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

APTA SS-SIS-RP-011-13
Approved March 26, 2013
Infrastructure Security Working Group

# Security Planning for Public Transit

**Abstract:** This document proposes recommended practices for security planning at transit passenger facilities to enhance the security of people, operations, assets and infrastructure.

**Keywords:** assessment, balanced security, considerations, planning, security program

**Summary:** This *Recommended Practice* provides planning strategy and background information. It offers an overview and description of the applicability of the planning pillar. It discusses how to integrate planning with other security standards and best practices used by transit agencies to enhance their security program(s).

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

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

## Participants

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

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

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

Bill Pitard, *PB-Heery Americas*
Gabriela Amezcua, *CTA*
John Plante, *CTA*
Brian Taylor, *Halifax*
Charles Rappleyea, *CATS*
Rick Gerhart, *FTA*
Chris McKay, *TSA*
Jevon D'Souza, *TSA*
David Hahn, *APTA*
Allen Smith, *SPAWAR*
Mark Mahaffey, *VTA*
Brad Baker, *MBTA*
Eric Hartman, *OCTA*
Harry Saporta, *TriMet*
Gardner Tabon, *RPTA*
Ken Cummins, *Sound Transit*
Brad Baker, *MBTA*
Gary Gordon, *TSA*

# Contents

# Security Planning for Public Transit

## 1. Introduction

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

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

**TABLE 1**
APTA Security Standards Program Documents

| APTA Number | Document Title |
|---|---|
| APTA SS-SIS-RP-001-10 | "Security Lighting for Transit Passenger Facilities" |
| APTA SS-SIS-RP-002-10 | "Security Lighting for Nonrevenue Transit Passenger Facilities" |
| APTA SS-SIS-RP-003-10 | "Fencing Systems to Control Access to Transit Facilities" |
| APTA SS-SIS-RP-004-10 | "Chain Link, Mesh or Woven Metal Fencing Systems to Control Access to Transit Facilities" |
| APTA SS-SIS-RP-005-10 | "Gates to Control Access to Transit Facilities" |
| APTA SS-SIS-RP-006-10 | "Ornamental Fencing Systems to Control Access to Transit Facilities" |
| APTA SS-SIS-RP-007-10 | "Crime Prevention Through Environmental Design for Transit Facilities" |
| APTA SS-SIS-RP-008-10 | "Bus Stops Design and Placement Security Considerations" |
| APTA SS-SIS-RP-001-12 | "Anti-Vehicle Barriers for Public Transit" |

## 2. Planning pillar overview

The planning pillar is created by incorporating some or all elements of any one or several pillars together into a system that provides a uniform approach to applying a security solution. When effectively applied, these elements provide an agency with guidance or direction to mitigate risk and plan a balanced and effective security program. Adversaries target people, operations, assets and infrastructure in the transit environment. To reduce the risk from these threats, the effective implementation of security planning should be considered.

Examples of similarly structured *Recommended Practice* documents that describe a broad scope of infrastructure security and derivative topics are described in Table 1. Other Security Standards Program documents are also listed as resources herein to aid the development of a balanced security program and should be used where applicable by accessing APTA's Security Standards and Recommended Practices page at www.aptastandards.com/Documents/PublishedStandards/Security/tabid/329/language/en-US/Default.aspx.

## 2.1 Stakeholder considerations

Transit agencies should understand and buy into transit security planning to enhance the security posture of the environment(s) where they must operate. To the extent possible, the application of any or all of the topics of this *Recommended Practice* should be considered to assist agencies to meet their security program requirements and enhance their safe operations.

## 2.2 Benefits

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

- Fosters transit domain awareness (TDA).
- Creates pride of ownership by transit users and employees.
- Ensures transit employees, operators and first responders an understanding of response procedures.
- Enables the transit agency the opportunity to coordinate with federal, state, county, tribal and local host area government partners.
- Enhances the safety and security experience of its ridership within the transit environment.

# 3. Security risk assessment

Transit agencies should complete a systemwide security risk assessment to determine exposure to their systems' people, assets, operations and infrastructure. A risk-based approach that factors threat, vulnerability and consequence should be used to assess transit systems. The findings should be used to select security measures that mitigate risk to and enhance the protection of people, assets, operations and infrastructure. For more information regarding various security risk assessment methodologies, see:

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

# 4. Security planning strategies

The security planning pillar delineates security-specific program information and functions. For instance, mandated security planning for security operations (see cited References) that outline measures agency staff and employees are to take during certain events or incidents; staffing requirements, posts or positions that should be filled are identified; the contents of an agency's security awareness training program may be described; and guidance for implementing security outreach for operator and ridership preparedness, as well as providing signage and wayfinding guidance.

## 4.1 Types of planning guides and other documents

### 4.1.1 Transit domain awareness (TDA)

A key component of an active, layer-protected and balanced security program, TDA is the effective understanding of activities within or associated with the transit domain that could impact the security, safety, economy or environment of an agency. TDA is supported by other agency planning, some of which are described below.

### 4.1.2 System Security Plan (SSP) (49 CFR, Part 659)

When applicable, the state oversight agency shall require rail transit agencies to implement an SSP that, at a minimum, complies with the requirements of 49 CFR, Part 659.21 and the oversight agency's program standard. The SSP must be developed and maintained as a separate document and may not be part of the rail transit agency's system safety program plan. The state oversight agency may prohibit a rail transit agency from publicly disclosing the system security plan. After approving the SSP, the state oversight agency shall issue a formal letter of approval, including the checklist used to conduct the review, to the rail transit agency. The SSP must at a minimum do the following:

- Identify the policies, goals and objectives for the security program endorsed by the agency's chief executive.
- Document the rail transit 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.
- Identify controls in place that address the personal security of passengers and employees.
- Document the rail transit agency's process for conducting internal security reviews to evaluate compliance and to measure the effectiveness of the system security plan.
- Document the rail transit agency's process for making its system security plan and accompanying procedures available to the oversight agency for review and approval.

### 4.1.3 Rail Transportation Security (49 CFR, Part 1580)

When applicable, light-rail transit systems operating on track that is part of the general railroad system of transportation are required to allow the Transportation Security Administration (TSA) to inspect, to appoint a rail security coordinator and to report significant security concerns.

### 4.1.4 Security emergency preparedness planning (SEPP)

The SEPP ensures a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events. The SEPP should contain guidance on internal security, incident management systems and external plans for coordinating with local law enforcement, other local responders, local planning agencies, and state or federal agencies. While this section emphasizes planning for terrorism, basic principles and concepts are applicable to all emergency situations. The SEPP process at a minimum should address the following:

- System security and emergency preparedness program introduction
- Background and history of the system
- Mission statement and system security policy
- SEPP program description
- Threat and vulnerability identification, assessment and resolution
- Implementation and evaluation of the SEPP
- Modification of system security plan
- Department of Homeland Security regulations and requirements relevant to the SEPP

- Acronyms
- Definitions

### 4.1.4.1 Policies and procedures

Further, security program planning should include some or all of the below policies and procedures as elements of a balanced security program (where applicable). The following resources are available from APTA's Security Standards Program website at www.aptastandards.com/Documents/PublishedStandards/Security/tabid/329/language/en-US/Default.aspx:

- "Conducting Nonrevenue Vehicle Security Inspections"
- "Conducting Background Investigations"
- "Random Counterterrorism Measures on Transit Systems"
- "Conducting Revenue Vehicle Security Inspections"
- "Random Inspections of Carry-On Items in Transit Systems"
- "Sensitive Security Information"
- "Continuity of Operations Plan"
- "First Responder Familiarization of Transit Systems"
- "Security & Emergency Management Aspects of Special Event Service"
- "Developing a Contagious Virus Response Plan"
- "Shelter of Transit Vehicles and Nonrevenue Equipment During Emergencies"
- "Creating an Alternate or Backup OCC"
- "Safe Mail and Package Handling"
- "Emergency Communication Strategies for Transit Agencies"
- "Participating in Mutual Aid"
- "Responding to Threat Condition Levels"
- "Operational Strategies for Emergency Smoke Ventilation in Tunnels"

### 4.1.5 TSA/FTA Security and Emergency Management Action Items for Transit Agencies

Security and Emergency Management Action Items for Transit Agencies (SEMAI) at http://transit-safety.volpe.dot.gov/security/securityinitiatives/ActionItems/default.asp aims to elevate security readiness throughout the public transportation industry by establishing baseline measures for any transit agency to employ. The SEMAI is dynamic, with regular review and coordination between the federal government and the transit community, and updated as necessary to ensure that the recommended measures address current security realities.

Compliance with the SEMAI is voluntary. However, each SEMAI addresses current security threats and risks that confront transit agencies today, with particular emphasis on priority areas where gaps need to be closed in security and emergency preparedness programs. The SEMAI list provides improved guidance for their implementation and assessment to be incorporated into transit agency operations. An outline of the transit security program elements covered by the SEMAI is described in **Table 2**. A detailed listing is described in Appendix A.

**TABLE 2**
TSA/FTA Security and Emergency Management Action Items for Transit Agencies

| Program Element | Action Item(s) |
|---|---|
| Management and Accountability | 1–4 |
| Security and Emergency Response Training | 5 |
| Homeland Security Advisory System (HSAS)[1] | 6 |
| Public Awareness | 7 |
| Drills and Exercises | 8 |
| Risk Management and Information Sharing | 9–11 |
| Facility Security and Access Control | 12 and 13 |
| Background Investigations | 14 |
| Document Control | 15 and 16 |
| Security Audits | 17 |

1. Program renamed National Terrorism Advisory System (NTAS) by Department of Homeland Security.

### 4.1.6 Transit Agency Security and Emergency Management Protective Measures

Described below are several suggested categories for planning security and emergency management protective measures for transit agencies (www.fta.dot.gov/documents/ProtectiveMeasures.pdf). The protective measures are organized by transit agency security and emergency management function as the basis for developing and deploying specific implementation procedures. They are candidate actions, not requirements. Planning to implement procedures and processes should be determined by a transit agency in light of local and regional needs, conditions, capital and operations budgets, and operating environment. The protective measures are not intended to be exhaustive, and not all of the protective measures may be appropriate for every transit agency. **Table 3** provides a starting point for the categories included in the security planning process.

**TABLE 3**
Protective Measure Planning Scope

| Section | Category | Scope |
|---|---|---|
| 1.0 | Information & Intelligence | Information & intelligence gathering includes threat and vulnerability information collection and analysis, sharing information with and getting information from local, regional and federal sources such as DHS and the FBI. |
| 2.0 | Security and Emergency Management | All aspects of creating, updating, and executing the security and emergency management plans and procedures for the transit agency. |
| 3.0 | Regional Coordination | Participation of the transit agency in the region, including regional emergency response plans, relationships with other security-related organizations in the region and first responders, and conducting regional drills and exercises. |
| 4.0 | Information Technology and Communications Systems | All aspects of creating, updating, and executing the information system plans and monitoring and operating the communications equipment for the transit agency. |
| 5.0 | Employee and Public Communications | All aspects of creating, updating, and executing the employee and public information communications plans for the transit agency. |
| 6.0 | Contingency and Continuity Plans | All aspects of creating, updating, and executing the transit agency's contingency and continuity of operations plans for emergency incidents/events within the transit system and in the region. |

### 4.1.7 Crime Prevention Through Environmental Design Site Survey

Crime Prevention Through Environmental Design (CPTED) is a process that can assist a transit agency in designing crime-enabling elements out of a transit built environment. A site survey should be performed to identify and understand the environment where the transit system operates to incorporate CPTED principles into the security program planning process. At a minimum, a site survey should be completed and include locating and identifying:

- crime statistics and data in areas hosting a transit system component;
- access and egress points;
- multi-storied building critical structural, lighting, hazardous material storage, elevated structures, columns, and load-bearing walls, walkways, glass walls, and doors and windows; and utilities and services;
- environmental conditions;
- confined areas, such as: alcoves, passageways, tunnels, etc.;
- critical infrastructure; and
- areas adjacent to or in proximity to utilities such as HVAC, electrical panels, communications equipment, gas lines, fire life safety systems, high-pressure steam, and other subsystems.

Documented best practices in transit CPTED should be reviewed for appropriate incorporation in the design.

### 4.1.8 An Introduction to all-hazards preparedness for transit agencies

All-hazards preparedness planning for transit agencies includes a risk prioritization and management process to effectively allocate resources to continually reduce safety, security and emergency management risks and to prevent, protect, control and mitigate incidents and adverse events. The cited all-hazard preparedness resource document provides transit agencies with an explanation, a high-level process, and illustrative examples for applying an all-hazard preparedness approach consistent with the national guidance on all-hazards preparedness described in the National Preparedness Guidelines.

### 4.1.9 Continuity of operations

A transit agency’s Continuity of Operations Plan (COOP) should be planned and developed to provide essential agency functions following a significant emergency event that limits or restricts the availability of personnel, facilities or technical systems. The COOP is a specific component of a transit agency’s overall Emergency Operations Plan (EOP). While the EOP is an organized approach to emergency management including a concept of operations during, pre-, trans- and post-emergency situations, the COOP is very specific to the recovery and restoration aspects of emergency management. The COOP focuses on restoring limited operating capability, usually within a 12-hour time frame and for a period of up to 30 days. Beyond 30 days, it is assumed that an agency will have re-established a degree of normality.

### 4.1.10 Sensitive Security Information (SSI): Designation, Markings, and Control, Resource Document for Transit Agencies (49 CFR, Parts 15 and 1520)

Sensitive security information (SSI) is information about security, operations, facilities or other assets or capital projects whose disclosure would be detrimental to the security of transit employees or customers. Essential transit agency security program planning must include the designation, markings and control of SSI. By law, transit agencies are required to categorize and protect SSI. Protecting SSI means restricting its distribution and controlling access to it. By law, SSI is not subject to disclosure under the Freedom of Information Act (FOIA) or state “sunshine laws.” It is also not available under discovery in civil litigation, and it is not required to be part of the record in a federal rulemaking.

Transit agencies should use this guidance as a resource in planning and developing policies and procedures for identifying, marking and handling SSI in order to control access to it. To the extent practical, agencies should integrate the designation, marking and handling of SSI into their existing security program procedures.

### 4.1.11 National Terrorism Advisory System (NTAS)

NTAS alerts will be issued by the Department of Homeland Security (DHS) only when credible information is available (Appendix B). These alerts will include a clear statement that there is an imminent threat or elevated threat. NTAS alerts will be based on the nature of the threat: In some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels. During periods of an elevated sector NTAS threat alerts, transit agencies should implement protective measures that are tailored to the NTAS threat. For example:

- Remove all non-blast-resistant trash receptacles transit facilities.
- If unable to remove, secure the receptacle’s aperture in place to prevent its use
- Non-blast-resistant trash receptacles and recyclable containers that cannot be removed should be secured from use.

Transit agencies should refer to the References section (below) for guidance to develop responses to credible NTAS alerts and threats.

### 4.1.12 Additional security planning and other documents

Security planning has applicability with a broad range of transit agency functions. When required, security planning should be incorporated with other transit agency planning, events, or evolutions, such as:

- capital improvement projects;
- continuity of operations;
- emergency operations;
- wayfinding and signage;

- security design criteria; and
- other relevant agency security planning.

## 5. Training considerations

The Transportation Safety Institute (TSI) and the National Transit Institute (NTI) each offer transit-specific training courses that include information about several of the above security planning documents.

## 6. Maintenance considerations

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

# Appendix A: TSA/FTA Security and Emergency Management Action Items (SEMAI) for Transit Agencies

| Item | Action |
|---|---|
| 1 | Establish written system security programs and emergency management plans. |
| 2 | Define roles and responsibilities for security and emergency management. |
| 3 | Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control. |
| 4 | Coordinate Security and Emergency Management Plan(s) with local and regional agencies. |
| 5 | Establish and maintain a Security and Emergency Training Program. |
| 6 | Establish plans and protocols to respond to the DHS National Terrorism Alert System (NTAS) threat levels. |
| 7 | Implement and reinforce a Public Security and Emergency Awareness program. |
| 8 | Conduct tabletop and functional drills. |
| 9 | Establish and use a risk management process to assess and manage threats, vulnerabilities and consequences. |
| 10 | Participate in an information sharing process for threat and intelligence information. |
| 11 | Establish and use a reporting process for suspicious activity (internal and external). |
| 12 | Control access to security-critical facilities with ID badges for all visitors, employees and contractors. |
| 13 | Conduct physical security inspections. |
| 14 | Conduct background investigations of employees and contractors. |
| 15 | Control access to documents of security-critical systems and facilities. |
| 16 | Develop a process for handling and access to sensitive security information (SSI). |
| 17 | Audit program. |

# Appendix B: National Terrorism Advisory System

The National Terrorism Advisory System, or NTAS, replaced the color-coded Homeland Security Advisory System (HSAS). This new system will more effectively communicate 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.

It recognizes that Americans all share responsibility for the nation's security and should always be aware of the heightened risk of terrorist attack in the United States and what they should do.

After reviewing the available information, the secretary of Homeland Security will decide, in coordination with other federal entities, whether an NTAS alert should be issued. NTAS Alerts will be issued only when credible information is available.

These alerts will include a clear statement that there is an imminent threat or elevated threat. Using available information, the alerts will 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.

## Sunset provision

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.

## References

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

American Public Transportation Association *Recommended Practices*:
APTA SS-SIS-RP-001-10, "Security Lighting for Revenue Transit Facilities"
APTA SS-SIS-RP-002-10, "Security Lighting for Nonrevenue Transit Facilities"
APTA SS-SIS-RP-003-10, "Fencing Systems to Control Access"
APTA SS-SIS-RP-004-10, "Chain Link, Mesh, or Woven Fencing Systems to Control Access"
APTA SS-SIS-RP-005-10, "Gates to Control Access"
APTA SS-SIS-RP-006-10, "Ornamental Fencing Systems to Control Access"
APTA SS-SIS-RP-007-10, "Crime Prevention Through Environmental Design for Transit Facilities"
APTA SS-SEM-RP-004-09, "General Guidance on Transit Incident Drills and Exercises"
APTA SS-SRM-RP-001-09, "Security and Emergency Preparedness Plan" (SEPP)
APTA-SS- SEM-RP-001-08, "Recommended Practice for a Continuity of Operations Plan"

American Society for Industrial Security (ASIS), "International Glossary of Security Terms." www.asisonline.org/library/glossary/index.xml

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

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

Electronic Code of Federal Regulations, Title 49 – Transportation, Part 659 – Rail Fixed Guideway Systems; State Safety Oversight. http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title49/49cfr659_main_02.tpl

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

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

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

FTA, "Sensitive Security Information (SSI): Designation, Markings and Control, Resource Document for Transit Agencies" (2009). http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=968

FTA, "Transit Agency Security and Emergency Management Protective Measures" (2006). http://transit-safety.volpe.dot.gov/publications/security/ProtectiveMeasures/PDF/ProtectiveMeasures.pdf

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

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

National Transit Institute (NTI), Terrorist Activity Recognition and Reaction. www.ntionline.com/courses/courseinfo.php?id=128

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

Transportation Security Administration / Federal Transit Administration, “Security and Emergency Management Action Items for Transit Agencies.” www.tsa.gov/assets/pdf/mass_transit_action_items.pdf Rail PAX

Transportation Research Board (TRB), “Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies” (2006). www.trb.org/Main/Blurbs/156474.aspx R

## Definitions

**all-hazard preparedness:** An 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.

**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.

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

## Abbreviations and acronyms

| | |
|---|---|
| **APTA** | American Public Transportation Association |
| **AASHTO** | American Association of State Highway and Transportation Officials |
| **ASIS** | American Society for Industrial Security |
| **CFR** | Code of Federal Regulation |
| **COOP** | Continuity of Operations |
| **CPTED** | Crime Prevention Through Environmental Design |
| **DHS** | Department of Homeland Security |
| **FTA** | Federal Transit Administration |
| **FEMA** | Federal Emergency Management Agency |
| **FOIA** | Freedom of Information Act |
| **HSAS** | Homeland Security Advisory System |
| **NPRA** | National Petrochemical & Refiners Association |
| **NTAS** | National Terrorism Advisory System |
| **NTI** | National Transit Institute |
| **SEMAI** | Security and Emergency Management Action Items |
| **SEPP** | Security and Emergency Preparedness Plan |
| **SSI** | Sensitive Security Information |
| **SSP** | System Security Plan |

| | |
|---|---|
| **TDA** | Transit Domain Awareness |
| **TRB** | Transportation Research Board |
| **TSA** | Transportation Security Administration |
| **TSI** | Transit Safety Institute |