety codes all exterior doors should be used for emergency exit only. Additionally, all exterior hardware devices should be removed to reduce potential vulnerabilities associated with the devices. This includes exterior hardware where permissible.

FIGURE 1
Hinge Hardware Protection



To prevent removal of exterior doors from the hinge side, install hinges on the interior; provide concealed hinges; use heavy-duty grade with non-removable pins; or if removable pins are installed, weld them in place to prevent their removal and reduce their vulnerability to tampering. Alternatively, the stud-in-hole pinning method may be used. This type of hinge hardware is manufactured specifically with stud type pins attached to the inside face of a hinge leaf. When

the hinge closes, the stud pin inserts itself into a hole in the opposite hinge leaf to prevent removal of the door if hinge pins are removed or the edge of the hinge hardware is cut off (**Figure 1**).

High-risk-area doors may require ballistic protections against adversary actions to penetrate the opening. Exterior doors without glazing that require ballistic-level protection should be specified using industry standard ballistic level protection ratings (i.e., Underwriters' Laboratory [UL] Physical Security: Ballistics). See **Table 3**.

TABLE 3
Hinge UL 752 Ballistic Level Protection Ratings

Rating	Protection Against Weapons or Equivalents
1	9 mm or Super .38 caliber automatic handguns
2	.357 Magnum handgun
3	.44 Magnum handgun
4	30-06 rifle
5	.308 or equivalent rifle
6	9 mm submachine gun
7	M-16/AR-15 assault rifle (5.56 mm)
8	M-14 assault rifle (7.62 mm)
Shotgun	12 Ga. shotgun (lead slug and 00 lead buck)

4.4 Industrial doors

Although considered "doors," industrial doors (**Figure 2**) typically cover large openings in a facility's walls or exterior envelope to allow unloading and loading of trucks that back up to an elevated loading dock or platform. An industrial door's main function is to permit access to materials being introduced and or removed from the facility, but it also provides security. Industrial doors are used for material handling, not for pedestrian access.

FIGURE 2
Industrial Doors

Industrial door designs are typically roll up, coiled gates or sliding security grilles manufactured of steel, aluminum and/or stainless steel. Glass in-fill panels can be designed into the doors as a workforce safety measure. Industrial doors may be motorized and opened and closed with automatic gate operators, whereas smaller units may be operated by manual push-up, chain hoists or crank operations. Industrial doors may be designed with additional features, such as IDS, VSS and high-security locking devices. To accommodate pedestrian circulation, a commercial security hollow metal door may be designed and located nearby.

The design of industrial doors should complement the structural integrity of the facility envelope. Further, they should provide a level of protection against threats identified in the Transit Agencies security risk assessment.

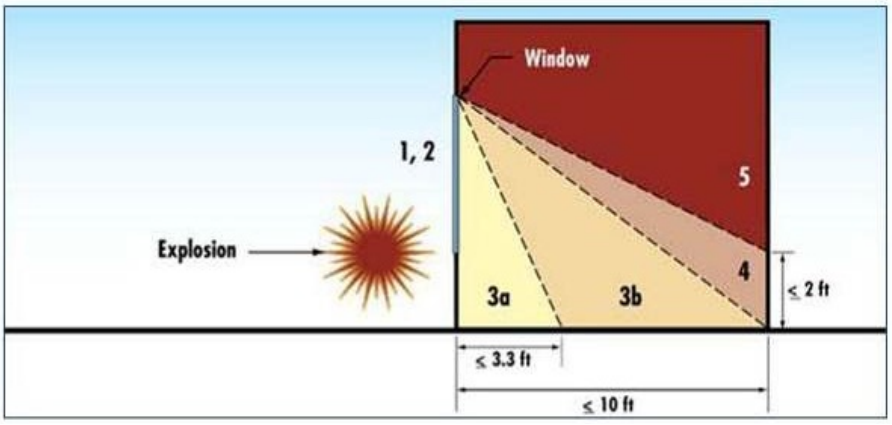
4.5 Windows

Window systems are a combination of glazing, anchorage, frames, supporting walls and connections to the building's structure on the exterior façade. Effective window system designs reduce the hazardous effects of flying glass shards and other fragmentation during an explosive event. The design of balanced window systems means these components would either resist or fail at the same explosive overpressure, and that the extent of damage would be controlled. The types of glass typically used in window glazing systems and their characteristics are listed in **Table 4**.

TABLE 4
Types of Glass Typically Used in Window Glazing Systems

Type of Glass	Strength	Fragment Fracture Characteristics
Annealed glass	Low	Razor-sharp shards, dagger-shaped fragments
Wire reinforced	Low	Razor-sharp shards, metal wire fragments
Heat strengthened	Low–Medium	Depends on surface compression and quality or manufacturing process. Can range from shards and fragments similar to annealed glass or small fragments similar to fully thermal tempered glass.
Laminated	Medium–High	Cracking of glass with interior layers retaining majority of fragments
Fully thermal tempered	Medium	Fractures into small cube-shaped fragments
Polycarbonate	High	Typically none

FIGURE 3
Window Glazing Performance



4.5.1 Performance conditions

Glass fragmentation entering a room or area after an explosive event can result in significant personal injury to occupants. The height of glass fragmentation's vertical entry into a room or area during a blast event, coupled with the distance it travels before landing on the floor away from the window are factors to determine the extent of personal injuries and sustained damages (**Figure 3**). Using these fragmentation performance conditions, desired window glazing response protection levels should be selected to reduce the risk to personnel, facilities, assets and operations (**Table 5**).

TABLE 5
Glazing Protection Levels Based on Fragment Impact Locations

Window Performance Condition	Description of Window Glazing Response	Protection Level	Hazard Level
1	Glazing does not break. No visible damage to glazing or frame.	Safe	None
2	Glazing cracks but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.	Very High	None
3a	Glazing cracks. Fragments enter space and land on floor not more than 3.3 ft from window.	High	Very Low
3b	Glazing cracks. Fragments enter space and land on floor not more than 10 ft from window.	High	Low
4	Glazing cracks. Fragments enter space and land on floor and impact a vertical witness panel at a distance of not more than 10 ft from the window at a height of no greater than 2 ft above the floor.	Medium	Medium
5	Glazing cracks and window system fails catastrophically. Fragments enter space, impacting a vertical witness panel at a distance of not more than 10 ft from the window at a height of no greater than 2 ft above the floor.	Low	High

4.5.2 Glass window protection from vandalism and other damages

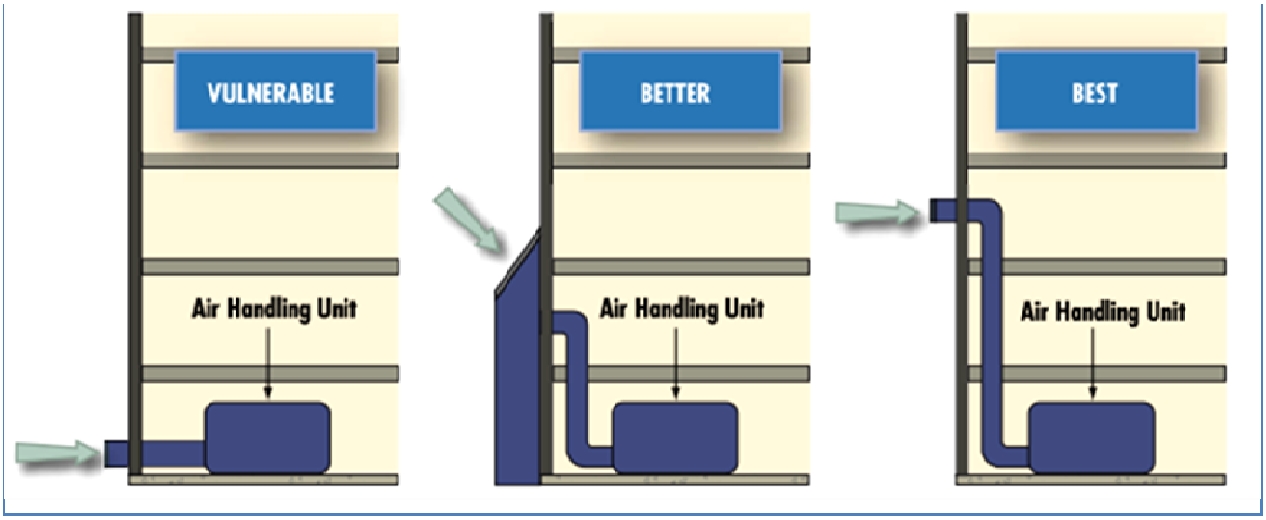
While replacement of vandalized vehicle glass windows is a viable option, it can also be a costly expense for transit agencies. Commercially available products ranging from heat treatment to repair/restore glass surfaces to multi-layered protective films applied directly to glass surfaces are available to control and reduce the incidents of graffiti vandalism (aka “scratchitti”) to glass surfaces on public transportation vehicles. Other associated measures to reduce vandalism issues throughout a system may also include a zero-tolerance policy that restricts vandalized vehicles from service and requires repair or removal of the damage within 24 hours of its discovery. Transit agencies should engage operators, staff and ridership in graffiti-prevention awareness campaigns to identify and report vandalism to vehicles. Local and transit law enforcement should work together to arrest and prosecute vandals.

4.6 HVAC control systems

HVAC system fresh air and return air intakes, fan rooms, air handling unit, and operations are vital building infrastructure. Designed well, these systems provide the facility with passive security countermeasure protection from hazardous materials released inside or outside a facility. For optimum effectiveness, the locations of HVAC zones and access to the system must be carefully planned, designed and controlled, and access to the system must be restricted. When planning for different conditioning zones, separate public areas from co-located operations to limit potential contamination of an entire facility resulting from a public area hazardous material release. Also, separate zone design should include emergency shutdown switches to control or slow the spread of hazardous material through a facility.

Air handling unit return air intakes should be elevated above the typical reach of people to limit the placement of objects and the introduction of hazardous materials into a facility. Under the best circumstances, the level of raised intakes should be as high as feasible from the ground (**Figure 4**). Where ground units cannot be relocated, install ducting to elevate the intake’s opening from the ground. Installing screening over an intake opening designed with a 45-degree angle reduces the placement or introduction of hazardous materials into the system. Securing rooftop access to HVAC system units and fencing off adjacent facility roof-to-roof accesses also restricts potential tampering of units. VSS should be installed to monitor high-risk systems.

FIGURE 4
Air Handling Security



4.7 Mail facility

Mail facilities, centers, mailrooms, interagency mail boxes, etc., are centralized “hubs” for collecting, holding and storing an agency’s packages, correspondence and other types of important documents shipped inbound and outbound of its facilities. These locations are vulnerable for an agency because they lack control of inbound shipments, but agencies are required to respond to any received threats.

To mitigate the risks that are inherent with mail centers, mailrooms, interagency mail boxes, etc., agencies should located these services away from main entrances and areas containing critical infrastructure, utilities, distribution systems and other important assets, and preferably on the outside perimeter of a facility. Additional safe mail handling guidance is available on the APTA security standards website (www.aptastandards.com/ Portals/0/Security_pdfs/APTA-SS-SEM-RP-008-09_mail_handling.pdf).

4.8 Utility openings

Protect utility openings using fastened grilles, locked manhole covers or other means to prevent entry. Steel bar grilles should be welded where the bars intersect in a crosshatch pattern and then to the pipe, culvert or opening they are intended to protect. Grilles may also be bolted or pinned in place to prevent removal of the grille. The bolts and pins must be peened to prevent their removal. When grilles or bars are used in drainage, sewerage, culverts, storm drains, etc., caution must be taken to ensure that they are not susceptible to clogging.

FIGURE 5
Utility Manhole Cover Locks

4.9 Perimeter roads

Perimeter roads provide an outer layer of protection and the ability to delay trespassers. They typically provide a means for law enforcement or security mobile patrols to randomly patrol a facility's or property's perimeter. Where the perimeter barrier (e.g., fencing) encloses an area generally greater than 1 sq. mi. (2.6 km^2), an interior perimeter road must be provided for the patrols. Drainage culverts passing under the road in clear zones must be secured at all openings as described herein for drainage and culverts under fences. Maintenance of the perimeter roadway should be regularly performed to prevent or remove overgrown vegetation, trees or shrubs; ensure snow or other debris removal; maintain an unobstructed line of sight along the property boundary; and to prevent damage to vehicles using the road.

4.10 Key and lock control

In the absence of an electronic access control system, mechanical locks and keys provide a method for controlling access to specific areas, equipment or facilities. The process for lock and key use in an agency's security program may be simple or complex, depending on the user's requirements. To ensure the integrity of accountable access control to specific areas, equipment and facilities, each property should establish a lock and key control program. Controlling locks and keys can reduce time-consuming and expensive lock and key control systems.

An agency key control program should, at a minimum, include the following:

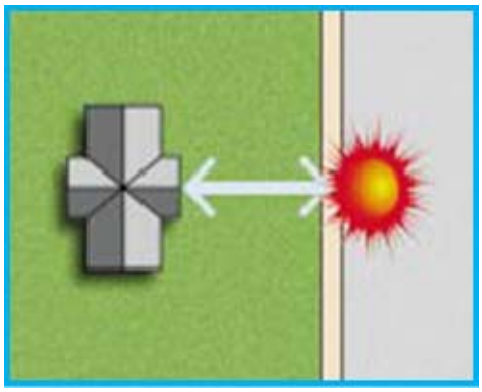
- Management's designation in writing of a person in charge of the agency's key control program and others who may be assigned agency key control program responsibilities.
- Development of a key control policy and procedures that describe agency master-keying, duplication, inventory, lock-outs, loss, rotation, storage and custody of key making materials, and other key program requirements.

4.11 Distances

4.11.1 Standoff distance

The distance from the threat (explosive device) to the target (facility or asset) is standoff. It is the most effective security measure for achieving protection from threats to a facility and its assets because as the shock wave expands over distance, the blast over-pressures decrease, resulting in less damaging pressure and forces reaching the target (**Figure 6**).

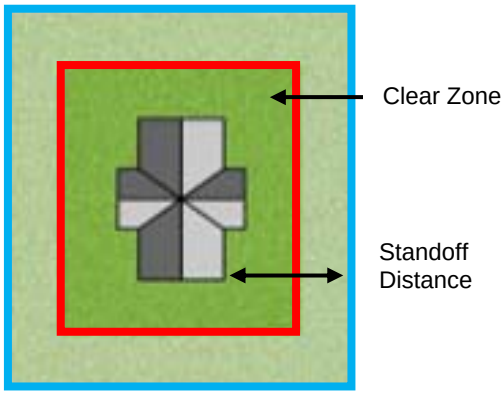
FIGURE 6
Standoff Distance



4.11.2 Clear zone

The clear zone is the area immediately adjacent to a facility's envelope by measuring outward from the facility's exterior. It provides facility occupants with an unobstructed view of the areas outside of the facility. The clear zone should remain clear of obstructions that could conceal the placement of a threat greater than 6 in. in height. Site furnishings or landscaping may be placed within the clear zone as long as threats are not concealed from the view of facility occupants. Electrical or mechanical equipment placed in the clear zone should be designed to prevent concealment of a threat in or around the equipment. Electrical and mechanical equipment in the clear zone should be either self-contained or screened on all five sides to prevent unauthorized access to the equipment. **Figure 7** shows the relationship between a clear zone and standoff distance.

FIGURE 7
Clear Zone



5. Training considerations

Most manufacturers recommend operator training for their systems. Operator training prevents serious injury and legal liability, as well as equipment damage caused by improper operations. If a manufacturer does not provide a thorough program for operator training, the user should develop the appropriate in-house checklist or policy for normal and emergency operations.

6. Maintenance considerations

Many manufacturers provide diagrams, maintenance schedules and procedures for their systems. They should also have spare parts available to keep the systems in continuous operation. The manufacturer should provide maintenance support in the form of training and operation and maintenance manuals. Maintenance contracts are available from most manufacturers. Reliability and maintainability data are available from most manufacturers. Maintenance should include inspection, adjustment, cleaning, pressure checks on operational systems and replacement of worn parts. If a manufacturer does not provide a thorough program for equipment maintenance, then the user should develop the appropriate in-house checklist or policy for normal and emergency operations.

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

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

American Public Transportation Association *Recommended Practices*:
APTA SS-SIS-RP-001-10: "Security Lighting for Revenue Transit Facilities"
APTA SS-SIS-RP-002-10: "Security Lighting for Nonrevenue Transit Facilities"
APTA SS-SIS-RP-003-10: "Fencing Systems to Control Access"
APTA SS-SIS-RP-004-10: "Chain Link, Mesh, or Woven Fencing Systems to Control Access"
APTA SS-SIS-RP-005-10: "Gates to Control Access"
APTA SS-SIS-RP-006-10: "Ornamental Fencing Systems to Control Access"
APTA SS-SIS-RP-007-10: "Crime Prevention Through Environmental Design for Transit Facilities"
APTA SEM-SS-RP-008-09: "Safe Mail and Package Handling"

Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, "Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks." http://www.cdc.gov/niosh/docs/2002-139/

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

Federal Emergency Management Agency (FEMA). "Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings." BIPS 06, October 2011. www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

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

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, *Risk Analysis and Security Countermeasure Selection*, (CRC Press, Boca Raton, FL, 2010).

Underwriter's Laboratory, "The Standard of Safety for Bullet-Resisting Equipment," UL 752. www.ul.com/global/eng/pages/offerings/industries/lifesafetyandsecurity/securityandsignaling/security/standards/

U.S. Postal Inspection Service, "Guide to Mail Center Security." http://about.usps.com/publications/pub166.pdf

Definitions

clear zone: The area immediately adjacent to a facility's envelope by measuring outward from the facility's exterior.

maintenance: The continued care and upkeep of a space for its intended purpose. It also serves as an expression of ownership.

scratchitti: A form of visual communications, typically illegal, involving the unauthorized marking of public space by an individual or group.

security risk assessment: A formal methodical process used to evaluate risks to a transit system. The security portion of the risk assessment identifies security threats (both terrorism and crime) to the transit system; evaluates system vulnerabilities to those threats; and determines the consequences to people, equipment and property.

standoff distance: The distance maintained between an asset or a portion thereof and the potential location for an explosive detonation or other threat.

Abbreviations and acronyms

AASHTO	American Association of State Highway and Transportation Officials
ACS	access control system
APTA	American Public Transportation Association
ASIS	formerly the American Society for Industrial Security
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FTA	Federal Transit Administration
HVAC	heating, ventilation, and air conditioning
IDS	intrusion detection system
NPRA	National Petrochemical & Refiners Association
UL	Underwriter's Laboratories
VSS	video surveillance system