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

APTA SS-SIS-S-010-13, Rev. 1
First Published: March 26, 2013
First Revision: May 23, 2023
Transit Infrastructure Security Working Group

Security Program Considerations for Public Transit

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

Keywords: anti-vehicle barriers, assessment, balanced security, ballistic, blast, clear zone, considerations, culverts, design considerations, doors, fencing, glass, hinges, key and lock control, layers of protection, planning, lighting, mailroom, perimeter roads, physical security, risk assessment, security, security program, site survey, standoff distance, windows

Summary: This standard proposes security program considerations for public transit to enhance the security of people, operations, assets and infrastructure. It offers an overview and descriptions of the applicability of the four pillars of security and how they may be integrated with other security standards and best practices to enhance transit security programs.

Scope and purpose: This standard addresses components of the four pillars of security—planning, operations, physical security, and equipment and technology—for consideration and use by the transit industry.

This document 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 recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Transit Infrastructure 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*

Ryan Chelski, *Sound Transit*
Neil Crosier, *King County Metro*
Matthew Dimmick, *STV Inc.*
Dean Fajerski, *TSA*
Kevin Franklin, *BART*
Rick Gerhart, *FTA*
Erin Gorrie, *ADS System Safety*
BJ Johnson, *RTA*
Stephan Parker, *Transportation Research Board*
Rob Pascoe, *King County Metro*
Jacob Peltier, *Community Transit*
John Plante, *METRA (retired)*
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Charles Rappleyea, *WSP USA*
Harry Saporta, *Tri-Met (retired)*
Jill Shaw, *DART*
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-SIS-S-010-13, Rev. 1, "Security Program Considerations for Public Transit."

A key objective of any public transportation system is to provide safe, secure and reliable public transportation services. Transit agency personnel, consultants and contractors are expected to implement appropriate security considerations throughout the planning, design, construction, fabrication, installation, testing, pre-operational and operational system phases of transit during the life cycle of the system.

This standard 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. Find APTA's Security Standards Program documents at www.apta.com.

Security Program Considerations for Public Transit

1. Overview

Transit agencies operate in inherently open environments. By design, transit systems provide ease of access and gather volumes of people in confined spaces to deliver efficient and convenient transportation throughout various regions and communities. These unique attributes make public transportation vulnerable to security-related risks and threats. For these reasons, transit agency understanding and buy-in to security program considerations is necessary to effectively manage organizational risks and enhance operational safety.

This standard proposes security program considerations for public transit to enhance the security of people, operations, assets and infrastructure. It offers an overview and descriptions of the applicability of the four pillars of security and how they may be integrated with other security standards and best practices to enhance transit security programs.

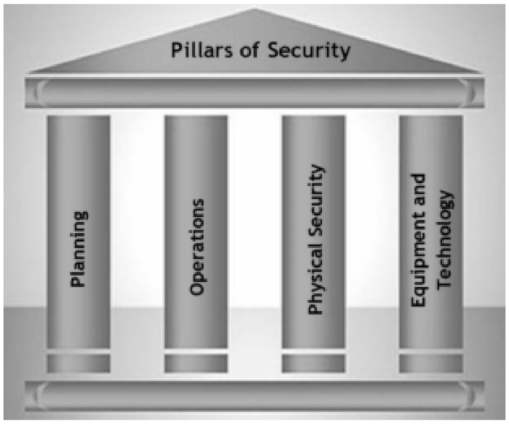
There is no “one size fits all” approach to implementing and operating security programs: Transit agencies may leverage different security methods, measures and solutions depending on their organizational realities. However, transit agencies should embrace foundational security practices and examine the full spectrum of security program considerations when making critical decisions. Well-administered security programs provide the following benefits to people, assets, operations and infrastructure.

- Enhance the safety and security experience of ridership within the transit environment
- Ensure that transit employees, operators and first responders understand security procedures
- Enable the transit agency to coordinate with federal, state, local, tribal and private sector partners
- Create a pride of ownership among transit users and employees

2. Pillars of security

To mitigate risks and operate effective security programs, transit agencies should align security methods, measures and solutions to the four pillars: planning, operations, physical security, and equipment and technology (**Figure 1**). The pillars exist collectively to provide a uniform approach to the application of security solutions. When effectively applied, these components provide an agency with an integrated and balanced approach to security.

FIGURE 1
Pillars of Security



2.1 Planning pillar

The planning pillar identifies processes for developing proactive and reactive plans to mitigate and/or respond to security incidents.

2.1.1 Security risk assessments

Risk is 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. Security risk assessments are intended to evaluate security-related risks (terrorism, criminal activity, etc.) to transit agencies and their assets. These assessments form the basis of robust security programs, as they will inform the implementation of plans, measures and procedures to mitigate risks.

Transit agencies should complete a system-wide Security Risk Assessment that incorporates all agency modes, assets and facilities. When agencies want to determine risk to a specific site or asset, they should perform a site-specific Security Risk Assessment.

See APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit," for more information.

2.1.2 System security plan (SSP)

An SSP is a roadmap that provides a thorough outline of an organization's system security requirements. Select transit agencies are required to develop SSPs in accordance with 49 CFR Part 1582. Transit agencies may also be required to develop SSPs in accordance with applicable state safety oversight agency program standards.

In addition to required components, transit agencies should consider conducting the following activities when developing SSPs:

- Identify the policies, goals and objectives for the security plan and consult with management to achieve initial buy-in.
- Review state and local regulations and guidelines; industry best practices; and all relevant security-related activities and documentation, including those generated or performed by outside agencies.
- Collect operational information, security risk assessment documentation, and transit crime statistics and trends.

- Document the agency's process for managing threats and vulnerabilities during operations and for major projects, extensions and new vehicles and equipment, including integration with the safety certification process.
- Catalog controls in place that address the personal security of passengers and employees.
- Document the agency's process for conducting internal security reviews to evaluate compliance to applicable regulations and to measure the effectiveness of the plan.
- Analyze collected security data to evaluate security events and programs to inform corrective actions.

Transit agencies may also incorporate an emergency operations plan (EOP) or emergency management plan into their SSP. This EOP should provide an operational framework for how the agency will plan for, respond to and recover from an emergency. An EOP may also include a crisis management plan. See APTA SS-SEM-S-014-19, "Transit Agency Emergency Management Program," for more information on EOPs.

2.1.3 Continuity of operations (COOP) plan

A COOP plan is a document that prepares a transit agency to provide essential agency functions following a significant event that limits or restricts the availability of personnel, facilities or technical systems. In many cases this is simply documenting and consolidating procedures and policies and, if there are failure points, how one continues to conduct essential business functions.

A COOP plan is a specific component of a transit agency's overall Emergency Management Program, serving as a standalone plan that focuses on agency recovery and restoration actions necessary to continue service to customers and other essential business functions. A COOP plan typically focuses on restoring limited operating capability, usually within a 12-hour period and for a period of up to 30 days. Beyond 30 days, it is assumed that an agency will have reestablished a degree of normality.

See APTA SS-SEM-S-001-08, "Continuity of Operations Plan for Transit Agencies," for more information.

2.1.4 Sensitive security information (SSI)

SSI is a specific category of information that if released to the public would be harmful to transportation security. It is a form of sensitive information but is not considered to be classified information. TSA issued an extension of SSI protections through all systems of transportation.

SSI regulations are set by the government to prevent harm to an organization or its customers. Refer to 49 CFR Part 1520 for the most current SSI policy information. Agencies should consult with their legal department to ensure that any actions the organization undertakes comply with 49 CFR Part 1520 and all other federal, state and/or local laws governing protection of information

See APTA SS-ISS-RP-003-23, "Sensitive Security Information Policy," for more information.

2.1.5 Security and emergency preparedness action items

The "Security and Emergency Preparedness Action Items for Transit Agencies" resource document provides a list of 17 baseline measures that any transit agency can employ to elevate security readiness. Developed collaboratively by FTA and TSA, these action items are dynamic and subject to regular review to ensure that recommended actions address current security realities. Compliance is voluntary; however, transit agencies may consider implementing these action items to address current security threats and risks. A detailed listing is described in **Table 1**.

TABLE 1
Security and Emergency Preparedness Action Items for Transit Agencies

Item	Program Element	Action
1	Management and Accountability	Establish written SSPs and emergency operations/response plans.
2	Management and Accountability	Define roles and responsibilities for security and emergency preparedness.
3	Management and Accountability	Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control.
4	Management and Accountability	Coordinate security and emergency operations/response plans with local and regional agencies.
5	Security and Emergency Response Training	Establish and maintain a security and emergency training program.
6	National Terrorism Advisory System (NTAS)	Establish plans and procedures to respond to the NTAS alert levels.
7	Public Awareness	Implement and reinforce a public security and emergency awareness program.
8	Risk Management and Assessment	Establish and use a risk management process.
9	Risk Information Collection and Sharing	Establish and use an information sharing process for threat and intelligence information.
10	Drills and Exercises	Conduct tabletop and functional drills.
11	Cybersecurity	Develop a comprehensive cybersecurity strategy.
12	Facility Security, Access Controls, and Background Investigations	Control access to security-critical facilities with identification (ID) badges for all visitors, employees and contractors.
13	Facility Security, Access Controls, and Background Investigations	Conduct physical security inspections.
14	Facility Security, Access Controls, and Background Investigations	Conduct background investigations of employees and contractors.
15	Document Control	Control access to documents on security critical systems and facilities.
16	Document Control	Process for handling and access to SSI.
17	Security Program Audits	Establish and conduct security program audits.

See “Security and Emergency Preparedness Action Items for Transit Agencies: A Resource Document for Transit Agencies” for more information.

2.1.6 Training considerations

Transit agencies should consult training resources for clarification on developing proactive and reactive transit security plans. Various federal agencies and private organizations including the Transportation Safety Institute (TSI), American Society for Industrial Security (ASIS) and the National Transit Institute (NTI) offer transit-specific training courses that discuss planning activities and documents. For example, TSA issued the Security Training for Surface Transportation Employees Final Rule, published March 23, 2020, which identifies training requirements for covered agencies. See APTA SS-SRM-RP-005-12, “Security Awareness Training for Transit Employees,” for more information.

Transit agencies may opt to validate plans, policies and procedures in an exercise environment. Exercises are a critical tool for assessing overall preparedness, determining organizational strengths and identifying areas for improvement. See APTA SS-SEM-S-004-09, "Transit Exercises," for more information.

2.2 Operations pillar

The operations pillar delineates security-specific program information and functions and involves agency management and staff who implement these functions on behalf of the system and its ridership. This pillar 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 operators and ridership preparedness.

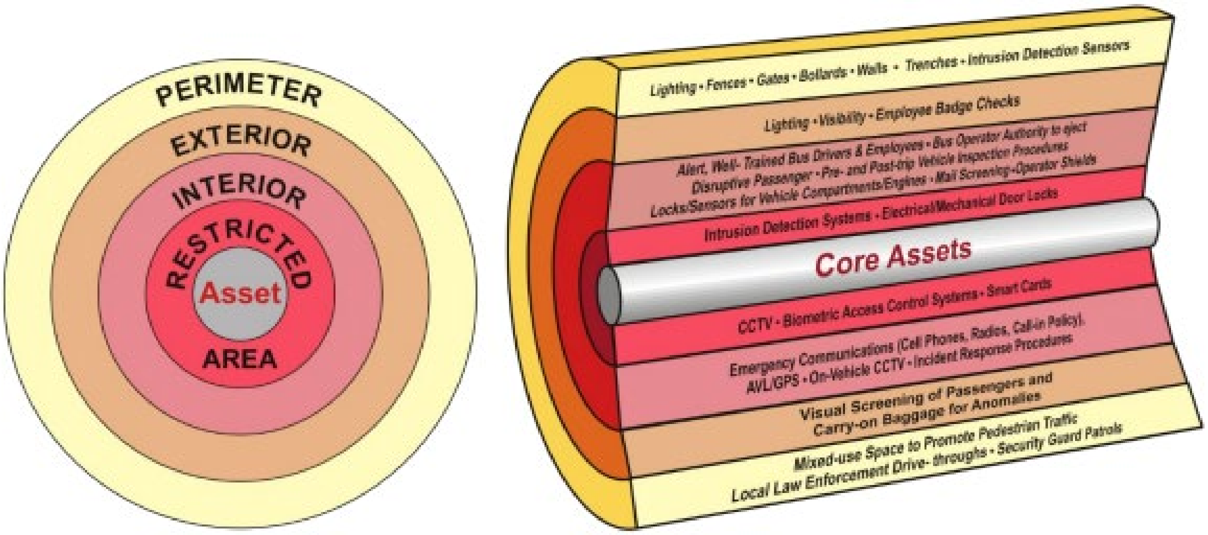
2.2.1 Deterrence and layered security

Transit agencies should achieve transportation security through coherent security systems that are well-integrated with transportation operations and are deliberately designed to deter terrorists even as they selectively guard against and prepare for terrorist attacks by adversaries. In particular, layered security systems, characterized by an interleaved and concentric set of security features, have the greatest potential to deter and protect.

Transit agencies could consider placing security measures at several different layers throughout a system to provide greater redundancy and protection for assets. The concept of layered protection recommends placing the most critical or vulnerable asset in the center of concentric levels of increasingly stringent security measures, as depicted in **Figure 2**. This allows multiple opportunities for thwarting or disrupting terrorist activities and is a key aspect of an effective security program.

The effectiveness of layered security is assessed by the ability of the measure to deter, delay, detect, respond and recover, per the five basic security principles.

FIGURE 2
Layered Security to Protect Critical Assets


PERIMETER
EXTERIOR
INTERIOR
RESTRICTED AREA
Asset
Lighting • Fences • Gates • Bollards • Walls • Trenches • Intrusion Detection Sensors
Lighting • Visibility • Employee Badge Checks
Alert, Well- Trained Bus Drivers & Employees • Bus Operator Authority to eject Disruptive Passenger • Pre- and Post-trip Vehicle Inspection Procedures Locks/Sensors for Vehicle Compartments/Engines • Mail Screening • Operator Shields
Intrusion Detection Systems • Electrical/Mechanical Door Locks
Core Assets
CCTV • Biometric Access Control Systems • Smart Cards
Emergency Communications (Cell Phones, Radios, Call-in Policy), AVL/GPS • On-Vehicle CCTV • Incident Response Procedures
Visual Screening of Passengers and Carry-on Baggage for Anomalies
Mixed-use Space to Promote Pedestrian Traffic
Local Law Enforcement Drive- throughs • Security Guard Patrols

See APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit," for more information about layered security.

2.2.2 Security manpower planning model (SMPM)

The SMPM is a flexible decision support tool created to enable transit security planners the ability to assess impacts of strategic decisions on resources and staffing. Based on input data, the model identifies staffing levels and budgeting. The SMPM is flexible and may be used by any transit agency with existing or planned security resources, regardless of operating mode(s) or size. Further, the model can assist security by assessing impacts of various scenarios on resource and deployment strategies, including:

- changes in revenue service operations (e.g., adding a new rail line, restructuring existing routes or special event service planning);
- changes in ridership patterns, crime/incident rates and threat information;
- changes in security personnel configurations (e.g., alternative mixes of internal/external security resources);
- changes in how security forces are deployed;
- adjustments to security coverage levels; and
- implementation of proof-of-payment fare enforcement or other related security duties.

Once the organization has made the determination that a change is necessary due to any of the above or other outside factors, SMPM will play a supporting role in the broader change management plan and program. The SMPM will address personnel-related aspects of the change, while other portions of the program will cover the technologies and processes implemented as part of the change.

2.2.3 Federal operational resources

The federal government has developed and implemented several programs to enhance the security posture of the nation's transit agencies, including the following:

- **Transit Security Grant Program (TSGP):** The Department of Homeland Security (DHS) allocates grant funding to the nation's mass transit and passenger rail systems. TSGP provides funds to owners and operators of public transit systems to protect critical transportation infrastructure and the traveling public from acts of terror. The TSGP is jointly managed by TSA and the Federal Emergency Management Agency (FEMA). TSA provides subject matter expertise on all matters relating to transportation security and other programmatic updates, and FEMA operates the administrative mechanisms needed to implement and manage the program.
- **Baseline Assessment and Security Enhancement (BASE):** BASE is TSA's no-cost, voluntary and risk-based program that evaluates the annual security posture of surface transportation systems. TSA transportation security inspectors assess organizations on Security Action Items (SAIs) that address industry fundamentals. BASE includes SAIs related to training/awareness programs and cyber/physical protections that are designed to measure the breadth of organizational security plans. Following the BASE, TSA inspectors provide organizations with the results of the assessment and actionable recommendations to improve their security posture.
- **Visible Intermodal Prevention and Response (VIPR):** TSA's VIPR Program provides VIPR teams that work with local security and law enforcement officials to supplement existing security resources. VIPR teams may consist of federal air marshals, transportation security inspectors, transportation security officers, explosives-detection canine teams, behavioral detection officers, explosives security specialists, and necessary supporting equipment. VIPR teams offer the ability to raise the level of security in any mode of transportation anywhere in the country, quickly and effectively provide deterrent presence and detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities.

2.2.4 Passenger security inspections (PSIs)

PSIs are inspections of transit passengers by transit security or staff and are believed to both deter and detect terrorist activity. PSIs are most often used by larger multimodal agencies and by ferry systems. A benefit of PSIs is the relative ease with which screening intensity, method and location can be altered based on the threat level and other intelligence information. Because the Fourth Amendment requires warrants or individual suspicion to conduct inspections, PSIs are legally permissible only if they can be justified. Therefore, transit agencies should consult legal counsel to carefully consider issues before implementation.

2.2.5 Security awareness campaigns

2.2.5.1 If You See Something, Say Something

This public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities.

2.2.5.2 "On the Tracks: Rail Sabotage Awareness and Reporting"

This educational video aims to provide those responsible for the safety and security of the nation's rail system with information on the nature of rail sabotage threats and the necessary steps to take in safeguarding against its execution. The video addresses where to look for potential sabotage threats, the categories of threats to be on alert for, and the steps to take in reporting objects or activities that appear out of the ordinary.

2.2.5.3 Transit Watch

This nationwide public awareness outreach campaign encourages the active participation of transit passengers and employees in maintaining a safe transit environment. The campaign was also designed to help foster the role of transit as a safe haven in communities across the country. The campaign has a useful toolkit that enables transit agencies to customize Transit Watch materials with local information and select the campaign and accompanying visuals that would most effectively address specific community interests and concerns.

2.2.5.4 "The Mark"

This training video depicts a fictionalized version of a threat against a metropolitan transit system. It demonstrates to transit employees how asking questions and following their instincts when faced with suspicious and unusual circumstances could ultimately mean the difference between life and death.

2.2.5.5 NTI's Public Transportation Emergency Preparedness Workshop

This course is designed to prepare transit systems, emergency service agencies and other emergency management partners to collaborate, share resources and implement plans to best mitigate injury, loss of life and damage to property and assets when incidents occur. This workshop provides a forum to discuss all aspects of the challenges of large-scale, multiagency response and incident management with selected representatives from public transit systems; private transportation companies; emergency services; various levels of transportation departments; healthcare facilities; and state, local and federal governments.

2.2.5.6 ASIS's Private Security Officer Guideline

This guideline provides a framework for private security officer job descriptions and recommended minimum selection criteria, as well as an outline for the design and delivery of private security officer training by employers and other agencies.

2.2.5.7 Security alerts

The National Terrorism Advisory System (NTAS) replaced the color-coded Homeland Security Advisory System. This system more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

NTAS alerts include a clear statement that there is an imminent or elevated threat. Using available information, the alerts provide a concise summary of the potential threat; information about actions being taken to ensure public safety; and recommended steps that individuals, communities, businesses and governments can take to help prevent, mitigate or respond to the threat.

An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves. NTAS alerts contain a sunset provision indicating a specific date when the alert expires; there will not be a constant NTAS alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the secretary of Homeland Security may announce an updated NTAS alert. All changes, including the announcement that cancels an NTAS alert, will be distributed the same way as the original alert.

2.2.6 Training considerations

Transit agencies should provide security awareness training to all employees—including most, if not all, contract employees—to strengthen transit system security. Topics may span a variety of critical learning objectives but should include identification and definitions of security concerns; security roles and responsibilities; and recognizing, reacting, reporting and responding to transit crime and terrorism. Transit agencies may also be subject to the Security Training for Surface Transportation Employees Final Rule, which requires owners/operators of public transportation agencies to provide TSA-approved security training to employees who perform security-sensitive functions. See APTA SS-SRM-RP-005-12, "Security Awareness Training for Transit Employees," for more information.

Transit agencies may opt to leverage exercises to supplement training. Exercises are planned events that provide a low-risk environment for individuals, organizations and jurisdictions to discuss and/or validate capabilities. Exercises also present an opportunity to familiarize agency personnel with their security-related roles and responsibilities while also encouraging communication and collaboration across the agency and surrounding community. See APTA SS-SEM-S-004-09, "Transit Exercises," for more information.

2.3 Physical security pillar

The physical security pillar is based on the notion that efficient design and effective placement of physical security elements in a transit environment help reduce risk from adversaries.

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.

2.3.1 Security principles

Transit agencies should leverage risk assessment findings to select security measures that adequately protect people, assets, operations and infrastructure. Specifically, agencies should evaluate security program measures through the lens of the five basic security principles: deter, delay, detect, respond and recover.

Each security measure should offer one or more of the five elements to a critical asset, and each critical asset should have security measures that collectively span all five elements. Together, these security measures provide obstacles that an adversary must overcome to gain access, and then minimize the consequences if the threat is realized.

See APTA SS-SIS-S-017-21, “Security Risk Assessment Methodology for Public Transit,” for more information.

2.3.2 Crime prevention through environmental design (CPTED) planning

CPTED is a process that focuses on designing safety and security into the natural, physical and social environment of a specific area to reinforce positive behavior. Transit agencies should perform CPTED site surveys to identify environmental vulnerabilities and recommend enhancements that reduce risk to people, operations and facilities. Site surveys should address the following CPTED principles:

- **Natural surveillance:** The design of an environment with clear sight lines to maximize visibility and observation. This includes the placement of physical features and activities to create a perception that individuals are under observation.
- **Natural access control:** Controlling access to a site through the strategic design of streets, sidewalks, building entrances and landscaping.
- **Territorial reinforcement:** The use of physical attributes that express ownership and notify users and nonusers of the boundaries of a space or facility.
- **Maintenance and activity support:** Care and upkeep demonstrate ownership and intolerance for disorder. Encouraging appropriate activities preserves the intended use of the space.

Documented best practices in transit CPTED should be reviewed for appropriate incorporation in the design. See APTA SS-SIS-RP-007-10, “Crime Prevention Through Environmental Design,” for more information.

2.3.3 Security lighting

Security lighting is a cost-effective and universally accepted security measure that any organization can use to improve its security posture. Effective security lighting both deters criminal behavior and enhances safety, thereby reducing overall risk. Properly designed and planned security lighting can create a sense of openness and security for passengers. Security lighting aids the ability to observe and monitor movements through the facilities and supports the fundamental principles of CPTED.

See APTA SS-SIS-RP-001-10, “Security Lighting for Passenger Facilities,” for more information.

2.3.4 Fencing and gates

Fencing systems are a component of access control systems. They define boundaries and limits, channel access and egress, provide visual barriers, support security and safety, and can deter and delay intrusion and trespassing. Many fencing systems are available to the public transportation industry, ranging from high-security grille type to cost-effective chain-link. Fencing systems should be integrated with other security standards and best practices, such as CPTED, lighting, barriers and so on to provide protection and enhance other security solutions.

See APTA SS-SIS RP-003-10, “Fencing Systems to Control Access to Transit Facilities,” for more information.

2.3.5 Physical security doors

Commercial security hollow metal doors, or “exterior doors,” typically serve as a facility’s public entrance/exit or as a service entrance for facility operations personnel. They may be manufactured in single- or double-leaf configurations. 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.

Industrial doors, on the other hand, cover large openings in a facility's walls or exterior envelope to allow unloading and loading of trucks. Trucks typically back up to the facility's elevated loading dock or platform. An industrial door's main function is to permit access to materials being introduced to or removed from the facility, but it also provides security. Industrial doors are used for material handling, not for pedestrian access.

Doors are a critical feature for physical security at transit agencies. See Appendix A: Physical Security Doors for more information.

2.3.6 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.

See Appendix B: Windows for more information.

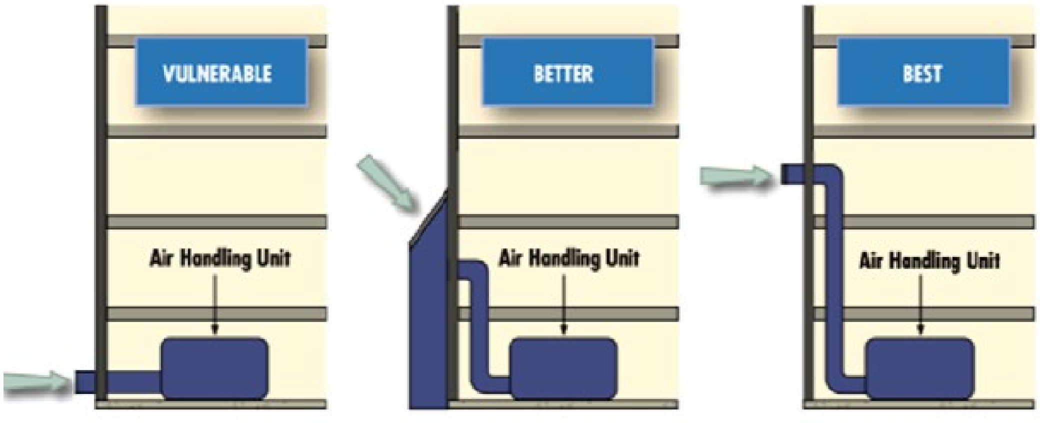
2.3.7 HVAC

HVAC system fresh air and return air intakes, fan rooms, air handling units 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 colocated operations to limit potential contamination of an entire facility resulting from a public area hazardous material release. Also, 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 3**). 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. Video surveillance systems should be installed to monitor high-risk systems.

FIGURE 3
Air Handling Security



2.3.8 Mail facility

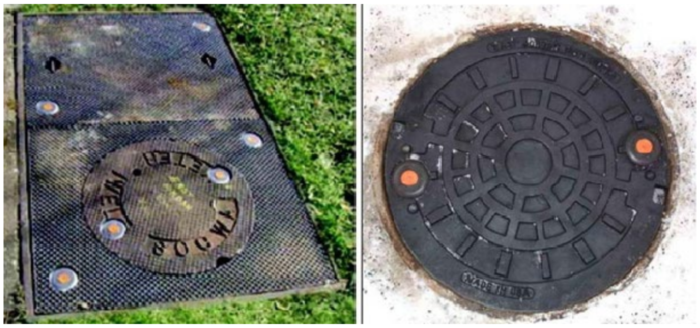
Mail facilities, centers, mail rooms and interagency mailboxes are centralized “hubs” for collecting, holding and storing an agency’s packages, correspondence and other types of important documents. To mitigate inherent risks, agencies should locate these services away from main entrances and areas containing critical infrastructure, utilities, distribution systems and other important assets, and preferably on the outside perimeter of a facility.

See APTA SS-SEM-RP-008-09, “Safe Mail and Package Handling,” for more information.

2.3.9 Utility openings

Transit agencies should protect utility openings using fastened grilles, locked manhole covers or other means to prevent entry (**Figure 4**). Steel bar grilles may 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 may 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 4
Utility Manhole Cover Locks



2.3.10 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 the perimeter of a facility or property. Where the perimeter barrier (e.g., fencing) encloses an area generally greater than 1 sq. mi (2.6 km^2), an interior perimeter road may be provided for the patrols. Drainage culverts passing under the road in clear zones should 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; to ensure snow or other debris removal; to maintain an unobstructed line of sight along the property boundary; and to prevent damage to vehicles using the road.

2.3.11 Key and lock control

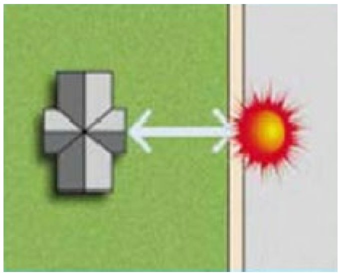
In the absence of an electronic access control system, mechanical locks and keys provide a method for controlling access to specific areas, equipment or facilities. The process for lock and key use in an agency's security program may be simple or complex, depending on the user's requirements. To ensure the integrity of accountable access control to specific areas, equipment and facilities, each property should establish a lock and key control program. 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, lockouts, loss, rotation, storage and custody of key making materials, and other key program requirements.

2.3.12 Distance considerations

Standoff distance (see **Figure 5**) is the distance from the threat (explosive device) to the target (facility or asset). 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.

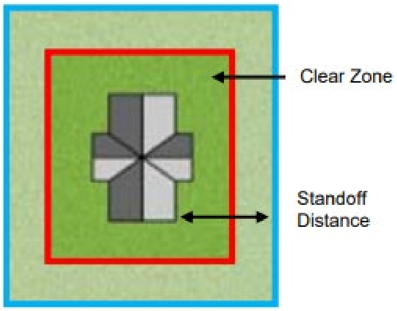
FIGURE 5
Standoff Distance



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 6 shows the relationship between a clear zone and standoff distance.

FIGURE 6
Clear Zone



2.3.13 Training considerations

Agencies may request operator training for their physical security measures, equipment and systems from the manufacturers. Operator training may prevent serious injury and potential legal liability, and mitigate equipment damage caused by improper operations. If a manufacturer does not provide a thorough program for operator training, the agency should develop the appropriate in-house program and include a checklist or policy for normal and emergency operations.

2.3.14 Maintenance considerations

It is recommended that agencies request diagrams, maintenance schedules and procedures for their physical security measures, equipment and systems. Manufacturers or integrators should also be required to have spare parts available to keep systems in continuous operation. The manufacturer should provide maintenance support in the form of training and/or operation and maintenance manuals. Maintenance contracts are available from most manufacturers. Reliability and maintainability data are also 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, the agency should develop the appropriate in-house checklist or policy for normal and emergency operations.

2.4 Equipment and technology pillar

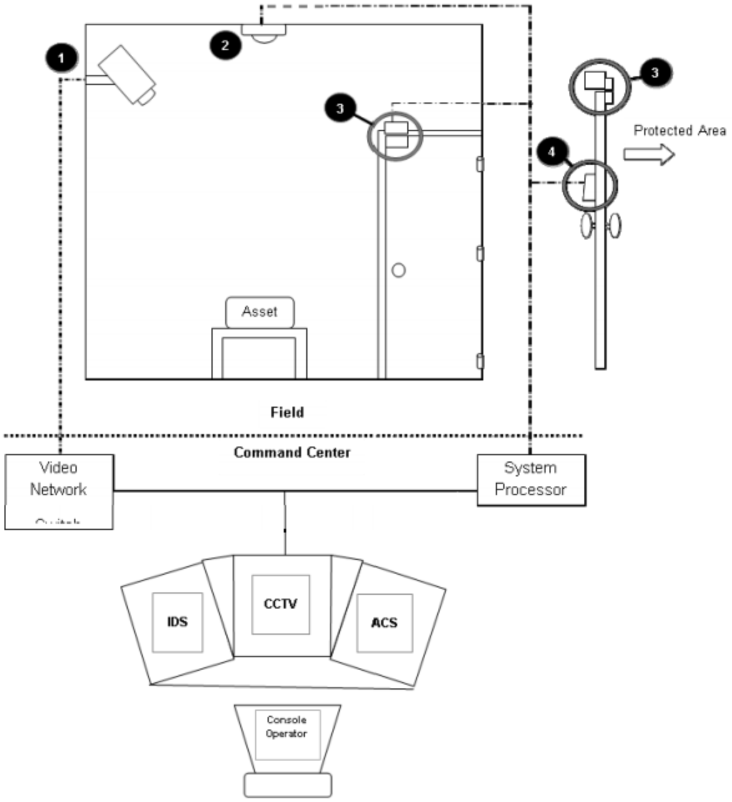
This pillar describes the basic elements of equipment and technology that transit agencies can leverage to reduce risk, including hardware and software applications to manage access to different areas of a protected facility. These elements should be coupled with other systems and technology to provide pinpoint or wide area surveillance and to integrate with systems that communicate internally to staff and employees and externally to first responders, operators and ridership. This pillar also includes features designed to protect these management systems from intrusion, hacking or access denial.

The equipment and technology pillar incorporates elements of several pillars together into a system that provides a uniform approach to applying a security mitigation strategy. However, equipment and technologies described herein may also be used as standalone systems.

2.4.1 Electronic security system (ESS)

An ESS should be designed to deter, detect, delay, assess and facilitate response to adversarial actions against an agency's facilities or users. The example in **Figure 7** demonstrates key elements of an effective ESS, including early warning of an internal or external intruder and consisting of hardware and software operated by trained personnel. An ideal system would include an access control system, an intrusion detection system and a video surveillance system integrated as a single physical protection system. To attain balanced protection, an agency should designate protection zones throughout its property and, by applying the basic principles of security, integrate layers of protection through deployment of ESS to mitigate risk.

FIGURE 7
Basic ESS Overview



2.4.2 Physical access control system (PACS)

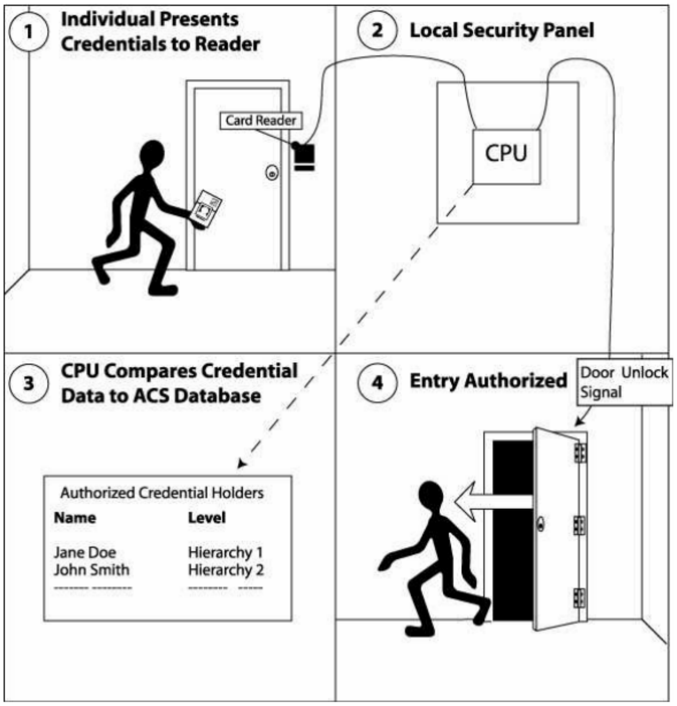
A PACS manages access to specifically designated areas of facilities. The basic PACS sequence is as follows: the user presents the access medium (credential) for authentication; the central processing unit (CPU) compares the credential with the PACS enrollment database; the credential is validated and authorizes access; and then the CPU unlocks the controlled door, permitting entry to the authorized user (see **Figure 8**). Authorized people may be employees, contractors or visitors.

At a minimum, components of a PACS should include an enrollment station (camera, computer, badge printer); credentials (key card/badge, PIN/biometric data); card readers (swipe, proximity); electric locks; and the capability to record authorized, unauthorized and attempted access control events.

PACS credentials are based on one or more of the following principles:

- **What you have:** A PACS credential (key card/badge).
- **What you know:** A personal identification number (PIN).
- **Who you are:** A personal attribute (e.g., fingerprint, other biometrics)

FIGURE 8
Basic PACS Sequence



All PACS credentials must be controlled. The access medium and a current picture of the user should be combined into the same credential. The user's picture should include a view from the shoulders to the top of the head, be colored and be heat laminated into the credential. The user's name, organization and an expiration date should be printed in a viewable font on the front of the credential and be visible from a distance. Include "Return if Found" information (e.g., address and contact) on the access medium to enhance its recovery if lost. To prevent a lost credential from posing a security threat, transit agencies may opt to leave credentials unmarked so as not to indicate the facility or system to which it grants access.

A PACS medium should also be integrated with video surveillance systems and intrusion detection systems to monitor time and attendance, providing authorized users access to areas without activating an alarm. Similar applications may be applied to vehicle gates or fencing, doors and other access openings.

2.4.3 Intrusion detection system (IDS)

An IDS combines detection sensors (e.g., door, window, area) with a computer, an alarm control panel and a power source to detect unauthorized entry into a protected area and to provide notification (e.g., alarm, siren) that a breach has occurred. IDS may also be integrated with the appropriate PACS and video surveillance system interfaces to detect one or more types of intrusion into protected areas.

See Appendix C: IDS and Sensors for additional information.

2.4.4 Video surveillance system (VSS)

A VSS is a collection of cameras and recording systems designed to capture video and/or audio information on an agency's network. Transit agencies may implement VSS as well as high-speed digital networks and trainlines for use within transit systems.

Practical applications for VSS include, but are not limited to, the following:

- security monitoring in stations
- security monitoring in parking lots and structures
- security monitoring for tunnels and bridges
- security monitoring for facilities
- operations monitoring in stations and key locations
- onboard monitoring on trains (safety, security, interior monitoring and loss prevention)
- onboard monitoring on buses (safety, security, interior monitoring and loss prevention)
- external monitoring (safety, security, accident investigation and platform monitoring)
- loss-prevention monitoring for revenue systems
- forensic evidence for criminal and/or accident investigations

Agencies may wish to implement VSS for any of the reasons above. If the intent is to utilize VSS to support investigations, then the design should address field of view, desired detail levels (scene, activity, identity), lens and image quality, frame rate considerations, and storage and retention with evidentiary requirements in mind during specification.

See APTA IT-CCTV-RP-001-11, “Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Trainlines for Use in Transit-Related CCTV Systems,” for more information.

2.4.5 Emergency call stations

Emergency call stations (ECS) provide ridership with a direct link from a point within the transit environment to a security operator. ECS are designed for installation at a variety of areas and to withstand the physical environment and operational conditions encountered.

See Appendix D: Emergency Call Stations for more information.

2.4.6 Training and maintenance considerations

ESS system operators should attend manufacturers’ basic and refresher training for the systems they operate.

Transit agencies should follow each ESS manufacturer’s recommended annual, quarterly and/or periodic maintenance schedule to maintain each system’s optimum functionality. Also, the transit agency’s bid review process may include contacting identified customers to ascertain performance and other service data about the bidder’s product. When advertising for bids from manufacturers, specifications should include a requirement that the bid response include a list of customers that have purchased/installed the bidder’s product.

Lastly, agencies should remain mindful of the potential adverse impacts of their operating environment on ESS equipment. Environmental factors such as brake dust, vehicle exhaust, vibrations of passing trains, etc. can all impact the standard maintenance schedules identified by manufacturers.

Related APTA standards

APTA IT-CCTV-RP-001-11, "Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Trainlines for Use in Transit-Related CCTV Systems"
APTA-SS-CCS-RP-001-10, "Securing Control and Communications Systems in Transit Environments, Part 1"
APTA SS-ISS-RP-003-23, "Sensitive Security Information Policy"
APTA SS-SEM-S-001-08, "Continuity of Operations Plan for Transit Agencies"
APTA SS-SEM-RP-004-08, "Security and Emergency Management Aspects of Special Event Service"
APTA SS-SEM-S-004-09, "Transit Exercises"
APTA SS-SEM-RP-008-09, "Safe Mail and Package Handling"
APTA SS-SEM-S-014-19, "Transit Agency Emergency Management Program"
APTA SS-SIS-RP-001-10, "Security Lighting for Passenger Facilities"
APTA SS-SIS RP-003-10, "Fencing Systems to Control Access to Transit Facilities"
APTA SS-SIS-RP-007-10, "Crime Prevention Through Environmental Design"
APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit"
APTA SS-SRM-RP-005-12, "Security Awareness Training for Transit Employees"
APTA SS-SRM-RP-006-11, "Random Counterterrorism Measures on Transit Systems"
APTA SS-SRM-RP-007-12, "Recognizing and Responding to Suspicious Unattended Packages, Devices and Baggage"
APTA SS-SRM-RP-009-09, "Identifying Suspicious Behavior in Mass Transit"

References

American Association of State Highway and Transportation Officials (AASHTO), "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection." https://trid.trb.org/view/718608

ASIS International, Standards and Guidelines. https://www.asisonline.org/publications--resources/standards--guidelines/

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," DHHS (NIOSH) Publication Number 2002-139, May 2002. http://www.cdc.gov/niosh/docs/2002-139/

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

DHS, "Privacy Impact Assessment for the Screening of Passengers by Observation Techniques (SPOT) Program," August 2008. www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_spot.pdf

Electronic Code of Federal Regulations, 49 CFR 659, "Rail Fixed Guideway Systems; State Safety Oversight," October 2004. https://www.govinfo.gov/app/details/CFR-2004-title49-vol6/CFR-2004-title49-vol6-part659

Federal Emergency Management Agency (FEMA), "Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks," FEMA 452, January 2005. https://www.fema.gov/sites/default/files/2020-08/fema452.txt

FEMA. “Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.” BIPS 06, October 2011. www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

Federal Transit Administration (FTA), “An Introduction to All-Hazards Preparedness for Transit Agencies,” May 2010. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/All_hazards.pdf

FTA, Office of Research Demonstration and Innovation, “Transit Security Design Considerations,” November 2004. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ftasesc.pdf

FTA, “Public Transportation System Security and Emergency Preparedness Planning Guide,” January 2003. https://www.transit.dot.gov/oversight-policy-areas/public-transportation-system-security-and-emergency-preparedness-planning

FTA, “Sensitive Security Information (SSI): Designation, Markings, and Control,” March 2009. https://www.transit.dot.gov/oversight-policy-areas/sensitive-security-information-ssi-designation-markings-and-control-march

FTA, “Transit Agency Security and Emergency Management Protective Measures,” November 2006. https://www.transit.dot.gov/oversight-policy-areas/transit-agency-security-and-emergency-management-protective-measures-november

FTA, “Traveler Information Systems and Wayfinding Technologies in Transit Systems,” March 2016. https://www.transit.dot.gov/research-innovation/traveler-information-systems-and-wayfinding-technologies-transit-systems

General Services Administration, “US General Services Administration Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings.” https://www.gsa.gov/cdnstatic/GSA_Testing_Standard.pdf

Mineta Transportation Institute, “Generic Continuity of Operations/Continuity of Government Plan for State Level Transportation Agencies,” CA-MTI-11-1080, 2011. http://transweb.sjsu.edu/PDFs/research/1080-COOP-COG-Transportation-Plan.pdf

Transit Cooperative Research Program, “Cybersecurity in Transit Systems,” 2022. https://doi.org/10.17226/26475

Transit Cooperative Research Program, “Transit Security Preparedness,” 2020. https://doi.org/10.17226/25764

National Cooperative Highway Research Program, “Update of Security 101: A Physical Security and Cybersecurity Primer for Transportation Agencies,” 2020. https://doi.org/10.17226/25554

National Cooperative Highway Research Program, “A Guide to Emergency Management at State Transportation Agencies,” 2020. https://doi.org/10.17226/25557

Transit Cooperative Research Program, “Practices to Protect Bus Operators from Passenger Assault,” 2011. https://doi.org/10.17226/14609

Transit Cooperative Research Program, “Public Transportation Passenger Security Inspections: A Guide for Policy Decision Makers,” 2007. https://doi.org/10.17226/23150

National Cooperative Highway Research Program and Transit Cooperative Research Program, "Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies," 2005. https://doi.org/10.17226/13553

Transit Cooperative Research Program, "K9 Units in Public Transportation: A Guide for Decision Makers," 2002. https://doi.org/10.17226/24721

Transportation Research Board, "Deterrence, Protection, and Preparation: The New Transportation Security Imperative," Special Report 270, 2002. https://doi.org/10.17226/11369

National Transit Institute (NTI), "The Mark," 2012. https://www.youtube.com/watch?v=uJHvrPB1ck0

NTI workplace safety courses. www.ntionline.com/courses/list.php?program_id=5

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.

TSA/Federal Transit Administration, "Security and Emergency Preparedness Action Items for Transit Agencies," 2016. https://www.transit.dot.gov/oversight-policy-areas/security-and-emergency-preparedness-action-items-transit-agencies

Underwriters Laboratory, "Standard for Bullet-Resisting Equipment," UL 752, 2005. https://www.shopulstandards.com/ProductDetail.aspx?productId=UL752_11_S_20050909

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

Definitions

access control: An aspect of security that often uses hardware 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.

all-hazard preparedness: Integrated planning and capability-building for safety, security and emergency management to optimize and continuously improve the use of resources and the management of risks from hazards, threats, vulnerabilities and adverse events or incidents for transit agencies.

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

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 of and incidence of crime, as well as an improvement in the quality of life.

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 using small hand tools (hammer, drills, electric power tools, etc.) or by using a specific tactic to bypass a security system.

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

evacuation: Organized, phased and supervised dispersal of people from dangerous or potentially dangerous areas.

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.

forced entry: Entry to a denied area achieved through force to create an opening in fencing, walls, doors, etc., or to overpower guards.

layers of protection: Using concentric circles extending out from an area to be protected as demarcation points for different security strategies.

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

notification: Capability to provide real-time information to all building or asset occupants or personnel in the immediate vicinity of the building or asset during emergency situations.

public access area: An area of a facility where public access is not restricted or prohibited.

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

restricted area: An established area requiring a higher degree of security to protect sensitive and/or high-value assets kept therein.

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

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

sensitive security information: Information about security, operations, facilities or other assets or capital projects whose disclosure would be detrimental to the security of transit employees or customers.

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

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

target hardening: Using physical barriers or changes in a location to reduce the opportunity for crime and to make the completion of a crime more difficult.

threat: 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.

Abbreviations and acronyms

AASHTO	American Association of State Highway and Transportation Officials
ACS	access control system
ASIS	American Society for Industrial Security
BASE	Baseline Assessment for Security Enhancement
CFR	Code of Federal Regulation
COOP	continuity of operations
CPTED	crime prevention through environmental design
CPU	central processing unit
DHS	Department of Homeland Security
ECS	emergency call stations
EOP	emergency operations plan
ESS	electronic emergency system
FTA	Federal Transit Administration
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
ESS	electronic system security
FTA	Federal Transit Administration
HVAC	heating, ventilation and air conditioning
IDS	intrusion detection system
NPRA	National Petrochemical & Refiners Association
NTAS	National Terrorism Advisory System
NTI	National Transit Institute
PIR	passive infrared
SAI	Security Action Items
SMPM	Security Manpower Planning Model
SSI	Sensitive Security Information
SSP	system security plan
TSA	Transportation Security Administration
TSGP	Transit Security Grant Program
TSI	Transportation Safety Institute
VIPR	Visible Intermodal Prevention and Response
VSS	video surveillance system

Summary of document changes

- Combines contents from the following five (previously independent) standards and recommended practices: “Security Considerations for Public Transit” (2013), “Security Planning for Public Transit” (2013), “Physical Security for Public Transit” (2013), “Security Operations for Public Transit” (2013), and “Equipment and Technology” (2013).
- Assorted changes to modernize standard contents.

Document history

Document Version	**Working Group Vote**	**Public Comment/ Technical Oversight**	**Rail CEO Approval**	**Policy & Planning Approval**	**Publish Date**
First published	—	—	—	—	March 26, 2013
First revision	June 29, 2022	December 1, 2022	March 6, 2023	March 31, 2023	May 23, 2023

Appendix A: Physical Security Doors

Exterior doors

Exterior doors may be weak points in the protected structure due to their service and functional requirements. 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 should provide a level of protection equal to the level of protection provided by a facility's associated walls, floors and ceilings to be effective. Door systems should withstand a certain amount of pressure from the identified threat such as direct force, prying, frame spreading, explosion, vandalism or firearms, and for a specific time under the identified threat or attack. Likely threats should be identified in the planning phase.

Depending on their specific function, exterior doors may be embedded with safety glazing, wired glass and louvers. The appropriate fire-resistant classification should be identified and included in the design as required by fire-life-safety codes. Intrusion detection systems (IDS), video surveillance systems (VSS) (formerly known as closed-circuit television systems) and/or access control systems (ACS) should be designed with door system features in mind. Similarly, transit agencies should prescribe similar designs for interior doors protecting high-value or critical assets.

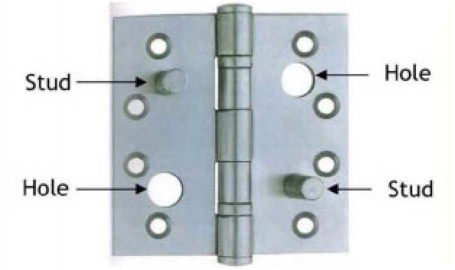
In coordination with IDS, all exterior doors should be clearly marked with numbers corresponding to an appropriate alarm zone to assist responding police and security with rapid identification of potential adversaries. Front and rear facility doors should be marked with the facility's address, on or above the doors. Peepholes or cameras should be included to enhance surveillance of the facility's exterior entrances from the inside. To ensure that all doors are illuminated during darkness, they should be 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.

To prevent removal of exterior doors from the hinge side, install hinges on the interior; provide concealed hinges; use security hinges with nonremovable 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 (see **Figure 9**).

FIGURE 9
Hinge Hardware Protection



High-risk-area doors may require ballistic protections against adversary actions to penetrate the opening (see **Table 2)**. Exterior doors without glazing that require ballistic-level protection should be specified using industry standard ballistic level protection ratings (Underwriters' Laboratory Physical Security: Ballistics).

TABLE 2
Hingle 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)

Industrial doors

Industrial door designs are typically roll up, coiled gates or sliding security grilles manufactured of steel, aluminum and/or stainless steel. Glass or composite 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.

Industrial door design should complement the structural integrity of the facility envelope. Further, they should provide a level of protection against threats identified in the transit agency's security risk assessment.

Appendix B: Windows

Window systems are a combination of glazing, anchorage, frames, supporting walls and connections to the building's structure on the exterior façade. Balanced window system designs help ensure that 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 3**.

TABLE 3
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
Full thermal tempered	Medium	Fractures into small cube-shaped fragments
Polycarbonate	High	Typically, none

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 10**). 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 4**).

FIGURE 10
Window Glazing Performance

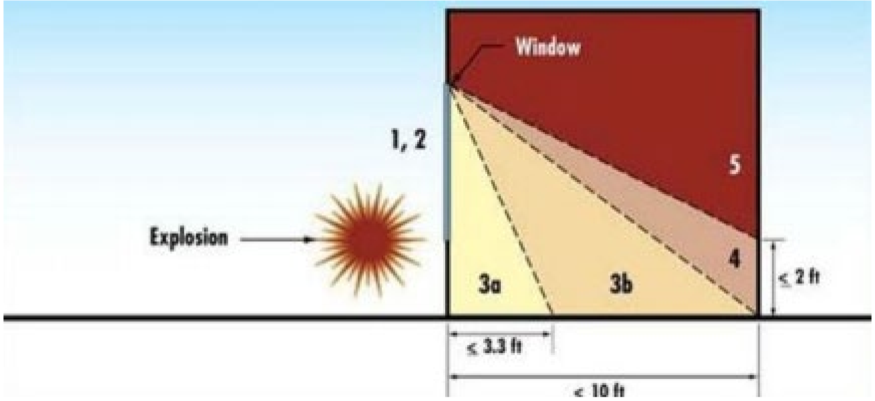


TABLE 4

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 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 not more than 10 ft from the window at a height of no greater than 2 ft above the floor.	Low	High

While replacement of vandalized vehicle glass windows is a viable option, it can also be a costly expense for transit agencies. Commercially available products can control and reduce incidents of graffiti vandalism (aka "scratchitti") to glass surfaces on public transportation vehicles, ranging from heat treatments to multilayered protective films. 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.

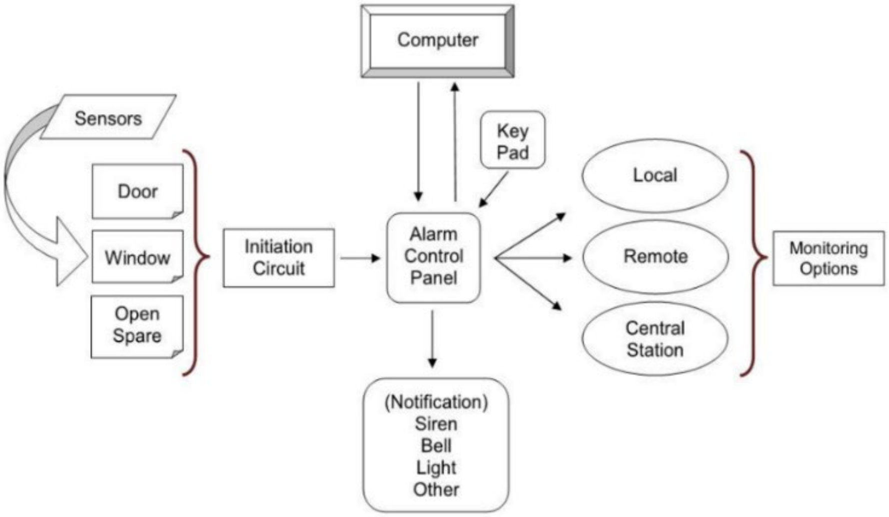
Appendix C: IDS and Sensors

Sensors are devices that are used to detect and monitor events or activities in protected areas under various conditions. They detect changes that occur to the specific operating conditions for the area they protect (door, window, etc.). There are numerous detection sensors available that offer monitoring and detection capabilities. Sensors have interior and exterior applications and can be active or passive, covert or visible, volumetric or line sensing. Specifically:

- Active sensors transmit a signal and detect a change in the signal; passive sensors only receive energy to generate a signal.
- Passive sensors simply detect energy emitted in the proximity of the sensor; they do not produce a signal from the transmitter.
- Covert sensors are hidden from view, whereas visible sensors are openly displayed and may act as visual deterrents to an adversary.
- Volumetric sensors can detect motion in designated detection zones, as well as larger rooms, closets and other interior spaces or areas, while line sensors detect intrusion in specific areas of the designated detection zone.

Detection sensor application should be designed, specified and tailored based upon the assessed risks. The purpose of IDS is to detect intrusions into protected areas, but these systems may be adversely impacted by the environment, weather, seismic events, natural hazards, wildlife and other conditions related to device location. These items should be assessed and understood prior to IDS selection, design and implementation.

FIGURE 11
Basic IDS Sequence



The following definitions relate to the basic IDS sequence shown in **Figure 11**:

- **Initiation circuit:** Any event or action that results in an alarm device initiating an alarm status, such as a pull station, a volumetric sensor, a door switch, etc.
- **Computer:** The computer is the central hub of an IDS. It provides monitoring, display, acknowledgement and control capabilities of the protected zone alarm sensor points.
- **Alarm control panel:** An alarm control panel is the system's main component. It operates either in a standalone or in a networked mode. It is designed to accept input from various detection sensors and to monitor their circuitry for abnormal operation. Generally, control panels have connections for

power supplies, batteries, bell outputs, programmable outputs, communication buses and a fixed number of input zones for connecting the detection devices. The battery backup for the IDS is typically located in the alarm control panel.

- **Keypad:** The keypad enables commands to be entered into the alarm control panel (user codes, silencing alarms, arming and disarming zones, etc.). It also provides system status, such as violated devices or zones, trouble signals, etc. Keypads may use a sound—such as a bell, chime or buzzer—to provide notice of a change in the state of the system. Keypads should be placed in areas that are readily accessible by the user, typically at the primary entrance to an area. Most systems allow multiple-unit keypad installation at multiple entrances or where they can be monitored by response personnel.
- **Notification:** Notifications are preset options designed to indicate an alarm status in a protected zone by way of an audible or visual device. Notification of an alarm status may include, but is not limited to, siren, lights, bells and other devices.
- **Monitoring:** ESS systems are most effective when monitored by exception in real time. This means that alarm monitoring system settings should be programmed to cause an alarm annunciation when an undesirable act takes place. Rapid response to activities or events in real time can provide a return on investment for a transit organization by addressing alarms as they occur. The typical types of alarm status monitoring follow:
  - **Local alarms** are simple alarms. Typically, they are installed on the exterior of the structure and are used for low-value assets. With this method, alarms initiate audible and/or visible signals, often at the facility or building where the IDS are installed. Local alarm annunciation relies on security or police patrols, passersby or building occupants returning to the structure to acknowledge the alarm status.
  - **Remote monitoring of systems** consists of alarm activations being monitored, transmitted to and annunciated at a local (contracted) security company or local police dispatch center that also records the alarm annunciation. A contracted service or a formal agreement with local police may be required to ensure monitoring and response.
  - **Central-station monitoring** includes proprietary devices and circuits that are automatically signaled to, recorded at, maintained by and supervised from an agency's owned central location with operators who monitor the system continuously. This type of monitoring is typically performed by contractors and/or in-house agency staff.

Interior sensor nomenclature

Type	Passive (P) or Active (A)	Covert (C) or Visible (V)	Volumetric (V) or Line (L)
Boundary Penetration Sensors			
Electromechanical	P	C	L
Infrared	P/A	V	L
Vibration	P	C	L
Capacitance	P	C	L
Fiber optic	P	C/V	L
Interior Motion Sensors			
Microwave	A	V	V
Infrared	P	V	V
Proximity Sensors			
Capacitance	P	C	L
Pressure	P	C	L
Fiber optic	P	V/C	L

Interior sensor challenges

VL: Very Low **L:** Low **M:** Medium **H:** High

Type	Wind	Temp	RH	Small Animals/ Wildlife	Electrical Interfere Lighting	Power	Radio Freq.	Seismic
Boundary Penetration Sensors								
Active glass break	L	VL	VL	VL	L	L	L	L
Continuity	VL	VL	VL	VL	VL	VL	VL	VL
Simple magnetic switch	VL	VL	VL	VL	L	L	L	L
Balanced magnetic switch	VL	VL	VL	VL	L	L	L	L/M
Passive ultrasonic	M	L	L	M/H	L	L	L	L
Vibration	L/M	L	L	L	L	L	L	H
Fiber optic	L/M	L	VL	VL	VL	VL	VL	L/M
Volumetric Sensors								
Active sonic	M	L	L	L	L	L	L	L
Microwave	L	L	L	M	M	M	M	L
PIR	L	H	L	M	M	M	M	L
Ultrasonic	L	L	M	M	M	M	M	L
Video motion	L	L	L	M	M	M	M	L
Proximity Sensors								
Capacitance	L	L	M	M	M	L	L	L/M
Pressure	L	L	L	L	L	L	L	L
Fiber optic	L	L	L	M	VL	VL	VL	M

Exterior sensors nomenclature

Type	Passive (P) or Active (A)	Covert (C) or Visible (V)	Line of Sight (LOS) or Terrain Following (TF)	Volumetric (V) or Line (L)
Buried Line				
Seismic pressure	P	C	TF	L
Magnetic field	P	C	TF	V
Ported coaxial cable	A	C	TF	V
Fiber optic cable	P	C	TF	L
Fencing Associated				
Fence disturbance	P	V	TF	L
Sensor fence (taut wire)	P	V	TF	L
Electric fence	A	V	TF	V
Freestanding				
Active infrared	A	V	LOS	L/V
Passive infrared	P	V	LOS	V
Bi-static microwave	A	V	LOS	V
Dual technology	A	V	LOS	V
Video motion detection	P	C	LOS	V

Exterior sensor challenges

VL: Very Low **L:** Low **M:** Medium **H:** High **VH:** Very High

Sensor Type	Wind	Rain	Standing Water/ Runoff	Snow	Fog	Small animals	Large animals	Small Birds	Large Birds	Lightning	Overhead Power Lights	Buried Power Lines
Fence-mounted	H	M	L	L	VL	L	M	L	L	L	VL	VL
Taut wire	VL	VL	VL	VL	VL	VL	L	VL	VL	VL	VL	VL
Electric field	M	LH	VL	M	VL	M	VH	L	M	M	L	VL
Capacitance	M	M	VL	M	VL	M	VH	L	M	M	L	VL
Ported cable	VL	M	H	L	VL	VL	M	VL	VL	M	VL	L
Seismic/pressure	M	L	L	L	VL	L	VH	VL	VL	L	L	M
Seismic/magnetic	M	L	L	L	VL	L	VH	VL	VL	H	M	H
Microwave	L	L	MH	LM	L	MH	VH	VL	M	LM	L	VL
Infrared (IR)	L	L	L	M	M	M	VH	L	M	L	VL	VL
Video motion	M	L	L	L	MH	L	VH	VL	M	L	L	VL

Appendix D: Emergency Call Stations

ECS provide ridership with a direct link from a point within the transit environment to a security operator. They may be scheduled to operate during specific days, hours or times via a controller or timer, and specific means of communication may also vary based on availability within a planned service area or areas. For example, ECS can be designed to communicate via landline phone service, cellular tower service, two-way radio, Voice over Internet Protocol (VoIP), Wi-Fi VoIP (wireless) or over a 900 MHz bandwidth. At a minimum, the following functional capabilities should be considered in the design of an ECS:

- Backup power and communication sources to ensure continuous ECS operation and connectivity during utility and service outages
- Call-back (aka ring-back) function to reconnect and communicate with the caller’s site in the event of a disconnected or dropped call

Additionally, various options may be available when considering requirements for an ECS. They may include cameras, audio siren, auto dial, continuously open microphones, synchronization with other ECS cameras to capture different angles and images of the area, signs designating the location of ECS devices, etc. If a VSS option is designed into the ECS, then cameras should be installed to synchronize their fields of view to the area of the activated ECS site to verify the caller, the nature of the call, the site, activities around the caller, etc. An agency should always consider the indigenous languages spoken and other means of communications used in the communities they serve to ensure that the services and instructions of an ECS are well-understood and that their locations are clearly identified.

Due diligence should precede any proposed procurement and installation of security equipment and technology by an agency. For example, an agency should first complete a security risk assessment to determine if a requirement exists for the equipment and technology to be installed at their properties. Then, a site survey should be completed to identify other requirements at the site, such as the Americans with Disabilities Act, OSHA requirements, local codes or ordinances, enablers (ridership volumes and pedestrian circulation) or challenges, utility service, installation location(s), etc. Finally, operation testing of functions should be performed before acceptance of the equipment and technology and its commissioning into service.

ECS policies and procedures should be prepared, exercised and implemented to validate an accurate, timely and effective response.