APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

APTA SS-SRM-RP-001-09, Rev. 2
First Published: February 18, 2009
First Revision: March 31, 2012
Second Revision: September 25, 2012

Infrastructure & Systems Working Group (ISSWG)

Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)

Abstract: This recommended practice describes the process by which a Security and Emergency Preparedness Plan (SEPP) may be developed, implemented and evaluated. A SEPP establishes a comprehensive, systematic management structure to safeguard personal security of passengers, employees and members of the public, as well as for the protection of physical assets and other property. The SEPP also is designed to foster a culture of security by assigning responsibility and accountability for security.

Keywords: emergency preparedness, security plan, security template, SEPP

Summary: This recommended practice describes the process by which a Security and Emergency Preparedness Plan may be developed, implemented and evaluated.

Scope and purpose: The primary goal of this document is to provide clear and straightforward direction to a transit agency to develop, implement and evaluate a SEPP. A secondary goal is to minimize the time and effort needed to prepare and implement the SEPP while maintaining the document's clarity and comprehensiveness. The implementation includes having the SEPP approved and supported by management and staff, sharing the SEPP with local transit and emergency management agencies, and continuing the security-related activities as identified in the SEPP. The audience for this recommended practice is the person or team responsible for developing and implementing the SEPP. Typically, this person 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.

Table of Contents

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Infrastructure & 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, Chair
Mark Uccardi, Vice Chair

Galen Bennett, *Sound Transit*
Michael Birch, *RAPT Dev USA*
Don Burr, *Community Transit*
Ryan Chelski, *Sound Transit*
Neil Crosier, *King County Metro*
Dean Fajerski, *TSA*
Kevin Franklin, *BART*
Paul Huston, *VIA Rail Canada*
Andy Niero, *TSA*
Mark Norton, *King County Metro*
Stephan Parker, *Transportation Research Board*
Rob Pascoe, *King County Metro*
Jacob Peltier, *Community Transit*
John Plante, METRA
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Charles Rappleyea, *WSP USA*
Sean Ryan, *MTA Metro-North Railroad*
Harry Saporta, *WSP USA*
Lurae Stuart, *WSP USA*
Brian Taylor, *Halifax Regional Municipality (retired)*
Kirsten Tilleman, *WSP USA*
Peter Totten, *AECOM*

Project team

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

Introduction

This introduction is not part of APTA SS-SRM-RP-01-09, Rev. 2, "Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)."

This recommended practice provides procedures for developing and implementing a security and emergency preparedness plan. APTA recommends the use of this document by all agencies that do not currently have a written plan. Agencies that do have a written plan should consider updating it to include additional information from this document.

A template for transit agencies to develop a customized SEPP is provided in Appendix A. Contained within the template is further guidance (written in [blue text]) that has been added to guide the user in the development of the template's sections. The template also contains placeholders (written in **<<RED TEXT>>**) for the transit agency's name, logo and other personalized information. This blue and red text should be deleted or replaced on completion of the SEPP.

Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)

1. Activities

This section contains specific activities for developing, implementing and updating the SEPP. These activities are meant to be used solely as guidance. Additional activities may be needed given the uniqueness of every situation.

1.1 Development activities

The time required by an agency to develop a SEPP will vary significantly. If older versions of a SEPP have been completed and their content can be leveraged, then the time required may be lessened. Recommended development activities for a transit agency are identified in this section.

1.1.1 Prepare for the SEPP

- Consult with management to achieve initial buy-in.
- Review recommended industry security and emergency management measures (e.g., TSA/FTA Security and Emergency Management Action Items for Transit Agencies, TSA Baseline Assessment for Security Evaluation [BASE]) and determine if all agency-applicable recommendations are being addressed.
- Review state and local security regulations and guidelines.
- Collect and review relevant security documents within the agency.
- Collect information on all security-related activities (e.g., background checks, badging, termination, security sweeps, dissemination/storage of Sensitive Security Information [SSI], training, exercises, and public awareness campaigns), including SEPP-related activity done by outside agencies (e.g., police patrols on transit system).
- Collect operational information on the transit system (e.g., riders, assets, operating environment and data reported as part of the FTA's National Transit Database [NTD] reporting requirement).
- Collect transit crime statistics and trends.
- Collect methodology and results from prior security risk assessments.

1.1.2 Develop the draft SEPP

- Designate the completed SEPP as SSI.
- Draft the SEPP describing the transit system, the context of the security program and activities by entering in the transit agency's name and appropriate information in the designated/prompted places of the template in Appendix A. The SEPP reflects the current security activities and procedures of the agency's organization.
- Involve a cross-section of all agency departments in development of the draft SEPP.
- Cite related security documents that contain standard and emergency operating procedures.
- Consult with adjacent and comparable transit systems and local emergency responders in identifying joint training, exercises, emergency points of contact, etc.
- Determine if the SEPP is supportive of all aspects of any related security programs involving the transit agency (such as the TSA BASE assessment).
- Identify and remove non-applicable sections of the SEPP template.

1.1.3 Review the draft SEPP

- Distribute the draft according to SSI requirements.
- Distribute the draft to management staff or a selection of management staff for review of clarity and comprehensiveness (e.g., directors, managers, supervisors).
- Allow management to disseminate the SEPP to select employees (including selected frontline employees) or the security committee (if one exists) to determine operational practicality.
- If substantive references are made to outside agency security measures that support the transit agency SEPP, then allow subject agencies to review the draft to ensure that their activities are accurately represented.
- Provide the draft to adjacent and comparable transit systems and local emergency responders.

1.1.4 Revise the draft SEPP

- Incorporate feedback.
- Managers should provide continual feedback to the person assigned to the SEPP (e.g., changes in operational environment, introduction of new security technology).

1.1.5 Submit the completed SEPP

- Distribute the completed document according to SSI requirements.
- Distribute the completed document to management staff (directors, managers, supervisors, etc.).
- Require managers and supervisors to communicate elements of the SEPP to staff as appropriate, and resolve all questions related to the SEPP.
- Share the SEPP with transit police, local law enforcement, emergency responders and other agencies as appropriate.

This effort may not produce a complete SEPP on the first attempt. However, beginning the creation of the SEPP is important for an agency. It is recommended that an agency produce as complete a SEPP as possible in the first attempt. Mark any incomplete areas of the SEPP as “in progress” while the agency takes the time to evaluate those sections. Do not let incomplete information halt the effort of creating the SEPP; it is important to start the SEPP process. The SEPP will remain a living document, requiring periodic review.

1.2 Implementation and evaluation

To effectively carry out SEPP implementation, a timeline or schedule with specific milestones should be developed. This schedule should consider the holder (commonly referred to as the champion) of the new SEPP to have responsibilities other than those defined in the SEPP. The actual schedule will depend on various factors, including the demands on the contributors to the SEPP. It should proceed chronologically from the completion of the SEPP to the beginning of the periodic modification process and include specific dates for each task required for implementation.

The implementation process is an excellent opportunity to ensure that the SEPP effectively mitigates the security threats affecting the transit agency. The implementation of the SEPP should be continually evaluated, not just at the end of the development life cycle. A recommended list of implementation activities is identified in this section.

1.2.1 Introduction of the SEPP

- Communicate the security program and associated activities to management staff.
- Distribute a “system security” memo to all transit personnel explaining the SEPP.
- Assign new security roles and responsibilities as necessary.
- Brief transit employees about the new security procedures set forth by the SEPP.
- Initiate new security policies, programs and training.

- Have managers distribute appropriate portions of SEPP-related procedures and assignments to authorized personnel.
- Have security personnel establish frequent meetings during the initial implementation of the SEPP to make use of feedback in order to facilitate the implementation process.
- Submit the SEPP to the transit agency's parent organization if applicable.
- Submit the SEPP to the state oversight agency for approval if applicable.

1.2.2 Implement the SEPP into current operations

- Managers and supervisors should ensure that all subordinate staff understand their roles and responsibilities according to the SEPP.
- Establish a Security Committee.
- Conduct operations according to the SEPP.

1.2.3 Evaluate the SEPP's implementation

- Evaluate legacy security programs as well as new security policies, programs and initiatives.
- Have managers step back and assess the effectiveness of implementation and include feedback from frontline personnel.

1.2.4 Modify the SEPP

- Schedule an annual review for the SEPP.
- Modify the SEPP after exercises or any security incidents that reveal important lessons learned and/or the need for new, improved or changed security measures and practices.
- Modify the SEPP after any significant operational changes (e.g., line extensions or vehicle procurements).

Abbreviations and acronyms

BASE Baseline Assessment for Security Evaluation
FTA Federal Transit Administration
NATSA North American Transportation Services Association
NTD National Transit Database
SEPP Security and Emergency Preparedness Plan
SSI Sensitive Security Information
TSA Transportation Security Administration

Summary of document changes

-

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	—	—	—	—	Feb. 18, 2009
First revision	—	—	—	—	Mar. 31, 2012
Second revision	May 7, 2020	Jun 6, 2020	Jun. 22, 2020	Aug. 20, 2020	Sept. 25, 2020

Appendix A: SEPP template

This appendix provides a template for transit agencies to develop a customized SEPP. The template contains further guidance (written in [blue text]) to guide the user in the development of the template's sections. It also contains placeholders (written in **<<RED TEXT>>**) for the transit agency's name, logo and other personalized information. The template should be revised as applicable, including the deletion or addition of sections.

Please note: This blue and red text should be deleted or replaced on completion of the SEPP.

Security and Emergency Preparedness Plan (SEPP)

<<AGENCY LOGO>>

<<AGENCY NAME>>

<<RELEASE DATE>>

<<VERSION #>>

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Revision record

Revision date	Draft #	Pages/sections affected	Comments

Requests for interpretation of this document and suggestions for changes should be addressed to the person mentioned below:

<<NAME>>
<<TITLE>>
<<MAILING ADDRESS>>
<<EMAIL ADDRESS>>

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Policy statement

The **<<AGENCY NAME>>**, in support of its mission to provide safe and secure transit services, and in response to TSA and FTA's emphasis on security, has developed this Security and Emergency Preparedness Plan (SEPP) as a means of integrating security measures and initiatives into and throughout all levels of the organization. The SEPP describes the policies, procedures, roles and responsibilities to be fulfilled by all employees and contractors, beginning with the highest levels of management.

All personnel and contractors are required to adhere to the policies, procedures and requirements stated herein and to properly and diligently perform the security-related functions of their jobs. Further, **<<AGENCY NAME>>**'s management team will be continually and directly involved in formulating, reviewing and revising security policies, procedures, goals and objectives.

The security function must be supported by effective emergency response capabilities to ensure that security-related incidents involving operations and services are responded to, resolved and recovered from quickly, safely and efficiently. To this end, **<<AGENCY NAME>>**'s management will also provide leadership in promoting safety, security and emergency preparedness throughout the organization and will consistently enforce related rules, policies and procedures throughout their areas of control.

It is a goal of **<<AGENCY NAME>>**, through the effective implementation and administration of this SEPP, to take proactive measures that will improve the overall safety and security of its transit operations and services. To achieve this goal, all employees are encouraged to report potential threats, vulnerabilities and/or hazards identified within the system to their direct supervisors and/or the **<<TITLE>>**. They are also encouraged to provide assistance as necessary to ensure that potential threats, vulnerabilities and/or hazards are eliminated, mitigated or controlled.

_____	_____
Name (executive director or equivalent)	Date
_____	_____
Name (deputy director, if appropriate)	Date
_____	_____
Name (director of security, if appropriate)	Date
_____	_____
Name (director of emergency management, if appropriate)	Date

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Table of Contents

List of exhibits

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Security & Emergency Preparedness Plan (SEPP)

1. Overview

The inherently open nature of public transportation systems, the large number of people they transport each day, and the diverse and oftentimes heavily populated areas through which they operate make such systems viable targets for various criminal activities, including acts of terrorism. A long history of worldwide terrorist attacks on transportation systems has created the need for security hardening within all transportation modes including public transportation.

The Transportation Security Administration and Federal Transit Administration have responded to this heightened level of risk by increasing their emphasis on security and emergency preparedness and by developing various action items and guidelines to assist transit agencies in their efforts to prevent and prepare for such events. **<<AGENCY NAME>>** considers the development, implementation and consistent enforcement of a comprehensive Security and Emergency Preparedness Plan (referred to throughout as the security plan or SEPP) as the first step in developing an effective security and emergency preparedness program. To this end, **<<AGENCY NAME>>** has developed this security plan in accordance with the following:

- FTA Security and Emergency Management Action Items for Transit, 2014
- Transit Agency Security and Emergency Management Protective Measures, FTA, November 2006
- Guidance Document: Immediate Actions (IAs) for Transit Agencies for Potential and Actual Life-Threatening Incidents, FTA, 2004
- Public Transportation System Security and Emergency Preparedness Planning Guide, FTA, January 2003
- Baseline Assessment for Security Enhancement (BASE), TSA, 2013

This security plan emphasizes **<<AGENCY NAME>>**'s commitment to protecting the safety of its customers and employees and the security of its vehicles, equipment, facilities and other properties. Much like **<<AGENCY NAME>>**'s system safety program establishes mechanisms for identifying and addressing hazards within its operations, this security plan establishes mechanisms through which security-related threats and vulnerabilities can be identified and addressed. It is therefore the intent of **<<AGENCY NAME>>**, through the implementation, enforcement and continued development of the security plan, to incorporate security measures into all aspects of its operations and services, including business administration and maintenance activities, and to establish a comprehensive and effective security program throughout the organization.

<<AGENCY NAME>>'s 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 **<<AGENCY NAME>>**'s operations. It is therefore 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 have been assigned to personnel and parties within **<<AGENCY NAME>>**, as identified in this SEPP. Activities conducted to improve the security of its operations and services also have been documented in this SEPP.

The SEPP will be reviewed at least annually and updated as necessary to ensure that it remains up to date and consistent with federal, state and local regulations and guidelines, as well as **<<AGENCY NAME>>**'s management goals and objectives. Additionally, the SEPP will be updated whenever a significant change occurs within the organization. In hopes of continually enhancing the SEPP, management will solicit feedback from its employees, contractors and customers on a constant and ongoing basis.

1.1 Purpose

[Insert what the purpose/intent of the SEPP will be and what the document is designed to do. Modify as appropriate.]

It is the purpose of this SEPP to establish formal mechanisms through which an effective agencywide security and emergency preparedness program can be developed, implemented and maintained, working in concert with its safety program. It is also the purpose of the SEPP to establish mechanisms through which **<<AGENCY NAME>>** and its employees, contractors, passengers and other personnel can do the following:

- Appropriately identify and report threats and vulnerabilities within **<<AGENCY NAME>>**'s operations to the correct personnel and/or external parties (emergency response agencies, law enforcement agencies, etc.) so preventive actions may be implemented to eliminate, control or minimize their impact.
- Introduce solutions to minimize the transit impacts of natural (e.g., storm, flooding), technological (e.g., power outage, hazmat spill) and security-related (e.g. crime, bomb threats, terrorism) calamities.
- Address strikes that may affect the transit agency or its operations.
- Establish security and emergency preparedness program responsibilities and ensure that tasks are assigned, understood, documented and tracked in an organized and useful manner.
- Implement security policies and procedures that can be measured, audited and evaluated to determine the effectiveness of **<<AGENCY NAME>>**'s security program.
- Satisfy local, state and federal requirements and guidelines, such as those of the city of **<<CITY NAME>>** as applicable.

1.2 Goals

[Insert what the extent of the SEPP is and what it covers. Modify as appropriate.]

The SEPP represents the agency's commitment to improving and maintaining security and emergency management functions across all operations and services and is designed to incorporate security into every aspect of the organization. The scope of the SEPP therefore applies to all **<<AGENCY NAME>>** organizational units, employees and contractors. This security plan is to include all current modes of

transportation but be scalable to incorporate any new service if and when it is introduced. Some specific goals:

- Foster the development of an agencywide security program that complements the safety program.
- Heighten security awareness among all employees, contractors and passengers.
- Develop relations and coordination with local law enforcement agencies and local and state government agencies.

1.3 Objectives

[Insert what the specific objectives of the SEPP will be. Objectives are more specific and focused than goals. Modify as appropriate.]

It is the objective of the SEPP to establish policies, procedures and requirements that can be used by personnel and contractors to integrate security practices into all processes, decision making and operations. It is therefore the objective of the program, through this security plan, to achieve the following:

- Define roles and responsibilities for all personnel with regards to security and emergency preparedness.
- Develop a management structure to maintain, evaluate and modify the plan.
- Enable employees, contractors, passengers and others to identify criminal acts, suspicious activities and occurrences, or other security concerns identified within **<<AGENCY NAME>>**'s operations and to properly report and address such events.
- Solicit security concerns from employees, contractors and passengers.
- Comply with the applicable requirements of regulatory agencies, as well as all local, state and federal requirements.
- Implement an annual security review and assessment process and verify adherence to **<<AGENCY NAME>>**'s security policies, procedures and requirements.
- Administer security-related training courses to address security threats and emergency response.
- Meet or exceed security requirements in all operations, services and maintenance activities.
- Limit security incidents and effectively resolve those that do occur.
- Thoroughly investigate all incidents involving security breaches or other security-related threats or vulnerabilities.
- Thoroughly evaluate the security implications of all proposed system modifications before implementation, and ensure that system modifications do not create new security risks.
- Address items covered by the TSA/FTA Security and Emergency Management Action Items for Transit Agencies.
- Address items covered by the BASE, as applicable, that are not already included above.

1.4 Mission statement

System security is defined as "the application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the

most practical level through the most effective use of available resources." **<AGENCY NAME>>**'s management recognizes the importance of system security to operational success and expects all employees and contractors, especially frontline employees, to understand and incorporate security practices into the performance of their assigned responsibilities. The mission of **<<AGENCY NAME>>**, as developed and approved by the **<<TITLE>>**, is defined as follows:

[Add mission statement.]

1.5 Transit system description

[Insert general system and organizational information that describes the agency.]

2.1 Organizational structure

[Insert information to identify how the transit agency is organized. If applicable, identify the organization of contractors, especially those responsible for system operations. Also add the organizational structure of partnering agencies, emergency responders, etc.]

2.2 Operating environment

[Insert information describing the operating area and environment. Specifically, describe the service area, size of the area, cities/counties served, population, rate of growth, climate, etc.]

2.3 System description

[Insert a description of the transit agency's operation. Include tables as applicable. Include ridership figures (annual, weekly, daily), routes and lines, fleet size, etc., as shown in Exhibit 1.]

EXHIBIT 1
Operating Statistics, **<<YEAR>>**

	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				

2.4 Facilities description

[Insert information describing the agency's facilities. Facilities should include transit centers, stations, maintenance and storage buildings, administrative and operational control buildings, etc. Information should include function of facility, address, hours, etc.]

2.5 Connecting transit services

[Insert the name(s) of any connecting transit service. A connecting transit service is an agency that accesses the same stations or facilities, thus allowing a passenger to easily transfer from one agency to another. Ensure that the names and contact information of security and emergency preparedness points of contact are included.]

2.6 Shared assets

[Insert the name(s) of any transit service or railroad the agency shares infrastructure with (right-of-way, track, stations, etc.). Ensure that the names and contact information of security and emergency preparedness points of contacts are included.]

2.7 Memorandum of understanding (MOU)

[Insert the name(s) of any partnering transit service or emergency service providers that the agency maintains an MOU or similar agreement with. Then summarize the agreement.]

3. Security conditions, trends and capabilities

Since Sept. 11, 2001, transit agencies have placed greater emphasis on mitigating terrorism-related events. Prior to 9/11, emphasis at **<<AGENCY NAME>>** was mostly placed on general criminal activity, including criminal property damage, unruly passengers and fare evasion. With recent worldwide terrorist attacks on mass transit systems, **<<AGENCY NAME>>** is increasingly becoming more focused on anti-terrorism measures, while still maintaining its determination to prevent crime. Because terrorists are unpredictable and prefer targets that are recognized landmarks, this makes the mass transit system susceptible to such attacks.

3.1 Security incident recording

<<AGENCY NAME>> records all criminal activity that takes place on the system. Much of what the agency records is also reported to the National Transit Database (NTD) on a periodic basis and can be found on its website. **<<AGENCY NAME>>** completes a standardized report that identifies all significant security incidents involving transit agency staff, contractors, patrons, equipment or facilities. This standardized form including the crime results from the previous calendar year is shown as Exhibit 2.

EXHIBIT 2
Reported Transit Crimes, **<<YEAR>>**

Security Incident		Number of Occurrences
Terrorism-related incidents	Bomb threat	
	Bombing	
	Chemical/biological/radiological/nuclear (CBRNE) release	
Other system security incidents	Arson	
	Sabotage	
	Hijacking	
	Cybersecurity event	
Other personal incidents	Aggravated assault	
	Burglary	
	Employee assault	
	Fare evasion[1]	
	Forcible rape	
	Larceny/theft	
	Homicide	
	Motor vehicle theft	
	Robbery	
	Suicide	
	Trespassing[1]	
	Vandalism[1]	

1. Report only those incidents that result in arrest.

3.2 Security incidents trend analysis

<<AGENCY NAME>> has developed internal metrics to facilitate trend analysis. The results of the analysis can assist the agency in allocating resources and supporting security enhancements and fixed site improvements. Using the annual standardized form, **<<AGENCY NAME>>** records all significant security incidents on a year-by-year basis to identify trends in criminal activity. The results of the analysis are contained in Exhibit 3.

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

EXHIBIT 3

Transit Crime Trends, **<<YEAR>>** to **<<YEAR>>**

Security Incident		Number of Occurrences			Percentage Change
		<<YEAR>>	**<<YEAR>>**	**<<YEAR>>**	
Terrorism-related incidents	Bomb threat				
	Bombing				
	CBRNE release				
Other system security incidents	Arson				
	Sabotage				
	Hijacking				
	Cybersecurity				
Other personal incidents	Aggravated assault				
	Burglary				
	Employee assault				
	Fare evasion[1]				
	Forcible rape				
	Larceny/theft				
	Homicide				
	Vehicle theft				
	Robbery				
	Suicide				
	Trespassing[1]				
	Vandalism[1]				

1. Report only those incidents that result in arrest.

Each **<<FREQUENCY>>**, **<<AGENCY NAME>>** uses the FTA's Security Manpower Planning Model (SMPM) to reassess coverage requirements of its security personnel (e.g., transit police, local law enforcement, contracted security personnel). The tool is used to assess security personnel deployment impacts resulting from changes in crime rates, as well as new service or other changes within the system. The most recent version of the SMPM can be found on the FTA Office of Safety and Security website.

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

3.3 Internal security component

[Transit agencies may have internal security personnel (security staff, transit police, security committees, outsourced security guards, etc.) who deal strictly with transit security issues. Modify this section as appropriate.]

3.3.1 Security department/organization

[A security department/organization includes transit agency employees who specifically focus on transit security issues. Employees of this department are non-sworn security personnel.]

3.3.2 Security Committee

[Modify as appropriate and if applicable.]

<<AGENCY NAME>>'s main internal security component is its Security Committee. Headed by the **<<TITLE>>**, the Security Committee is represented by all of **<<AGENCY NAME>>**'s divisions. The Security Committee assists in the security tasks of the agency, setting the direction of the SEPP, and helps to instill the agency's commitment to security in each employee. As a continuing responsibility of the committee, there is a permanent agenda oriented toward security and emergency preparedness matters, including a review of current threat conditions, comments on the management of the SEPP and processes for interacting with other public agencies. The Security Committee is dedicated to the idea that security is vital to the agency and is incorporated into every aspect of its operations. Activities performed by the Security Committee include, but may not be limited to, the following:

- Establish management and training emphasis on agency personnel awareness.
- Analyze security incidents and suspicious activities to determine a proper course of action.
- Strengthen preventive, detection and response support capabilities.
- Pursue additional grant opportunities to support regional mission requirements.
- Work to identify potential and existing problem areas.
- Assist with development and implementation of countermeasures and corrective actions.
- Develop inspection checklists and conduct periodic security surveys and inspections.
- Review and evaluate security and emergency plans for completeness and accuracy.
- Participate in formal threat and vulnerability analyses.
- Create and improve the SEPP.

3.3.3 Law enforcement

[Include a sworn law enforcement force that provides service to the agency. This section could include officers from a local police department who are dedicated to transit security.]

3.3.4 Contracted law enforcement security services

[Another component of the agency's security is its contracted law enforcement security force. This force is comprised of non-agency police officers and can typically be obtained in two basic ways: either via individual contracts with each officer or via a contract with the officers' employer, such as a local police department or sheriff's office.]

3.3.5 Contracted security services

[Another component of the agency's security is its security guard force. The security guards are hired for surveillance at the agency's facilities. Their responsibilities are to maintain a presence at these locations and to conduct security patrols.]

3.3.6 Facility security

[Modify as appropriate.]

Crime and terrorism prevention in the transit environment begins with the securing of facilities where passengers are present, where personnel work and where vehicles are stored. This requires a keen awareness of security issues and close cooperation among all levels of transit personnel. **<<AGENCY NAME>>**'s facilities have security features to limit the chances of a security breach or attack on the system. See Exhibit 4 for a more detailed description of the security functions, capabilities and provisions that are common at each facility.

EXHIBIT 4
Facility Security Features

Security Features	<<FACILITY #1 NAME>>	<<FACILITY #2 NAME>>
External		
Fencing		
Lighting		
Sensors		
Guard post		
Gate arms		
Motion detectors		
Burglar systems		
Intrusion alarms		
Video surveillance		
Public address systems		

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

EXHIBIT 4
Facility Security Features

Security Features	<<FACILITY #1 NAME>>	<<FACILITY #2 NAME>>
Panic button (to police or security)		
Card or controlled access		
Law enforcement presence (24/7)		
Security guard presence (off-hours)		
Law enforcement patrol		
Internal		
Intrusion alarms		
Motion detectors		
Video surveillance		
Card or controlled access		
Public address systems		

3.3.7 Vehicle security

[Modify as appropriate.]

<<AGENCY NAME>> has implemented some security features and practices for increasing the safety and security of its vehicles. These features include **<<DESCRIBE SECURITY FEATURES>>**. In addition to security equipment, vehicle operators are required to perform inspections on their assigned vehicles at the beginning and end of each work shift. The inspection checklists are tailored for each vehicle and reviewed daily by maintenance personnel responsible for correcting problems. The inspections include but are not limited to identification of suspicious packages.

[Add checkmarks to Exhibit 5 as appropriate.]

EXHIBIT 5
Vehicle Security Features

Security Features	Rail Cars	Buses	Support Vehicles
Automatic vehicle location (AVL) system			
Global Positioning System (GPS)			
Radios			
Direct phone			
Covert or silent alarms			
Radio speakers			
Drivers-only speakers			
Operator safety shields			
Onboard cameras (audio capable)			
Audio microphones			

3.3.8 Information technology and operational technology security

[Modify as appropriate. Ensure that the section covers how information technology team counters cyber-threats. Agencies may also reference a separate cybersecurity plan.]

<<AGENCY NAME>>'s information technology team maintains a firewall-protected intranet system for management and other personnel. **<<AGENCY NAME>>** has procured standard virus protection software and firewalls to protect its information technology infrastructure. For security purposes, **<<AGENCY NAME>>** maintains a list of the users who have access to the system. Additionally, the system requires each employee to enter a username and password at login.

3.4 Internal security practices

[In developing internal security procedures/practices, the agency should use applicable APTA standards as well as FTA and TSA guidance documents. Further, the agency should use the TSA/FTA Top 17 document to identify additional security procedures/practices not contained in this section.]

This SEPP includes internal security practices or procedures that are adhered to by all employees and contractors. Specific components deal with the personnel hiring and termination process, personnel identification and access control, and security awareness. Most requirements are directed toward the agency's employees and its contractor staff; however, some of these requirements apply to subcontractors, vendors, building tenants, visitors and patrons. Exhibit 6 identifies which security procedures **<<AGENCY NAME>>** has in place, including the source document in which the procedures can be found.

EXHIBIT 6
Security Procedures

Security Procedures	Security Procedures Exist?	Source Document
Background investigation		
Badging and uniforms		
Communication with passengers		
Identifying suspicious behavior		
Passenger and baggage screening		
Safe mail package handling		
Sensitive Security Information		
Security procurement language checklist		
Termination		
Trash container procurement and placement		
Unattended items		
Vehicle security sweeps		

3.5 External security component

The interface between **<<AGENCY NAME>>** 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.

3.5.1 Local law enforcement interface

[Describe interface between transit agency and local law enforcement.]

3.5.2 Local/county/state/tribal interface

[Describe interface between transit agency and local/county/state/tribal government security and emergency preparedness agencies, groups, committees, working groups, etc. Examples may include security and emergency preparedness committees, emergency operations centers (EOC), offices of emergency services (OES), local security and emergency preparedness committees, regional emergency preparedness working groups, etc.]

3.5.3 Federal interface

[Describe interface between transit agency and federal agencies. Examples of federal agencies may include FBI Joint Terrorism Task Force (JTTF), fusion centers, TSA's supported Regional Transit Security Working Groups (RTSWG), National Guard civil support teams, etc.]

4. Management of SEPP

This SEPP serves as a security and emergency preparedness tool to ensure that the agency's defined goals and objectives are achieved. The SEPP is intended to be a living document, requiring annual updating. As authorized by the **<<TITLE>>**, the responsibility and authority for the preparation, implementation and enhancement of the plan rests with **<<TITLE>>**. It is the responsibility of all management personnel to support the implementation and administration of the plan. The following are the top management activities associated with the security program, as identified in the SEPP:

- Communicate that security is paramount for all employees.
- Define ultimate responsibility for secure transit system operations.
- Enforce all security rules applicable to employees.
- Develop relations with outside organizations that contribute to the program.
- Identify potential security concerns in any part of the transit system.
- Actively solicit the security concerns of all employees, customers and other stakeholders.
- Ensure that the program is carried out on a daily basis.
- Provide leadership and direction during security incidents, including making decisions regarding the continuation of operations and services.

Additional responsibilities of all management personnel include the following:

- Assist with the development of implementation plans and strategies for new security initiatives and activities.
- Review new security initiatives and activities before their implementation to determine their impacts on the areas under the manager's control.
- Include security considerations in the design and construction of new equipment and facilities.

NOTE: The term "frontline employees" used in this security plan includes all vehicle operators, maintenance personnel, security personnel, receptionists, etc.—anyone who interfaces with transit customers, visitors and transit system infrastructure (e.g., vehicles, equipment, facilities).

4.1 Employees

It is the responsibility of each and every employee to place safety and security as paramount. Therefore, each employee should focus on maximizing the level of security experienced by all passengers, employees and individuals who come into contact with the system. **<<AGENCY NAME>>** hopes to ensure that, if confronted with a security event or major emergency, its employees will respond effectively, using good judgment,

applying due diligence and building on best practices identified in drills, training, rules and procedures. **<<AGENCY NAME>>**'s management expects all employees, volunteers, contractors and consultants, especially those working directly with passengers, to support this SEPP.

> **NOTE:** It is not possible to address all the specific security-related responsibilities of all personnel in a plan of this type. However, this plan will address those security-related responsibilities defined for all departments. For specific security-related responsibilities of individual personnel, the user should reference all relevant documents, such as standard operating procedures, policies, plans and programs, to achieve a complete understanding of his or her security-related responsibilities.

4.2 Agency personnel

All personnel are responsible and accountable for fulfilling and complying with the security requirements of their positions. All department heads and managers are likewise responsible and accountable for enforcing the security requirements pertaining to their employees. Further, it is the responsibility of all employees to notify their immediate supervisors whenever a criminal act or suspicious activity or occurrence has taken place. All personnel are required to understand and perform their duties, during normal and emergency operations, in accordance with all established security rules and procedures. The general security and emergency preparedness responsibilities of all employees and contractors are to do the following:

- Consider the security of transit passengers, employees, vehicles and facilities at all times while performing job duties.
- Participate in all required security training, including drills and tabletop exercises, as deemed necessary by direct supervision.
- Cooperate fully with personnel and departments conducting investigations of security breaches or other security-related incidents.
- Become familiar with all security and emergency operating procedures for the assigned work activity.

4.2.1 Transit police chief (or equivalent)

[Modify as appropriate or applicable.]

The transit police chief is empowered and authorized to design, implement and administer a comprehensive, integrated and coordinated security and emergency preparedness program that encompasses all aspects of the organization. This includes the development and administration of a specific plan for the prevention, identification, notification, analysis, control and resolution of any threats or vulnerabilities within or directed toward its operations and services. The transit police chief is responsible for ensuring that sufficient resources and attention are devoted to the SEPP, including the following:

- Development of standard operating procedures related to employee security duties
- Development and enforcement of safety and security regulations
- Development of emergency operating procedures to maximize transit system response effectiveness and minimize system interruptions during emergencies and security incidents
- Development of proper training to allow an effective response to security incidents and emergencies

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

- Development of an effective notification and reporting system for security incidents and emergencies
- Communication of security and emergency preparedness as paramount to all employees
- Development of relations with outside organizations that contribute to the SEPP, including local public safety and emergency planning agencies and major neighboring facilities or buildings

4.2.2 Director of security (or equivalent)

[Modify as appropriate. This position may assume some or all of the duties described under Section 4.2.1.]

The director of security is responsible for the daily oversight and administration of the security and emergency preparedness program and has been granted the authority to monitor and enforce its implementation to ensure achievement of security-related goals and objectives. Responsibilities include, but may not be limited to, the following:

- Chairing the Security Committee
- Developing, organizing and implementing a security and emergency response training curriculum for all employees (including contractors)
- Developing, organizing and implementing security and emergency response exercises
- Initiating a threat and vulnerability assessment process
- Compiling and analyzing security breach and system threat and vulnerability data
- Performing periodic reviews and updates of the SEPP and other relevant documents, such as operating procedures, security policies and training materials, to ensure compliance with applicable state and federal regulations, guidelines and industry best practices
- Evaluating security practices of all departments and personnel, and coordinating the establishment of new security procedures with other departments and division managers
- Participating in meetings with external public safety agencies, local community emergency planning agencies and local human services agencies to discuss security and emergency preparedness issues and to develop procedures for responding to such issues
- Developing and enforcing reasonable security and emergency preparedness procedures pertinent to agency activities
- As appropriate, communicating to other agencies the policies and procedures for dissemination of SSI displayed on drawings, schematics and other information
- Reviewing system changes or modifications to identify security-related impacts
- Evaluating and determining the need for security equipment and devices
- Ensuring that security information is made available to appropriate personnel and departments

4.3 Agency divisions

It is the responsibility of each division to place security as paramount. Therefore, each division should focus on maximizing the level of security experienced by all passengers, employees, contractors and individuals who come into contact with the transportation system.

[In some transit agencies, some of the following functions may be performed by other entities.]

4.3.1 Human resources

[Modify as appropriate.]

The specific security responsibilities of human resources personnel include the following:

- Ensuring that all pre-employment screening processes and background checks are carried out effectively
- Notifying supervisors of employee disciplinary action that may result in the affected employee becoming a risk to transit operations
- Educating employees on employee ID policies and procedures
- Participating in the development of security policies

4.3.2 Public affairs

[Modify as appropriate.]

The specific security responsibilities of public affairs personnel include the following:

- Requesting assistance from transit public safety resources as needed for special events
- Providing insight into potential threats and vulnerabilities through feedback from customer focus groups and other information sources
- Designating an agency spokesperson or public information officer (PIO) as a media contact regarding security incidents and issues
- Communicating security and encouraging riders to become part of the security effort

4.3.3 Finance

[Modify as appropriate.]

The specific security responsibilities of finance personnel include the following:

- Taking security needs and improvements into consideration when developing budgets
- Considering security aspects in all agencywide acquisitions

4.3.4 Legal

[Add as appropriate.]

4.3.5 Operations

[Add as appropriate.]

4.3.6 Paratransit

[Add as appropriate.]

4.3.7 Risk management

[Add as appropriate.]

4.3.8 Safety

[Add as appropriate.]

4.3.9 Engineering

[Add as appropriate.]

4.3.10 Maintenance

[Add as appropriate.]

4.3.11 Enterprise information and operational technology/systems

[Add as appropriate.]

4.4 Investigation and security incident reporting

[This section identifies the transit agency's investigation and security reporting procedures, both internal and external.]

Investigations must be performed on all security incidents involving **<<AGENCY NAME>>**'s system operations and services to identify what occurred and the root causes, and to develop possible countermeasures that may be implemented to prevent or minimize the impacts of future security-related incidents. It is the responsibility of **<<AGENCY NAME>>**'s **<<TITLE>>** to ensure that all security breaches and incidents are thoroughly investigated and that all applicable records are maintained.

Security and transit contractors are responsible for developing internal policies to support **<<AGENCY NAME>>**'s incident reporting requirements.

The degree of the investigation and the parties involved with the investigation will be dependent upon the type and extent of the security breach. Investigations involving **<<AGENCY NAME>>**'s assets, for example,

may involve city, state and/or federal agencies. If evidence indicates that the security breach was an act of terrorism, the FBI and other federal agencies would be involved in the investigation process. Law enforcement agencies are generally authorized to impound, receive and examine any evidence related to the incident and are responsible for maintaining the integrity of the evidence and the chain of custody. It is the responsibility of all **<<AGENCY NAME>>**'s employees, contractors and others who may have witnessed or have been involved in the incident to cooperate with all investigation processes and law enforcement agencies.

If necessary, the incident scene may be designated a crime scene by law enforcement agencies. In such cases, all operations and services may be halted in the location, and personnel may be prohibited from entering the location until the applicable law enforcement agency has completed its investigation and released the scene back to **<<AGENCY NAME>>**'s control.

In all cases, **<<AGENCY NAME>>** will strive to identify the causes and contributing factors to the security breach and will take immediate corrective actions to ensure that the same or a similar type of incident does not recur. Accordingly, it is critical that the investigation process maintain a strong link to the threat and vulnerability identification and resolution process. System threats and vulnerabilities identified as a result of the investigation are to be evaluated according to the processes detailed in Section 5.

4.4.1 Internal security incident reporting

[This section identifies and describes internal reporting procedures. Modify as appropriate.]

<<AGENCY NAME>> maintains security and emergency preparedness incident reports **<<TITLES>>**, which generally include, as a minimum, the following information:

- Physical characteristics of the scene (including photos if available)
- Significant interview findings (description of what was witnessed, the sequence of events, what may have contributed to the incident, and where the individual was located during the time of the incident)
- Sequence of events (time and date of the incident; when emergency responders arrived at the scene; when applicable local, state and federal agencies were notified; when vehicles, equipment or victims were removed from the scene and where they were taken; and when the scene was released)
- Cause(s) and contributing factors (most likely cause of the incident, as well as potential contributing factors)
- Recommendations, corrective actions and countermeasures (based on investigative findings)
- Document control number (to allow tracking of corrective actions)

4.4.2 External security incident reporting

[Each agency should determine the applicable security incident reporting requirements that may include, but are not limited to the following:

- TSA Transportation Security Operations Center
- FTA's National Transit Database—State Safety Oversight
- State and local government
- Agency-specific reporting requirements]

5. Security design

<<AGENCY NAME>> considers security in the protection of every transit asset (e.g., vehicles, stations, rail lines). The agency also takes a systems-approach to security, ensuring that all systems, components and elements, including access management, communications, infrastructure, vehicles and stations, have been analyzed and properly secured. In the design of all new assets (e.g., stations, terminals, rail lines) and vehicles (e.g., rail, bus), the agency implements best practices in security design. Among the best practices that the agency considers and references in the design of new transit assets are the "FTA Transit Security Design Considerations" document and the FTA's "Safety and Security Management Plan."

5.1 Security design considerations

<<AGENCY NAME>> considers security in the protection of every transit asset (e.g., vehicles, stations, rail lines). In doing so, the agency takes a systems approach to addressing security by analyzing the integration and interdependencies of each major elements of the transit system, including access management, communications, infrastructure, vehicles and stations. **<<AGENCY NAME>>** uses the FTA and Volpe's co-developed "Transit Security Design Considerations" report as guidance.

5.2 Crime Prevention Through Environmental Design (CPTED)

[APTA standards, including APTA SS-SIS-RP-007-10, "Crime Prevention Through Environmental Design (CPTED) for Transit Agencies," may be good resources for this section.]

<<AGENCY NAME>> employs physical design features that discourage crime while at the same time encouraging legitimate use of the asset. The agency employs CPTED concepts that include defensible space, territoriality, surveillance, lighting, landscaping and physical security planning.

5.3 Safety and Security Management Plan (SSMP)

[This section should reference the FTA's Circular 5800.1 Safety and Security Management Guidance for Major Capital Projects.]

<<AGENCY NAME>> prepares an SSMP to identify how the agency addresses safety and security in any major capital project, from initial project planning through initiation of revenue service. The SSMP is a document required by the FTA that must be prepared by applicants and recipients of FTA funds for major capital projects.

5.4 Security design verification

<<AGENCY NAME>> verifies that security design criteria identified in the threat assessment are being met. Verification methods include the safety and security certification program.

[See the FTA's Handbook for Transit Safety and Security Certification.]

6. Threat advisories

<<AGENCY NAME>> recognizes National Terrorism Advisory System (NTAS) advisories, to include both alerts and bulletins. **<<AGENCY NAME>>**'s preparedness and response actions during and immediately following an event have been developed in accordance with FTA's recommended protective measures. Additionally, **<<AGENCY NAME>>** keeps current of the federal threat level in addition to regularly receiving and monitoring alerts distributed by other organizations, including the FBI. TSA may also issue Surface Transportation Security Awareness Messages (SAM) and Cybersecurity Awareness Messages (CAM) that provide threat information and encourage additional protective measures.

6.1 National Terrorism Advisory System (NTAS)

Through the NTAS, DHS and other federal entities issue advisories based on credible threat intelligence. Advisories include:

- **Bulletin:** Describes current developments or general trends regarding threats of terrorism
- **Elevated Alert:** Warns of a credible terrorism threat against the United States
- **Imminent Alert:** Warns of a credible, specific and impending terrorism threat against the United States

DHS issues NTAS advisories to the entire community, to include law enforcement agencies, affected stakeholders and the general public, through official and social media channels. Alerts will include specific information about the threat (geographic region, mode of transportation, or critical infrastructure potentially affected), actions currently underway to protect the public, and recommended steps that individuals and stakeholders can take to help prevent, mitigate or respond to a threat. **<<AGENCY NAME>>** uses the NTAS as a guide for its own preparation and response to alerts.

6.1.1 Active Incident phase

At this phase, an attack against the transit agency or an agency's service area is occurring or has occurred. **<<AGENCY NAME>>**'s activities at this phase include the following:

- Responding to casualties
- Assisting in evacuations
- Reporting the incident (see Section 4.4)
- Inspecting and securing transit facilities
- Helping with other tasks directed by local emergency management personnel

6.1.2 Recovery phase

At this phase, the recovery of transit service after an attack has occurred. It follows the previous phase (Active Incident) and may also exist for short time periods when the agency is transitioning from a higher threat condition to a lower threat condition. This phase coexists with the prevailing threat condition. In other words, business recovery will be accomplished while maintaining the prevailing readiness status. **<<AGENCY NAME>>**'s activities at this phase include the following:

- Restoring service, routes and schedules
- Repairing or reopening facilities
- Adjusting staff work schedules and duty assignments
- Responding to customer inquiries about services
- Undertaking other activities necessary to restore transit service

6.2 FBI alerts

<<AGENCY NAME>> regularly monitors, examines and evaluates the security alerts distributed by the FBI. These alerts help identify current security issues and threats affecting the nation as a whole. **<<AGENCY NAME>>** distributes the list to selected individuals of the agency. Any questions or concerns relating to the FBI security alerts should be addressed directly to the local field office of the FBI at **<<PHONE NUMBER>>** or via **<<WEB ADDRESS>>**.

[Add name of specific contact, perhaps with JTTF]

FBI **<<CITY NAME>>**
<<FBI OFFICE ADDRESS>>

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

<<AGENCY NAME>> regularly reviews information disseminated by the PT-ISAC. In January 2003, the U.S. Department of Transportation designated the APTA as the sector coordinator in the creation of a PT-ISAC to further promote security for the public transportation industry. Through this role, APTA serves as the primary contact to organize and bring the public transportation community together to work cooperatively on physical and cybersecurity issues.

The PT-ISAC collects, analyzes and distributes critical cyber and physical security and threat information from government and numerous other sources. These sources include law enforcement, government operations centers, the intelligence community, the U.S. military, academia, IT vendors, the International Computer Emergency Response Team (CERT) and others. The PT-ISAC is full-service, responding to incidents and warnings on a 24-hour basis, seven days a week. Any questions concerning the service should be directed to:

PT-ISAC
866-STISAC-1 (866-784-7221)
www.surfacetransportationisac.org

6.4 Homeland Security Information Network–Public Transit (HSIN-PT)

<<AGENCY NAME>> regularly reviews information disseminated by TSA through DHS's HSIN-PT. HSIN-PT (dhs.gov/homeland-security-information-network-HSIN#) is a security information sharing resource for the public transit community to share unclassified security and threat information and establish relationships and network with both private and public transportation security officials. HSIN-PT 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.

7. Training

An important aspect of every employee's job is his or her individual responsibility for safety and security. As a result, **<<AGENCY NAME>>** provides security-related training for all employees. Targeted security training at **<<AGENCY NAME>>** incorporates such security and emergency management concepts as terrorism awareness, planning and management; the National Incident Management System (NIMS); and federal, state and local plans (e.g., EOPs). Security awareness training is required for all personnel and is considered an essential and proactive element of the security program. It is designed to reinforce security roles and responsibilities for all employees by doing the following:

- Preparing employees for the requirements of their jobs
- Increasing the level of security awareness throughout the organization
- Reinforcing any applicable security policies and procedures, including standard and emergency operating procedures (SOPs and EOPs)
- Providing each employee with an opportunity to take part in the security program by asking questions and voicing any concerns
- Increasing employee understanding pertaining to the potential threats and vulnerabilities within the system and what measures can be taken to eliminate, control and prepare for those threats and vulnerabilities

On March 23, 2020, TSA published the Security Training for Surface Transportation Employees Final Rule in the Federal Register. The rule requires owner/operators of higher-risk freight railroad carriers, public transportation agencies (including rail mass transit and bus systems), passenger railroad carriers, and over-the-road bus companies to provide TSA-approved security training to employees who perform security-sensitive

functions. Each owner/operator covered by this rule must designate a Security Coordinator and at least one alternate Security Coordinator, report significant security concerns to TSA, develop a comprehensive security training program, and provide security training to employees in security-sensitive positions.

7.1 General employee training (all employees)

[General employee training may be offered as onboarding and refresher training. Potential concepts and principles include transit operations and services; general rules, policies and procedures; how to best use resources; what is expected of employees; what employees should expect of others; how to identify, report and react to suspicious behavior, activity and unusually threatening activities; evacuation procedures; and the types of emergencies that may be experienced during the performance of employee duties.]

7.2 Frontline employee training (non-operators)

[Frontline employee training for non-operators (mechanics, customer service reps, receptionists, station managers, fare collectors, etc.) is essential because employees have daily contact with the agency's customers and vehicles.]

7.3 Vehicle operator training

[Training for vehicle operators may include safety, security and emergency preparedness procedures; pre-trip inspection; fare handling; radio procedures, etc.]

7.4 Management training

[Management training may include crisis management, emergency response, resource allocation, media relations, interagency coordination, information sharing, incident reporting, internal/external hierarchies of authority, continuity of operations requirements and procedures, etc.]

7.5 Emergency responder training

[Training for local emergency responders (e.g., fire, police, EMS) may be offered by the transit agency. Additional details may be contained in the emergency preparedness plan. Concepts of emergency responder training may include the following:

- Operating territory familiarization (e.g., types of operating environments and hazards within each vehicle, facility and equipment function)
- Emergency access and egress locations
- Emergency power shutoff devices and fire suppression systems
- Hazardous materials storage locations
- Communications with transit personnel

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

- Transit organizational roles and responsibilities
- Coordination of functions/lines of authority (e.g., personnel responsibilities during events)
- Relevant transit rules and operating procedures]

7.6 National Incident Management System (NIMS) training

[National Incident Management System (NIMS) training may be made available to various staff members. These staff members may include managers and supervisors, frontline employees, road supervisors, etc. NIMS training may include the following concepts and principles: benefits of using the Incident Command System (ICS) as the national incident management model, when to institute an area command, when to institute a multiagency coordination system, benefits of using a joint information center (JIC) for public information, managing resources using NIMS, and technology.]

8. Exercises and drills

[This section should be modeled after APTA's drills and standards document developed by the Security Emergency Management Working Group. Include any exercises or drills sponsored by state, local or federal agencies (e.g., emergency operations centers) but involving the transit agency. It is important for transit agencies to coordinate with local emergency operation centers, offices of emergency support or other related entities in participating, designing and supporting exercises and drills. Agencies may also use TSA's Exercise Information System (EXIS) to design and develop agency exercises.]

A program for effective joint training exercises and drills involving **<<AGENCY NAME>>** and other external agencies including local police, fire and emergency management agencies is maintained by the **<<TITLE>>** or an appointee. This program includes discussion- and operations-based exercises.

The purpose of these exercises is to demonstrate that participants understand their individual roles and responsibilities and are familiar with the equipment and layout of facilities. The results of exercises are documented in an after-action report. Exercises involve local law enforcement and emergency response personnel and are indicative of the types of emergencies typical of transit operations and services. For a list of the exercises that **<<AGENCY NAME>>** has participated in and will participate in, see Exhibit 11.

EXHIBIT 11
Exercise List

Fiscal year	Description of exercises

9. Public awareness

<<AGENCY NAME>>'s passengers are considered the eyes and ears of the agency's operations and services and play an instrumental role in its security program. As a result, the agency maintains a public awareness program to maximize passenger involvement in security. This program includes the following:

- Vehicle interior card ad campaigns
- External newsletters
- Transit education programs
- "See Something, Say Something" campaign

These are designed to promote transit operations and services while reinforcing safety and security policies and procedures. Literature to educate the public on riding the transit system is always available and can be found aboard transit vehicles. Overall, these materials are directed toward educating passengers with regard to the following:

- The steps to be taken upon witnessing suspicious, malicious or destructive activities, people, packages or materials within the system
- The steps to be taken upon identifying a potential hazard within the system, including unattended items
- The steps to be taken upon witnessing or being the victim of a criminal act
- How to properly communicate incidents to transit, law enforcement and emergency response personnel
- Emergency procedures, including emergency egress paths, exit locations and emergency equipment use
- General customer service information, including schedules, service areas, emergency contact information and relevant updates pertaining to system changes

10. Evaluation and modification

The evaluation and modification process is an excellent opportunity to ensure that the SEPP effectively eliminates and mitigates security threats. As **<<AGENCY NAME>>**'s operations change and expand; there may be a need for additional security requirements, policies, equipment and staffing. The SEPP is therefore

considered a living document that is reviewed **<<FREQUENCY>>** and updated as needed to ensure that it remains up to date and consistent with all other **<<AGENCY NAME>>** rules, procedures and policies.

10.1 Evaluation

The security program and this SEPP are constantly evaluated. This evaluation extends from the initial draft of the plan through its full implementation. Evaluations identify those areas needing additional attention, and as a result offer suggestion for improvement, either to fine-tune the program or to implement new objectives in a revised plan. The **<<TITLE>>** or designee is responsible for the evaluation or review process.

10.2 Modification

Modifications occur after a significant security incident, audits, exercises and operational changes. Also, management personnel are to recommend changes at any time when, in their opinion, there is a need for a modification. Moreover, employees are to submit proposed changes to their managers and supervisors, who evaluate the proposed change and, if warranted, submit the proposed change to the **<<TITLE>>** for review.

If system changes occur outside a scheduled review of the plan, the **<<TITLE>>** ensures that the changes are reviewed and incorporated as necessary. The **<<TITLE>>** has the primary responsibility for reviewing and updating the SEPP. Change bulletins are issued once changes are made to the plan, provided that they are properly authorized and distributed. The final decision about whether a change is issued as an addendum or one that requires a complete revision and redistribution of the SEPP rests solely with the **<<TITLE>>**.

10.3 SEPP control

The **<<TITLE>>** is responsible for the distribution of the SEPP and any revisions to it. In order to ensure that all copies are accounted for, the distributor numbers each copy and records the recipients who have been given copies. Every modification or update is distributed to **<<TITLES>>** as well as all directors, supervisors and managers.

Definitions

accident: An unforeseen event or occurrence that results in an injury, fatality or property damage.

all hazards: The concept of integrating all aspects of crisis management for safety, security and emergency management, including prevention, protection, response and recovery. Homeland Security Presidential Directive (HSPD) 8 (Dec. 17, 2003) used the term “all hazards” to include preparedness for terrorist attacks, major disasters and other emergencies.

Americans with Disabilities Act (ADA): A comprehensive civil-rights measure designed to ensure that people with disabilities receive equal access to transportation and other services.

American Public Transportation Association (APTA): An international organization that represents the transit industry.

audit: A formal or official examination and verification.

Baseline Assessment for Security Enhancement (BASE): The Baseline Assessment for Security Enhancement, performed by TSA surface inspectors, is a comprehensive security assessment of a transit agency's implementation of the TSA/FTA Security Action Items for Transit Agencies. The BASE is a Microsoft Excel–based template designed to provide uniform guidance to inspectors and security auditors for review of transit agency security programs. The tool is a means for establishing baseline security program information applicable to all surface mass transit systems and measuring their progress in security enhancements.

contractors: Includes temporary workers, day laborers, operational service providers and vendor consultants.

Code of Federal Regulations: A codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the federal government.

disaster: An event or any set of events during which injury, death, damage to property or a combination thereof occurs to the extent that resources beyond the state and local level are required.

downtime: A period in which a vehicle is inoperative due to repairs or maintenance.

emergency: A sudden, urgent, usually unforeseen event during which injury, death, damage to property or a combination thereof may occur.

emergency preparedness plan: One or more documents focusing on preparedness and response in dealing with a disaster or emergency event.

emergency response personnel: Members of police, fire, ambulance or other organizations involved with public safety and charged with providing and coordinating emergency services in response to emergencies or disasters.

employee: Any person employed by the transit agency.

equipment: Any machinery utilized on the track, road or elsewhere.

frontline employees: Personnel who have daily contact with the agency's customers and vehicles. These personnel include operators, facilities maintenance workers, customer service representatives, receptionists, station managers, fare collectors, etc.

Federal Railroad Administration (FRA): A division of the U.S. Department of Transportation that promotes railroad safety nationwide and enforces safety standards.

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Federal Transit Administration (FTA): A division of the U.S. Department of Transportation that provides leadership, guidance, technical assistance and financial resources for mass transit agencies in the United States.

hazard: Any condition or set of conditions, internal or external to the system or system operation, that when activated can cause injury, illness, death or damage to or loss of equipment or property.

hazard probability: A measurement of potential occurrences per units of time, miles, trips/runs or passengers carried.

hazard resolution: The analysis and subsequent actions taken to reduce, to the lowest level practical, the risk associated with an identified hazard.

hazard severity: The measure of the worst potential consequences that could be caused by a specific hazard.

headway: The time interval between vehicles moving in the same direction on a particular route.

incident: An unforeseen event or occurrence with the potential to cause injury or property damage.

maintenance: All actions necessary for retaining an item in, or restoring it to, an operable condition.

National Incident Management System (NIMS): A consistent nationwide template to enable all government, private sector and nongovernmental organizations to work together during domestic incidents.

off-peak period: The time period when vehicle usage is lightest, usually between the hours of 8 p.m. to 6 a.m. and 9 a.m. to 4 p.m.

park-and-ride lot: Designated parking area where vehicle drivers park and board transit vehicles to other locations.

peak period: Morning and afternoon time periods when vehicle usage is heaviest, usually between the hours of 6 to 9 a.m. and 4 to 8 p.m.

revenue vehicle: A vehicle that carries fare-paying passengers.

risk: A subjective evaluation of the possibility of incurring a physical or personal loss or injury.

rules and instructions: Procedures, policies and guidelines that must be obeyed by all employees. This may be supplemented and revised by bulletins or other written directives.

safety: Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Safety and Security Management Plan (SSMP): A document required by the FTA that must be prepared by applicants for and recipients of FTA funds for major capital projects. It is a part of the project management plan (PMP) and is written to describe how the recipient will address safety and security in major capital projects.

security: Freedom from intentional harm.

security breach: An unforeseen event or occurrence that endangers life or property and may result in the loss of services or system equipment.

system: A composite of people, procedures and equipment integrated to perform a specific operational task or function within a specific environment.

system safety: The application of operating, technical and management techniques and principles to the safety aspects of a system throughout its life to reduce hazards to the lowest practical level through the most effective use of available resources.

system security: The application of operating, technical and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.

security plan: A document adopted by the transit agency detailing its security policies, objectives, responsibilities and procedures.

system security program: The combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner.

threat: Any action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations or denial of services.

threat analysis: A systematic analysis of a system operation performed to identify threats and to make recommendations for their elimination or mitigation during all revenue and non-revenue operations.

threat resolution: The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.

Transit Watch: An FTA-sponsored program that aims to increase security through the awareness of passengers and transit agency employees.

Transportation Security Administration (TSA): An agency within the U.S. Department of Homeland Security charged with protecting the U.S. transportation system to ensure freedom of movement for people and commerce.

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

vehicle operator: An employee who controls the movement and operation of buses, paratransit, rail or other vehicles.

vulnerability: Anything that can be taken advantage of to carry out an attack.

Abbreviations and acronyms

ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
AVL	automatic vehicle location
BASE	Baseline Assessment for Security Enhancement (TSA)
CBRNE	chemical, biological, radiological, nuclear, explosive
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security
EOC	emergency operation center
EOP	emergency operating procedure
EXIS	Exercise Information System
FBI	Federal Bureau of Investigation
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
GPS	Global Positioning System
HSIN-PT	Homeland Security Information Network – Public Transit
HSPD	Homeland Security Presidential Directive
ICS	Incident Command System
IT	information technology
JIC	joint information center
JIS	Joint Information System
JTTF	Joint Terrorism Task Force
MIS	Management Information System
MOU	memorandum of understanding
NIMS	National Incident Management System
NTAS	National Terrorism Advisory System
NTD	National Transit Database
OES	Office of Emergency Services
PIO	public information officer
PMP	project management plan
PT-ISAC	Public Transit Intelligence Sharing and Analysis Center
RTSWG	Regional Transit Security Working Group
SAM	Security Awareness Message
SEPP	Security and Emergency Preparedness Plan
SMPM	Security Manpower Planning Model

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SOP	standard operating procedure
SSI	Sensitive Security Information
SSMP	Safety and Security Management Plan
TSA	Transportation Security Administration

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Appendix A: Points of contact list

Contacts					
Name	**Company**	**Title**	**Work phone**	**Cell phone**	**Email**

[When transit agency data is added to this document, it must be labeled Sensitive Security Information, and the following text should be included:]

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Appendix B: Communications tree

Communications tree	
Event	
Communications steps	1.
	2.
	3.
	4.
	5.
Event	
Communications steps	1.
	2.
	3.
	4.
	5.
Event	
Communications steps	1.
	2.
	3.
	4.
	5.
Event	
Communications steps	1.
	2.
	3.
	4.
	5.