APTA STANDARDS PROGRAM
RECOMMENDED PRACTICE

APTA SS-ISS-RP-007-24
First Published: Jan. 23, 2024
APTA Security Risk Management Working Group

Security Measures for Elevated Threats

Abstract: This recommended practice provides transit agencies options and considerations for selecting, implementing and evaluating security measures for elevated threats.

Keywords: elevated threats, protective measures, security measures

Summary: This recommended practice provides transit agencies a comprehensive menu of security measures to consider when confronting elevated threats. Transit agencies should review and assess options based on each agency's unique environment and threat intelligence, identifying risk-based measures and planning implementation prior to an elevated threat.

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 Infrastructure and Systems Security Working Group (ISSWG) 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.

Table of Contents

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*
Stephan Parker, *Transportation Research Board*
Jacob Peltier, *Community Transit*
John Plante, *METRA*
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Diana Rawles, *Denver RTD*
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-007-24, "Security Measures for Elevated Threats."

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 understand options for security measures for elevated threats. By assessing and planning security measures prior to the existence of a heightened threat environment, transit agencies can be better prepared to implement security measures and strengthen preparedness capabilities.

Security Measures for Elevated Threats

1. Overview

Public transportation agencies face various 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. Furthermore, threats can employ a variety of tactics, manifest differently (e.g., physical, cyber), and originate from a host of actors.

While transit agencies typically employ several security measures during day-to-day operations to reduce, protect against and counter threats and vulnerabilities, they should also be prepared to incorporate additional security measures during heightened threat environments. Depending on the nature of the elevated threat and the security environment, additional security measures should be applied for a duration that is reasonable and prudent given the nature of the threat, the quality of the information available and the agency's resources. Additionally, federal agencies may recommend and/or require transit agencies to implement particular security measures during an elevated threat to mitigate specific threats.

This recommended practice provides transit agencies security measures to consider implementing during times of elevated threats.

2. Recognizing an elevated threat

Transit agencies have many resources available to identify elevated threat environments. Transit agencies may self-identify elevated threats based on agency-developed intelligence analysis or receive awareness of elevated threats from external partners. External partners that may raise awareness of elevated threats include the Federal Bureau of Investigation, Department of Homeland Security, Transportation Security Administration, Cybersecurity and Infrastructure Security Agency, Public Transit Information Sharing and Analysis Center, and state and local law enforcement and fusion centers. Transit agencies should evaluate received threat assessments for credibility, specificity, time frames, applicability and levels of corroboration to determine their response.

2.1 National Terrorism Advisory System

The Department of Homeland Security uses the National Terrorism Advisory System to communicate current developments and general trends, as well as specific, credible information about a terrorist threat.

> **NOTE:** NTAS replaced the color-coded Homeland Security Advisory System in 2011.

NTAS uses *bulletins* to communicate current developments or general trends regarding terrorism threats and *alerts* to warn of credible terrorist threats against the United States. NTAS supplies the following two types of alerts:

- **Elevated Threat Alert:** Warns of a credible terrorist threat against the U.S.
- **Imminent Threat Alert:** Warns of a credible, specific and impending terrorist threat against the U.S.

NTAS alerts may include specific information about the nature of the threat, as well as a geographic region, mode of transportation or critical infrastructure affected. Finally, an alert may include measures that individuals and communities can take to help prevent, protect against, mitigate or respond to the threat. Transit agencies should be aware of all notifications from NTAS, as they may necessitate the implementation of enhanced security measures.

3. Security risk assessment considerations

Transit agencies should use a risk-based approach to select and implement security measures that are aligned with the agency's resources, communities and requirements. Transit agencies should maintain a current system-wide security risk assessment with recommendations to identify, evaluate and reduce risks to the system's people, assets, operations and infrastructure. Additional information about security risk assessments can be found in APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit."

4. Threat scenarios

Transit agencies should select security measures for elevated threat environments based on the assessed threat. Threats applicable to transit agencies include but are not limited to the following:

- active assailants
- arson
- improvised explosive devices (IEDs)
- hijacking
- sabotage
- standoff weapons
- vehicle ramming
- weapons of mass destruction (WMDs)

Threat scenarios may change and evolve over time. Further, it is possible that agencies may not identify all relevant threats during an assessment. These factors contribute to the need for continuous monitoring of the threat environment and risk assessments that recur on a regular basis, as determined by the agency's policies.

5. Integrated planning

Effective implementation of most security measures for elevated threats requires advanced and integrated planning among internal transit agency partners and external stakeholders. Planning for security measures should address resources, policies, legal authorities, procedures, finances, communication, coordination, options, prioritization and other considerations. Transit agencies should consider planning for elasticity in their security programs to provide for both escalating security measures if conditions warrant and reducing security measures when a threat subsides.

6. Security measures for elevated threats

The following security measures may be considered for implementation during elevated threat environments to reduce vulnerabilities and deter, detect, delay, assess and respond to adversaries. Measures that contribute to a holistic security program that can mitigate multiple threats and maintain operations should be the focus of these enhanced measures. Agencies should consider establishing a charge code to track expenses associated with implementing additional security measures.

Some measures may not be appropriate for all transit agencies or modes, and agencies should thoughtfully evaluate options based on the system's and the threat's specifics. For the purposes of this recommended practice, security measures for elevated threats are divided into the following categories:

1. Access control
2. Alarms
3. Alter operations
4. Cybersecurity
5. Evacuation, lockdown and shelter
6. High-visibility patrol
7. Intelligence, information sharing and cooperation
8. K-9 teams
9. Personal protective equipment
10. Screening and inspections
11. Surveillance
12. Training and exercises

6.1 Access control

Access control security measures restrict access to and use of critical facilities and infrastructure, security information, and high-risk areas. Security measures include the following:

- Providing additional alarms, barriers and/or physical personnel presence to further monitor, control or restrict access to identified sites, egresses or areas.
- Restricting non-passenger facilities to employees only and/or requiring visitors to have preauthorization and escorts.
- Closing public restrooms.
- Restricting access to elevators.
- Conducting inventory of and verifying employee badging.
- Limiting access to sensitive information and systems.
- Conducting an asset inventory of sensitive equipment.

6.2 Alarms

Alarms-related security measures include confirming functioning of and deploying intrusion detection systems, network monitoring systems, operation alarms, and sensors to detect and report threats. Security measures include the following:

- Confirming functioning of system alarms, remote kill switches and other related systems.
- Deploying additional alarms and/or sensors.
- Deploying or increasing monitoring of the operating status and sampling results for chemical, biological, radiological and explosives alarms and sensors.

6.3 Alter operations

Alter operations security measures include confirming operations of primary and alternate systems, as well as deliberately changing operations to address risks, reduce vulnerabilities and create uncertainty for adversaries. Security measures include the following:

- Reviewing and verifying functioning of alternate/emergency communication methods, backup plans, operations/control facilities and infrastructure, and monitoring and tracking capabilities.
- Limiting, altering and/or reducing service and/or routes to avoid high-risk areas.

- Increasing unpredictable security sweeps of transit vehicles and facilities.
- Increasing frequency of operator and system-wide announcements regarding security measures and reporting suspicious activity.
- Changing visible security procedures, such as the timing and frequency of random train, bus and facility sweeps.
- Evaluating and adjusting working schedules to provide necessary staffing levels.
- Limiting vehicle speeds to improve stopping capability.

6.4 Cybersecurity

Cybersecurity measures for elevated threats include limiting access to sensitive information, conducting an asset inventory, changing passwords, and confirming operations of primary and alternate systems. Security measures include the following:

- Conducting an updated cybersecurity risk assessment.
- Confirming computer and power backup systems.
- Confirming that systems and patches are up to date.
- Changing passwords.
- Deploying internal anti-phishing campaigns.
- Limiting access to sensitive information and systems.
- Conducting an asset inventory of sensitive equipment.
- Identifying changes in baseline configurations.
- Increasing the agency’s review of system logs or the infrastructure related to the threat.
- Confirming that individuals with system ownership or responsibility are aware of their responsibilities.
- Identifying individuals who have administrative privileges and ensuring that no additional privileges have been granted.
- Increasing physical presence and patrols at critical infrastructure locations (e.g., substations, communications system nodes/hubs, data centers, signaling equipment, communications systems), as addressed in other overall system security measures.
- Ensuring availability of secondary communications system(s) should email or radios be debilitated or rendered unsecure.

See APTA-SS-ESC-RP-001-14, “Cybersecurity Considerations for Public Transit,” for more information about cybersecurity recommendations and requirements.

6.5 Evacuation, lockdown and shelter

Evacuation, lockdown and shelter measures include reviewing and practicing plans and procedures for immediate emergencies. Security measures include the following:

- Reviewing security plans, emergency action plans, evacuation procedures and shelter-in-place policies with all employees, and updating plans and procedures if required.
- Reviewing situational tactics for responding to active assailant scenarios.
- Preparing to establish perimeters, including inner and outer, to deny access to or to intercept potential assailants, and ensuring that security personnel and measures are in place at high-risk areas.

6.6 High-visibility patrol

High-visibility patrol measures include increasing the presence and visibility of security, law enforcement and operations personnel in and around transit systems. Security measures include the following:

- Increasing the presence and visibility of security, law enforcement, operations and other uniformed personnel in and around stations and stops, yards, and other critical infrastructure along routes and rights-of-way.
- Deploying uniformed transportation and/or security personnel to ride and monitor trains and/or buses.
- Requesting assistance from federal, state and local law enforcement agencies to provide uniformed personnel on transit system property.
- Conducting increased, regular and/or unpredictable security sweeps of trains and buses.

6.7 Intelligence, information sharing and cooperation

Intelligence, information sharing and cooperation measures include executive intelligence analysis and sharing capabilities with transit partners. Security measures include the following:

- Reviewing and updating identification of transit facilities, systems and infrastructure considered critical.
- Conducting security awareness briefings to all employees and security personnel, inviting local law enforcement personnel to attend.
- Ensuring that transit blueprints, floor plans and/or relevant documents are available to responding law enforcement and/or other first responders.
- Reviewing plainclothes recognition protocols by law enforcement personnel with all employees.
- Verifying points of contact with first responder personnel and reviewing response tactics to be used in the event of an attack affecting transit infrastructure and operations.
- Verifying open lines of communication with public health officials.
- Coordinating with neighboring transit agencies to enable security awareness and heightened vigilance of suspicious activity.
- Reviewing scenario-specific emergency procedures, such as hijacking and/or hostage prevention and response procedures, with transit bus system personnel and local law enforcement agencies.
- Confirming procedures to exchange threat and intelligence information with federal, state and/or local law enforcement agencies (e.g., seeking intelligence updates from a local FBI Joint Terrorism Task Force [JTTF] officer).
- Designating a primary and alternate security coordinator to coordinate with TSA and other agencies.
- Monitoring threat level communications (e.g., NTAS) from federal, state and local partners.
- Advising all transit staff and passengers to report all suspicious activity according to transit procedures.
- Designate an insider threat program coordinator to work with internal and external partners to avert insider threats
- Reporting all suspicious activity reports (SARs) to the TSA Transportation Security Operations Center; JTTF; and other relevant federal, state and local law enforcement partners.
- Coordinating public messaging with public information officers.
- Keeping employees and the public informed.
- Sending public awareness messages via social media and other system communication tools.
- Establishing a Joint Information Center to coordinate regional public information.
- Opening the transit agency’s emergency operations center.

6.8 K-9 teams

K-9 team measures include executing procedures associated with deployed canine teams. Security measures include the following:

- Using canine patrols on trains and buses, as well as at stations, stops, and critical facilities and infrastructure, if available.
- Verifying communications procedures with local explosive detection and canine response law enforcement personnel.

6.9 Personal protective equipment

Personal protective equipment measures include confirming availability and deployment of specialized gear. Security measures include the following:

- Conducting PPE refresher training, certification and medical checks.
- Confirming that PPE and portable detection equipment are fully functional and ready for deployment.
- Issuing PPE to law enforcement, operations and/or other identified staff.
- Requiring law enforcement, operations and/or other identified staff to carry PPE, such as specialized respiratory protection.

6.10 Screening and inspections

Screening measures include inspecting individuals, conveyances and systems for dangerous materials. Security measures include the following:

- Inspecting conveyances, stations and stops, and critical infrastructure under the control of the transit system for indications of sabotage or suspicious items, identifying focus areas (tracks, under-platform lip areas, etc.) based on vulnerabilities and threats.
- Conducting random inspections of passengers’ accessible property, consistent with federal, state and local laws and regulations.
- Verifying currency and validity of background investigations (initial and recurrent) for all employees and contractors with access to security information and/or critical facilities and systems.
- Deploying maintenance personnel to ride the first train each day to assist with a visual track inspection.
- Requiring transit staff to inspect each station prior to opening.
- Removing and/or securing trash receptacles.
- Removing and/or securing newspaper and other vending machines.

6.11 Surveillance

Surveillance measures include monitoring systems for dangerous and/or suspicious activity. Security measures include the following:

- Confirming video surveillance system coverage.
- Increasing monitoring of video surveillance systems.
- Deploying security, law enforcement, other personnel and/or equipment to perform surveillance at critical facilities and areas/locations of high pedestrian traffic, including terminals, stops, stations, conveyances and yards, consistent with federal, state and local laws and regulations and system policies.

- Increasing or maximizing lighting levels at transit system facilities during both revenue and nonrevenue hours.
- Requiring all employees and contractors to visibly display employer-provided identification while on transit system property or performing assigned duties.

6.12 Training and exercises

Training and exercise measures include conducting planned and emergent sessions to increase personnel and system preparedness for emergencies. Security measures include the following:

- Coordinating training and exercises with transit personnel and first responders.
- Conducting training with all transit employees to review critical and/or updated policies, processes and procedures, considering involving external stakeholders such as first responder personnel.
- Conducting discussion- and/or operations-based exercises to prepare all transit employees for potential security threats, considering involving external stakeholders such as first responder personnel.
- Implementing corrective actions and recommendations identified during exercises.
- Updating job aids, checklists, scripted messages and other material used during emergencies.

7. Evaluating security measures' effectiveness

Evaluating security measures is critical to ensuring the effectiveness of a transit system's security posture. The following approach outlines actions to assess effectiveness:

- **Define clear goals and objectives.** Transit agencies should define specific goals and objectives driving the implementation of security measures for elevated threats.
- **Identify metrics and performance indicators.** Transit agencies should identify metrics and performance indicators that will be used to measure the effectiveness of the security measures. For example, a transit agency may consider measuring the number of security incidents that occur during the deployment of security measures.
- **Collect data.** Transit agencies should collect data to assess identified metrics and performance indicators. This might involve using sensors, cameras or other monitoring equipment, as well as collecting data from passenger surveys and other sources.
- **Analyze the data.** Transit agencies should analyze collected data and information to identify patterns and trends and determine the effectiveness and impact of security measures.

Once transit systems complete their analysis, it is necessary to take action to improve the security measures. Actions may involve adjusting security protocols, increasing security personnel or making other changes to improve the security of the transit system. Evaluating the effectiveness of implemented security measures at a transit system is an ongoing process that requires careful planning, data collection, analysis and action.

Related APTA standards

APTA-SS-ESC-RP-001-14, "Cybersecurity Considerations for Public Transit"
APTA-SS-SEM-S-004-09, "Transit Exercises"
APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit"

References

Federal Transit Administration, "Transit Agency Security and Emergency Management Protective Measures," November 2006. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ProtectiveMeasures.pdf

Abbreviations and acronyms

IED	improvised explosive device
ISSWG	Infrastructure and Systems Security Working Group
JTTF	Joint Terrorism Task Force
NTAS	National Terrorism Advisory System
PPE	personal protective equipment
SAR	suspicious activity report
SDOC	Standards Program's Standards Development Oversight Council
SSPC	Security Standards Policy and Planning
WMD	weapons of mass destruction

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	Rail CEO Approval	Policy & Planning Approval	Publish Date
First published	May *6*, 2023	July 30, 2023	September 30, 2023	October 21, 2023	Jan. 23, 2024