APTA STANDARDS PROGRAM
RECOMMENDED PRACTICE

APTA SS-ISS-RP-006-23
First Published: July 25, 2023

APTA Transit Infrastructure and Systems Security Working Group

Security Plan

Abstract: This recommended practice provides guidance to assist transit agencies in developing and implementing a standalone Security Plan.

Keywords: security, Security Plan

Summary: This recommended practice provides guidance and describes the core components for a transit agency Security Plan. Transit agencies should use Security Plans to facilitate informed security decision-making for their operations, assets, passengers, employees and communities. Ultimately, a Security Plan enables agency personnel to proactively manage security incidents or emergencies.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the APTA Transit Infrastructure and Systems Security Working Group, as directed by the APTA Security Standards Policy and Planning (SSPP) Committee.

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.

This is a new document.

APTA Standards

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **APTA Transit Infrastructure and Systems Security Working Group**, which provided the primary effort in the drafting of this document. At the time this standard was completed, the working group included the following members:

Lurae Stuart, *WSP USA,* Chair
Mark Uccardi, *Booz Allen Hamilton,* Vice Chair

Aldon Bordenave, *LA Metro*
Ryan Chelski, *Sound Transit*
Neil Crosier, *King County Metro*
Matthew Dimmick, *STV*
Dean Fajerski, *TSA*
Kevin Franklin, *Bay Area Rapid Transit*
BJ Johnson, *New Orleans RTA*
Stephan Parker, *Transportation Research Board*
Jacob Peltier, *Community Transit*
John Plante, *METRA*
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Charles Rappleyea, *WSP USA*
Harry Saporta, *WSP USA*
Jill Shaw, *Dallas Area Rapid Transit*
Kirsten Tilleman, *WSP USA*

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

Introduction

This introduction is not part of APTA SS-ISS-RP-006-23, "Security Plan."

APTA recommends the use of this document by:

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

Scope and purpose

The primary goal of this document is to provide clear and straightforward direction to a transit agency to develop, implement, evaluate and maintain a standalone Security Plan. Transit agencies should possess both a Security Plan and an emergency preparedness plan (also known as an emergency response or emergency operations plan). When combined, these documents are considered the Security and Emergency Preparedness Plan (SEPP). However, agencies should consider standalone Security Plans so that emergency planning components can be shared where appropriate.

A secondary goal is to minimize the agency time and effort needed to prepare and implement a Security Plan while maintaining the document's clarity and comprehensiveness. The implementation includes having the Security Plan approved and supported by management and staff, and continuing security-related activities as identified. The audience for this recommended practice is the person or team responsible for developing and implementing the Security Plan. Typically, this is a member of the agency's security team, usually the security director or appointee. This document is simply one approach and is meant as a guide. If an agency decides that another process is a better fit, then that process should be used to ensure success.

Security Plan

1. Overview

Public transportation agencies face many security threats that have the potential to disrupt transit operations, cause harm to transit customers and employees, damage public and private property, and create significant economic losses. Conducting and documenting formal security planning ensures that public transportation agencies leverage resources for managing security risks.

The Security Plan should establish a comprehensive, systematic framework to safeguard the security of people (transit agency customers, employees and members of the public) and infrastructure (vehicles, rights-of-way, equipment, facilities and cyber systems). The Security Plan should also be designed to foster a culture of security within the transit agency by assigning responsibility and accountability for security.

Transit agency employees, contractors and passengers are considered the first line of defense against criminal or terrorist activities, as these individuals will most likely be the first to witness or identify criminal or suspicious behavior within a transit agency's operations. It is critical to the success of the security program that all employees, contractors, passengers or other parties who may come into contact with its operations and services become and remain actively involved in the security program. Security-related roles and responsibilities, as well as activities conducted to improve security readiness, are assigned to personnel in a Security Plan.

1.1 Sensitive security information

A transit agency Security Plan should comply with the Transportation Security Administration, state safety oversight agencies and any security grant information security requirements. In particular, TSA designates transit agency Security Plans as sensitive security information (SSI). For this reason, all Security Plans must comply with the SSI marking requirements as found in 49 CFR Part 15 and 49 CFR Part 1520.

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

1.2 Relationship between SEPPs and safety

Transit agencies should possess both a Security Plan and an emergency preparedness plan (also known as an emergency response or emergency operations plan). When combined, these documents are considered a Security and Emergency Preparedness Plan (SEPP). However, agencies should consider standalone Security Plans so that emergency planning components can be shared where appropriate.

Regardless of whether these two plans are separate or combined, they establish a comprehensive, systematic management structure to enable security, prevention, protection, mitigation, response and recovery activities. Security and emergency preparedness plans should be reviewed annually and updated if needed. Similarly, the transit agency's Agency Safety Plan (ASP) is a companion document to the Security Plan. Both Security Plan and ASP address the control of system risk, but from the perspective of intentional harm and unintentional harm, respectively. The safety management system (SMS) principles in the ASP can be applied to the management of system security. Certain aspects of security are required in the ASP. Appendix A details the relationships among safety, security and emergency preparedness plans.

See APTA SS-SRM-RP-001-09, “Development and Implementation of a Security and Emergency Preparedness Plan (SEPP),” for more information about developing and implementing a SEPP.

2. Security Plan components

Transit agency security personnel should engage in a collaborative planning process with security stakeholders to achieve comprehensive security planning that achieves the transit agency’s requirements. The following recommended Security Plan components may provide a baseline level of security. Appendix B includes a sample table of contents for a Security Plan.

2.1 Overview

The first core section of a transit agency Security Plan should provide foundational information about the agency and the plan.

2.1.1 Purpose

Security Plans should contain a statement describing the reason for establishing the plan, noting its importance in proactively managing security risks. Transit agencies may consider applying the following sample purpose statement:

> The purpose of the [Transit Agency] Security Plan is to achieve the highest reasonable level of security by developing and communicating a comprehensive, systematic, responsive and effective security management program. This Security Plan documents our security management strategy, goals and objectives, which includes security roles, responsibilities and activities. This Security Plan also supports the implementation of security technology programs, outlines security training and exercises, and describes coordination with internal and external security stakeholders.

2.1.2 Scope

The scope of the Security Plan should be applicable to all transit agency modes of operations and departmental activities, including operations, maintenance, planning and design, construction, procurement, testing, and training. The Security Plan should also encompass any contracted operations by defining the security requirements for the contracted operators. An example scope is below:

> The Security Plan applies to all [Transit Agency] staff, including contractors and subcontractors working on the [Transit Agency] transit system. It is applicable to all bus, rail and paratransit services, including operations, maintenance, planning and design, construction, procurement, testing, and training.

2.1.3 From the chief executive officer

The Security Plan should include a policy statement from the agency’s chief executive officer or equivalent. The statement is a commitment to fully support the security program and should complement and not conflict with similar safety and emergency management policy statements. The statement should also direct responsibility for implementing and administering the Security Plan and is the basis to implement security roles, responsibilities and procedures. In addition to the signature of the CEO, signatures from the management executive team and security lead may be included to further indicate support from executive management. The policy statement could include safety and security or include a standalone security statement, as shown in the example below.

> [Transit Agency], in support of its mission to provide safe and secure transit services, has developed this Security Plan as a means of integrating security measures and initiatives into and throughout all levels of the organization. This Security Plan describes the policies, procedures, roles and responsibilities to be fulfilled by all employees and contractors, beginning with the highest levels of management.
>
> To ensure that the Security Plan is fully implemented and administered, [Position Responsible for Plan Implementation and Administration] has been appointed as the security lead for [Transit Agency].
>
> All personnel and contractors are required to adhere to the policies, procedures and requirements of the Security Plan and to properly and diligently perform the security-related functions of their jobs. Further, the [Transit Agency] management team will be continually and directly involved in formulating, reviewing and revising security policies, procedures, goals and objectives.
>
> Effective implementation and administration of our Security Plan will improve the overall security of our transit operations and services. To achieve this goal, all employees are encouraged to report potential threats and vulnerabilities identified within the system to their direct supervisors. All employees are also encouraged to provide assistance, as necessary, to ensure that potential threats and vulnerabilities are eliminated or controlled.
>
> ____________________________________ ____________
>
> Chief executive officer   Date

2.1.4 Goals and objectives

The ultimate goal of a security program is to achieve the highest reasonable level of security appropriate to the agency. The Security Plan should identify the goals developed to achieve the purpose established for the Security Plan. Goals are broad statements for achievement for the security program, endorsed by top management, and are supported by specific objectives to aid in their attainment. Goals should be realistic and generally are presented in qualitative terms. See an example below:

1. <u>Security:</u> Mitigate security vulnerabilities and threats against the transit agency to the lowest practical level.
2. <u>Security awareness and involvement:</u> Engage all transit employees and contractor personnel in a program of security awareness activities to ensure that they serve as “eyes and ears” for the system. Also establish a similar process of engagement in awareness activities for passengers and others who come into contact with the system.
3. <u>System approach:</u> Systematically and continually identify and assess threats and vulnerabilities and mitigate security risks to the system, optimizing use of human resources, operating procedures, technology and equipment, facilities design and improvements, and community and interagency partnerships to maximize security effectiveness.

Objectives are the means by which the transit agency achieves its identified goals. Unlike goals, objectives should be quantifiable. Objectives should provide a framework for guiding day-to-day activities that provide for a safe and secure transit operation and services. Objectives are often supported by the identification of required associated tasks. See an example below:

Goals and Objectives	Associated Tasks
1. Security: Reduce the rate of crime. **1A.** Establish annual target goal for reported crimes, per 100,000 boarding rides.	**1.1** Base routine deployment and tactics of police and contracted security personnel on current intelligence, analysis of crimes and trends, and threats on the transit system.
	1.2 Fulfill perceived security and order on the transit system by security personnel deployment
2. Awareness and Involvement: Engage all employees and police/security personnel in awareness and security responsibilities. Engage transit customers and public in security awareness. **2A.** Achieve broad-based awareness of security responsibilities, alertness and procedures by transit personnel. **2B.** Achieve broad-based security alertness by transit customers.	**2.1** Communicate the security strategy to all transit agency employees and police/security personnel.
	2.2 Involve employees in security program through participation in Safety/Security Committees.
	2.3 Ensure that “If You See Something, Say Something” or similar security awareness program information is posted in all transit vehicles, transit centers and facilities, and is included in customer information materials.
3. System Approach: To maximize security effectiveness, systematically and continually identify and assess crime and other security threats to transit agency customers, employees and property. **3A.** Assess deployments and tactics of police, transit agency personnel and contracted security personnel in relation to analyzed information on crime, threats and effectiveness on customer perception of security. **3B.** Systematically integrate security design considerations and security technology and equipment into the design of facilities and transit operations.	**3.1** In coordination with police, collect and analyze crime/security data on the transit system.
	3.2 Use security technologies to optimize the effectiveness of security.
	3.3 Incorporate crime prevention through environmental design (CPTED) guidelines and Federal Transit Administration Transit Security Design Considerations into transit agency design criteria and facilities designs.

2.1.5 Management and administration

The Security Plan should identify a Primary and Alternate Security Coordinator as the primary contact for security-related activities and communications. The Security Coordinator should coordinate security practices and procedures with appropriate law enforcement and emergency response agencies.

The Security Coordinator should review and update, if needed, the Security Plan at least annually. Updates may be required in the event of:

- security incidents that necessitate changes to the security strategy or tactics
- new transit facilities, infrastructure or operating environment, or changes to any of these
- organization changes or function reassignments
- changes to applicable federal or state regulations
- changes to security threats or vulnerabilities
- identification of gaps or shortcomings following a security audit, drill or exercise

See example language below:

> The Security Coordinator has the responsibility for the annual review and revision of the Security Plan. Plan updates consider outcomes and lessons learned from security incidents or changes to the transit operating environment, including but not limited to new facilities or new transit routes, organizational changes and reassignment of functions, changes in applicable federal or state regulations, changes in security threats or vulnerabilities as identified in threat and risk assessments, and detection of any gaps or shortcomings following a security incident, audit, drill or exercise.
>
> If updates are required, a written summary that explains the proposed revisions are submitted to [names of individuals or group responsible for approving updates] for review and approval. If no update is necessary, a written summary is submitted to [names of individuals or group responsible for approving updates] stating that a review was conducted, that personnel and contact information was validated, and that no update is necessary.

2.1.5.1 Security audits and reviews

The Security Plan objectives should be periodically evaluated through internal audits and reviews. Audits are periodic checks to confirm, on an ongoing basis, that a suitable and sufficient security management system is implemented and effective.

Audits and reviews serve the following purposes:

- Identify changes in operations or resources that necessitate updating the SSP.
- Determine whether security measures and procedures are adequate.
- Ensure that the security measures and procedures are being implemented effectively.
- Identify those areas needing additional attention and, as a result, offer suggestions for improvement to either fine-tune the security program or to implement new objectives in a revised SSP.

Approximately one-third of the Security Plan performance objectives and security program elements should be audited each year, such that all security performance objective areas and program elements will have been completed within a three-year cycle.

2.1.6 Compliance

State safety oversight requirements vary by jurisdiction, and transit agencies should confirm compliance with their SSO.

3. Transit system

The next section of a transit agency Security Plan should describe the system, structure and stakeholders.

3.1 System description

The general system, organization and operational information that describes the transit agency should be included in this section of the plan. As shown below, a table could be added to include ridership figures (annual, weekly, daily), routes and lines, fleet size, etc. Other modes (e.g., ferry) should be added as applicable.

	Rail	Bus	Paratransit	Total
Stops and routes				
Routes/lines				
Stops/stations				
Park-and-rides				
Ridership				
Average weekday ridership				
Average weekend ridership				
Annual ridership				
Annual vehicle miles				
Annual trips taken				
Fleet and operators				
Vehicles				
Vehicle operators				

3.2 Organizational structure

Transit agencies may have internal security personnel (e.g., security staff, transit police, security committees, outsourced security guards, contracted security services) that deal strictly with transit security issues. A description of those personnel, positions and responsibilities should be included in this section.

3.3 External stakeholders

The interface between the transit agency and other local, state and federal governmental agencies exists on all levels. These interfaces and relationships ensure that communications are ongoing and that the development and implementation of various security-related activities occur, including exercises, simulations, drills and training. Such information regarding interface between any federal, state/local and law enforcement agencies should be included here.

3.4 Agency risk tolerance

In this section, agencies should define their security risk tolerance levels. Each agency has its own risk tolerance level that is typically established through its risk acceptance program. This would include who within the agency has the ability to accept risk on behalf of the agency. Often elevated or undesirable levels of risk require some type of executive-level acceptance, whereas lower levels of risk can be accepted by lower or technical levels within the agency. It is important to understand that reducing security risk requires the application of resources, either staffing or physical measures. The level or tolerance for the agency should directly relate to investments in mitigations or controls that transit agencies implement to manage risk.

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

4. Security program elements

Security program elements are the combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying security requirements in a timely and cost-effective manner. The following sections provide elements to include in a transit agency Security Plan.

4.1 Coordination among emergency personnel

The Security Plan should incorporate command and control procedures, including chain of command, and specify decision-makers and roles and responsibilities of all local partners (e.g., first responders) in case of an emergency. This section should address information sharing, coordination, communications planning, and memoranda of understanding/memoranda of agreement supporting all-hazard preparedness.

4.1.1 External support organizations/mutual aid agreements

In this section, transit agencies should include a list of external stakeholders with which the agency maintains MOUs and MOAs. MOUs/MOAs with external stakeholders offer support with an established plan and framework that allows the transit agency to plan for, source, acquire, use and in some cases provide other resources. As shown below, a table could be added for tracking all MOUs/MOAs.

Organization	Contact Information	Agreement Description	Expiration Date

4.1.2 Security input in other agency plans

Security staff should provide input into other agency plans (e.g., site emergency plan, continuity of operations plans) and should ensure that plans align with the Security Plan.

4.2 Designating and handling SSI

Transit agencies should describe how the agency creates and maintains an SSI policy and program to protect and safeguard sensitive information. See “Sensitive Security Information Best Practices Guide for Non-DHS Employees and Contractors” provided by TSA for more information about SSI recommendations and requirements. Also see APTA SS-ISS-RP-003-23, “Sensitive Security Information Policy,” for more information.

4.3 Security risk management

In this section, transit agencies should identify a system-wide security risk assessment process to determine the exposure of the system’s people, assets, operations and infrastructure. A risk-based approach that factors threat, vulnerability and consequence should be used for this purpose. Transit agencies should complete system-wide security risk assessments to determine the threats, vulnerabilities and consequences to their overall systems and properties. The assessment should compare and assess all agency transit modes, assets and facilities that make up the system. Alternatively, when transit agencies want to determine risk to a specific site or asset, they should perform a site-specific security risk assessment.

Security risk assessments should be evaluated and updated at least every three years or when a new threat arises, an incident occurs, or an agency significantly changes assets or policies. Reevaluating and updating assessments confirms that they adequately address the security risks faced by the agency and provide the basis to allocate resources to reduce risks.

The risk assessment process should include the following:

- Identify the critical assets.
- Identify the threats.
- Identify the vulnerabilities.
- Identify the likelihood of an attack/incident.
- Identify the consequences/impacts of an attack/incident.
- Assign the initial risk index to determine the basis for risk decision criteria.

- Identify potential mitigation measures/countermeasures.
- Determine residual risk acceptability.

4.4 Crime and security data analysis

Recognizing crime and security issue trends for transit agencies is pivotal to preventing security incidents. Transit agencies should include a section that identifies agency protocols for recording crime and security data, data storage locations and personnel who analyze the data. The Security Plan should also describe how the transit agency analyzes data resulting from security incidents to assess the effectiveness of mitigations.

Additionally, partnering with state or local fusion centers may help provide further insight into crime and security trends in the transit agency's area. Fusion centers serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between state, local, tribal and territorial (SLTT); federal; and private sector partners.

4.5 Safety and security certification

In this section, transit agencies should describe their safety and security program. Many transit agencies self-certify the safety and security of their facilities and operations and safety-significant modifications prior to the initiation of service or major change. This process is typically part of the agency's existing program for system safety and security and is integrated through a Safety and Security Certification (SSC) program, documented in a Safety and Security Certification Plan (SSCP). SSC activities support analysis that reduces the need for expensive retrofitting to correct hazards or vulnerabilities after the system is placed in revenue service. Certification also typically supports improved integration of operational considerations into project design. Related regulations are described in 49 CFR 270.103(S), 49 CFR 673.27 and FTA Circular 5800.1.

4.6 Security capabilities and procedures

In this section, the Security Plan should include internal security practices or procedures that all employees and contractors must fulfill. Specific components should cover personnel identification and access control, the personnel hiring and termination process, procurement, and security awareness. Most requirements are directed toward the transit agency's employees and contractor staff; however, some of these requirements apply to subcontractors, vendors, building tenants, visitors and patrons.

4.7 Security protective measures and capabilities

The Security Plan should outline strategies to address crimes and other security issues that may occur on the agency's transit system. Transit agency Security Plans should address, at a minimum, the following security concerns:

- loitering
- operator and transit personnel harassment and assaults
- unlawful transit conduct
- non-destination riders
- terrorist activity
- workplace violence
- passenger harassment and assaults
- theft of personal items
- vandalism of transit vehicles and at passenger facilities
- fare evasion measurement and management
- vehicle theft and break-ins at park-and-ride lots
- bomb threats
- drug and alcohol use

Documented protective measures to mitigate security issues typically include the following:

- **Security staffing:** Internal and external personnel resources to observe, assess and respond to security events. Examples may include high-visibility patrols and K-9 teams.
- **Security technologies:** Security technologies to restrict access, assess, observe and respond to security events, and to capture forensic and evidentiary evidence for criminal events. Examples include surveillance platforms, access control systems, personal protective equipment and alarms.
- **Hardening:** Physical measures to protect facilities and infrastructure from attack. Examples may include reinforced walls or doors and barriers and berm fencing.
- **Plans and procedures:** Documented and exercised procedures to report and manage security events. Examples may include lockdown procedures and altering operations.

4.8 Physical security and hardening

This section of the Security Plan should identify physical security and access control measures the transit agency will use to prevent unauthorized entry to perimeters and facilities. Transit agencies may also consider adding a weapons and other prohibited items policy.

See APTA SS-SIS-RP-010-13, "Security Considerations for Public Transit," for more information about physical security recommendations and requirements.

4.9 Cybersecurity

In this section, the Security Plan should identify measures the transit agency will implement to protect its electronic data and information. Measures should include efforts to limit access to sensitive information, conduct an asset inventory, make passwords complex, and establish and implement physical and cyber access control policies. Other recommended measures include maintaining a secure off-site backup of all computer-generated data and establishing and implementing cyber reporting policies. The Security Plan should include and/or reference the agency's Cybersecurity Plan to confirm alignment.

See APTA SS-ESC-RP-001-14, "Cybersecurity Considerations for Public Transit," for more information about cybersecurity recommendations and requirements. Moreover, the Cybersecurity & Infrastructure Security Agency's Shields Up and Cyber Essentials websites have multiple actions and recommendations to mitigate cybersecurity risks.

5. Training and exercises

In this section of the Security Plan, transit agencies should document training and exercises and include the agency's approach for conducting and addressing evaluations, which may include after-action reviews and after-action reports.

5.1 Security training

In this section, transit agencies should document security training for all employees and contractors, capturing initial and refresher training requirements. All employees should be trained in security awareness and observing, assessing and reporting procedures, while additional training will apply to specific roles. The Security Plan should also document policies for retaining training records.

Transit agencies should also identify all necessary safety and security certifications required or recommended for employees. The system safety and security discipline manages hazards and vulnerabilities throughout the life cycle of a project, program or activity through a committed approach to risk management. Certification for safety and security verifies application of this discipline for transit projects. Through this process, hazards and vulnerabilities are translated into risks, which are then analyzed, assessed and prioritized, and then resolved, accepted or tracked.

Furthermore, on March 23, 2020, TSA published the *Security Training for Surface Transportation Employees Final Rule*, which requires transit agencies covered by this rule to develop a comprehensive security training program and provide security training to employees in security-sensitive positions, among other requirements.

See APTA SS-SRM-RP-005-12, “Security Awareness Training for Transit Employees,” for more information about training recommendations and requirements.

5.2 Security exercises

In this section, a transit agency Security Plan should document agency participation in discussion- and operations-based exercises and include those conducted by the agency, as well as those organized by partners. A Security Plan should include schedules, partners, and descriptions of exercises, as well as record retention policies.

See APTA SS-SEM-S-004-09, “Transit Exercises,” for more information about developing, conducting and evaluating exercises.

5.3 Public safety awareness and education

Periodic public outreach campaigns should be conducted to educate the public in crime prevention and awareness programs to keep themselves and their belongings and vehicles (at park-and-rides) safe and secure. “If You See Something, Say Something” or similar security promotions may be used to promote and heighten the public’s awareness of transit security issues.

Transit agencies may also consider creating customized public awareness campaigns to tailor messaging to systems, issues and riders.

6. Levels of protection and alerts

In this section, a transit agency Security Plan should clearly state the levels of protection based on threats received from federal, state and local partners to enable risk-based escalation of security operations. Partners, including law enforcement, fusion centers and DHS, often provide information on intent and capability of a threat. It is important to have each threat level defined and transparency in the reasoning behind the rating.

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

6.1 National Terrorism Advisory System (NTAS)

The Department of Homeland Security uses the National Terrorism Advisory System to communicate current developments, general trends, and/or specific, credible information about a terrorist threat through alerts and bulletins. These alerts provide timely, detailed information to the public. Transit agencies should be aware of all notifications from NTAS, as they may necessitate the implementation of reactionary security procedures.

6.2 Public Transit Information Sharing and Analysis Center (PT-ISAC)

Transit agencies should regularly review information disseminated by the Public Transportation Information Sharing and Analysis Center. PT-ISAC is a trusted, sector-specific entity that provides to its constituency a 24/7 Security Operating Capability that established the sector’s specific critical information/intelligence requirements for incidents, threats and vulnerabilities. This security information-sharing resource for the public transit community allows users to share unclassified security and threat information and establish relationships and network with both private and public transportation security officials. PT-ISAC provides the nation, including the transit security community, a “one-stop shop” to aid in its efforts to maintain vigilance and readiness to prevent terrorism in the mass transit and passenger rail environment.

6.3 Homeland Security Information Network (HSIN)

Transit agencies should regularly review information disseminated by the Homeland Security Information Network. HSIN is the Department of Homeland Security’s official system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international and private-sector partners. Mission operators use HSIN to access Homeland Security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe.

Related APTA standards

APTA SS-ESC-RP-001-14, “Cybersecurity Considerations for Public Transit”
APTA SS-ISS-RP-003-21, “Sensitive Security Information Policy”
APTA SS-SEM-S-004-09, “Transit Exercises”
APTA SS-SIS-S-017-21, “Security Risk Assessment Methodology for Public Transit”
APTA SS-SIS-RP-010-13, “Security Considerations for Public Transit”
APTA SS-SRM-RP-001-09, “Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)”

References

American Public Transportation Association Information Sharing & Analysis Center (PT-ISAC). https://www.apta.com/research-technical-resources/safety-security/information-sharing-analysis-center-pt-isac/

Code of Federal Regulations, 49 CFR Part 15. https://www.ecfr.gov/current/title-49/subtitle-A/part-15

Code of Federal Regulations, 49 CFR Part 1582 – Public Transportation and Passenger Railroad Security. https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-D/part-1582

Department of Homeland Security, “Developing and Maintaining Emergency Operations Plans,” September 2021. https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf

Department of Homeland Security, Fusion Centers website. https://www.dhs.gov/fusion-centers

Department of Homeland Security, National Terrorism Advisory System website. https://www.dhs.gov/national-terrorism-advisory-system

Federal Transit Administration, “Handbook for Transit Safety and Security Certification,” November 2002. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/SSC.pdf

National Academies of Science, Transit Cooperative Research Program, “Measuring and Managing Fare Evasion,” 2022. https://nap.nationalacademies.org/catalog/26514/measuring-and-managing-fare-evasion

Transportation Security Administration, “Surface Transportation Security Training.” https://www.tsa.gov/for-industry/surface-security-training-rule

Transportation Security Administration, “Sensitive Security Information.” https://www.tsa.gov/for-industry/sensitive-security-information

Abbreviations and acronyms

ASP	Agency Safety Plan
CPTED	crime prevention through environmental design
DHS	Department of Homeland Security
FTA	Federal Transit Administration
HSIN	Homeland Security Information Network
MOA	memorandum of agreement
MOU	memorandum of understanding
NTAS	National Terrorism Advisory System

PT-ISAC	Public Transit Information Sharing and Analysis Center
SBU	Sensitive But Unclassified
SEPP	Security and Emergency Preparedness Plan
SLTT	state, local, tribal and territorial
SMS	safety management system
SSC	Safety and Security Certification
SSCP	Safety and Security Certification Plan
SSI	sensitive security information
SSO	state safety oversight
TSA	Transportation Security Administration

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	Rail CEO Approval	Policy & Planning Approval	Publish Date
First published	January 13, 2023	March 30, 2023	May 31, 2023	June 30, 2023	July 25, 2023

Appendix A: Safety management system component relationships

TABLE 1
Alignment Among Safety, Security and Emergency Preparedness Plans

SMS Component	Safety Plan	Security Plan	Emergency Preparedness Plan
Policy, Goals and Objectives	Defines the fundamental approach, goal and objectives, and organizational structure for managing safety.	Defines the fundamental approach, goal and objectives, and organizational structure for managing security.	Defines the fundamental approach, goal and objectives for requiring responsive action to protect life, property and/or the environment.
Risk Management	Hazard identification, assessment, evaluation and control to an acceptable or tolerable level.	Threat and vulnerability identification, evaluation and mitigation.	Threat and vulnerability identification, evaluation and mitigation of natural disasters and human-made events.
System Assurance	• Safety data collection and analysis • Incident/accident investigation • Safety reviews and audits	• Security data collection and analysis • Event and security breach investigation • Security reviews and audits	• Data collection and analysis • Post-event assessments • Emergency management procedures, including integration with city/county/ state resources • Drills and exercises • Audits
Promotion	• Employee competency training • Safety public education and awareness	• Employee awareness training • Security public education and awareness	• Emergency preparedness awareness and training • Employee response training

Appendix B: Sample Security Plan table of contents