Security Risk Management Working Group
APTA SS-SRM-RP-001-09, Rev. 1
Published March 31, 2012

Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)

January 31, 2012, Revision 1
March 12, 2008
APTA Security Risk Management Working Group

February 28, 2012, Revision 1
May 7, 2008
APTA Technical Oversight Group/Committee

June 30, 2012, Revision 1
Authorized February 18, 2009
APTA Transit Security Standards Policy and Planning Committee

Abstract: This Recommended Practice describes the process by which a Security and Emergency Preparedness Plan (SEPP) may be developed, implemented and evaluated.

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

Introduction

(This introduction is not a part of APTA SS-SRM-RP-01-09, *Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP).)*

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

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.

The purpose of an APTA Transit Recommended Practice is to ensure that each transit system achieves a high level of safety for passengers, employees and the public. APTA Transit Recommended Practices represent an industry consensus of acceptable safety practices that should be used by a transit system. However, APTA recognizes that some transit systems have unique aspects of their operating environment that, when combined with levels of service that must be provided, may make strict compliance with every provision of an APTA Transit Recommended Practice impossible.

When a transit agency is faced with this situation, it may specify in its system security plan an alternate means to achieve an equivalent level of security as that provided by this APTA Transit Security Recommended Practice. The system security plan should do the following:

- Identify the Transit Security Recommended Practice provisions that cannot be fully met.
- State why these provisions cannot be fully met.
- Describe the alternate means to ensure that equivalent security is achieved.
- Provide a reasonable basis (i.e., operating history or threat and vulnerability analysis) for why security is not compromised through the alternate means.

Participants

The American Public Transportation Association greatly appreciates the contributions of Mark Uccardi who developed this Recommended Practice. At the time this was completed, the Security Risk Management Working Group included the following members:

- Michael Birch, Chair
- Mark Uccardi, Vice Chair
- Chris Chock
- Jennifer Donald Kevin Dow Clare Mueting
- Heyward Johnson
- Richard Gerhart
- Karen Head
- Sheila Hockel
- Scott Strathy
- Stephen Schwimmer
- Ben Titus
- Peter Totten
- Morvarid Zolghadr

Contents

Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP)

1. Overview

This Recommended Practice describes the process by which a Security and Emergency Preparedness Plan (SEPP) may be developed, implemented and evaluated. It gives guidance on how to develop and implement a SEPP. A template for transit agencies to develop a customized SEPP is provided in Annex D. 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. It 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.

The intent of this document is to ensure that an agency is well-prepared to write and implement its SEPP. Writing the document is only part of the challenge. The other challenge is the implementation of the SEPP. 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.

1.1 Scope

This document covers recommended activities that a transit agency may initiate to develop, implement and evaluate a 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.

1.2 Purpose

The purpose of this document is to aid the transit agency in the development and implementation of a SEPP. This document is simply one approach and is meant as a guide for creating the SEPP using the SEPP template found in Annex D. If an agency decides that another process is a better fit, then that process should be used to ensure success.

1.3 Goals

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 amount of time and effort needed to prepare and implement the SEPP while maintaining the document's clarity and comprehensiveness.

2. 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.

2.1 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 below.

2.1.1 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 existing within the agency.
- Collect information on all security-related activities (e.g., background checks, badging, termination, security sweeps, dissemination/storing 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-type information on the transit system (e.g., riders, assets, operating environment, and data reported as part of FTA's National Transit Database [NTD] reporting requirement).
- Collect transit crime statistics and trends.
- Collect methodology and results from prior security risk assessments.

2.1.2 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 your transit agency's name and appropriate information in the designated/prompted places of the template. 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 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.

2.1.3 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, 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.

2.1.4 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).

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

2.2 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 below.

2.2.1 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.

2.2.2 Implement 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.

2.2.3 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.

2.2.4 Modify the SEPP

- Schedule an annual update 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).

Annex A: Implementing recommendation of the 9/11 Commission Act of 2007 (H.R.1/H.R. Report 110-259; Public Law 110-53)

This legislation, also referred to as the 9/11 Act, directs the Department of Homeland Security (DHS) to promulgate regulations requiring "high-risk" mass transit systems to develop and implement a security plan. The security plan provisions of the 9/11 Act are summarized below.

Section 1405: Security Assessments and Plans

DHS must issue regulations requiring public transportation agencies determined to be at "high risk" of terrorism to maintain and implement a comprehensive security plan. DHS must provide technical assistance and guidance to public transportation agencies on preparing and implementing security plans. No public transportation system is required to develop a security plan if it does not receive security grants authorized under Section 1406 (summarized immediately below), unless the DHS determines otherwise and informs the Congress in writing.

DHS must ensure that the required security plan contains the following elements:

- Prioritized list of all items in the public transportation agency's security assessment that have not been addressed
- Detailed list of any capital and operational improvements identified either by DHS or the public transportation agency and certification of the agency's capacity for operating and maintaining security equipment included on this list
- Specific procedures for responding to attacks or emergencies
- Coordinated response plan with procedures for interacting with state and local agencies
- Strategy and timeline for conducting security training
- Plans for redundant operations capabilities and for providing service in the event of a terrorist attack or other major incident
- Methods to mitigate damage in case of an attack, including plans for communication and coordination with first responders

DHS must complete review of a covered public transportation agency's security plans within six months of its being submitted to ensure the requirements of this section are met. DHS/TSA must encourage coordinated planning by agencies using sharing facilities. Beginning in fiscal year 2008, DHS must consult with management and labor organizations to establish security improvement priorities and must allocate risk-based grant funds based on these priorities. DHS/TSA may recognize existing procedures, protocol and standards that meet the requirements of this section.

Section 1406: Public Transportation Security Assistance

DHS must establish a grant program for public transportation security assistance. Eligibility for grants under this program is restricted to those agencies for which DHS has performed a security assessment or those that have developed a security plan per Section 1405. Funds may be used for either capital or operating security enhancements, with a lengthy list of possible actions. DHS must determine grant recipients "based solely on risk" and establish the priorities for use of the grants. Each grant recipient must report annually to DHS on use of funds.

Annex B: FTA State Safety Oversight Program

Contained within the FTA's State Safety Oversight Program are requirements for a rail transit agency's system security plan. The system security plan requirements of the State Safety Oversight Program under 49 CFR 659 are identified below.

659.21: System security plan, general requirements

(a) The oversight agency shall require the rail transit agency to implement a system security plan that, at a minimum, complies with requirements in this part and the oversight agency's program standard. The system security plan must be developed and maintained as a separate document and may not be part of the rail transit agency's system safety program plan.

(b) The oversight agency may prohibit a rail transit agency from publicly disclosing the system security plan.

(c) After approving the system security plan, the oversight agency shall issue a formal letter of approval, including the checklist used to conduct the review, to the rail transit agency.

659.23: System security plan, contents

The system security plan must, at a minimum, address the following:

(a) Identify the policies, goals and objectives for the security program endorsed by the agency's chief executive.

(b) Document the rail transit agency's process for managing threats and vulnerabilities during operations, and for major projects, extensions, new vehicles and equipment, including integration with the safety certification process;

(c) Identify controls in place that address the personal security of passengers and employees;

(d) Document the rail transit agency's process for conducting internal security reviews to evaluate compliance and measure the effectiveness of the system security plan; and

(e) Document the rail transit agency's process for making its system security plan and accompanying procedures available to the oversight agency for review and approval.

659.25: Annual review of system security plan

(a) The oversight agency shall require the rail transit agency to conduct an annual review of its system security plan.

(b) [*pertains only to a system safety plan]*

(c) In the event the rail transit agency's system security plan is modified, the rail transit agency must make the modified system security plan and accompanying procedures available to the oversight agency for review, consistent with the requirements specified in **659.23(e)** of this part. After the plan is approved, the oversight agency shall issue a formal letter of approval to the rail transit agency.

Annex C: FRA Emergency Preparedness Plan Requirements

The Federal Railroad Administration (FRA) has emergency preparedness plan requirements, which are contained in 49 CFR Part 239 (Passenger Train Emergency Preparedness) as well as the Presidential Executive Order 13347: Individuals with Disabilities in Emergency Preparedness. The specific emergency preparedness plan requirements are identified below for those agencies that come under FRA regulations.

49 CFR 239 (Section 101): Specific Requirements for Emergency Preparedness Plans

(a) Each railroad to which this part applies shall adopt and comply with a written emergency preparedness plan approved by FRA under the procedures of Section 239.201. The plan shall include the following elements and procedures for implementing each plan element.

(1) Communication

> (i) Initial and on-board notification. An on-board crewmember shall quickly and accurately assess the passenger train emergency situation and then notify the control center as soon as practicable by the quickest available means. As appropriate, an on-board crewmember shall inform the passengers about the nature of the emergency and indicate what corrective countermeasures are in progress.
>
> (ii) Notifications by control center. The control center shall promptly notify outside emergency responders, adjacent rail modes of transportation, and appropriate railroad officials that a passenger train emergency has occurred. Each railroad shall designate an employee responsible for maintaining current emergency telephone numbers for use in making such notifications.

(2) Employee training and qualification

> (i) On-board personnel. The railroad's emergency preparedness plan shall address individual employee responsibilities and provide for initial training, as well as periodic training at least once every two calendar years thereafter, on the applicable plan provisions. As a minimum, the initial and periodic training shall include:
>
> > (A) Rail equipment familiarization;
> >
> > (B) Situational awareness;
> >
> > (C) Passenger evacuation;
> >
> > (D) Coordination of functions;
> >
> > (E) "Hands-on" instruction concerning the location, function, and operation of on-board emergency equipment.
>
> (ii) Control center personnel. The railroad's emergency preparedness plan shall require initial training of responsible control center personnel, as well as periodic training at least

once every two calendar years thereafter, on appropriate courses of action for each potential emergency situation. As a minimum, the initial and periodic training shall include:

(A) Dispatch territory familiarization;

(B) Protocols governing internal communications between appropriate control center personnel whenever an imminent potential emergency situation exists.

(iii) Initial training schedule for current employees. The railroad's emergency preparedness plan shall provide for the completion of initial training of all on-board and control center employees who are employed by the railroad on the date that the plan is conditionally approved under Sec. 239.201(b)(1), in accordance with the following schedule:

(A) For each railroad that provides commuter or other short-haul passenger train service and whose operations include less than 150 route miles and less than 200 million passenger miles annually, not more than one year after January 29, 1999, or not more than 90 days after commencing passenger operations, whichever is later.

(B) For each railroad that provides commuter or other short-haul passenger train service and whose operations include at least 150 route miles or at least 200 million passenger miles annually, not more than two years after January 29, 1999, or not more than 180 days after commencing passenger operations, whichever is later.

(C) For each railroad that provides intercity passenger train service, regardless of the number of route miles or passenger miles, not more than two years after January 29, 1999, or not more than 180 days after commencing passenger operations, whichever is later.

(D) For each freight railroad that hosts passenger train service, regardless of the number of route miles or passenger miles of that service, not more than one year after January 29, 1999, or not more than 90 days after the hosting begins, whichever is later.

(iv) Initial training schedule for new employees. The railroad's emergency preparedness plan shall provide for the completion of initial training of all on-board and control center employees who are hired by the railroad after the date on which the plan is conditionally approved under Sec. 239.201(b)(1). Each employee shall receive initial training within 90 days after the employee's initial date of service.

(v) Testing of on-board and control center personnel. A railroad shall have procedures for testing a person being evaluated for qualification under the emergency preparedness plan. The types of testing selected by the railroad shall be:

(A) Designed to accurately measure an individual employee's knowledge of his or her responsibilities under the plan;

(B) Objective in nature;

(C) Administered in written form;

(D) Conducted without reference by the person being tested to open reference books or other materials, except to the degree the person is being tested on his or her ability to use such reference books or materials.

(vi) On-board staffing

(A) Except as provided in paragraph (a)(2)(vi)(B), all crewmembers on board a passenger train shall be qualified to perform the functions for which they are responsible under the provisions of the applicable emergency preparedness plan.

(B) A freight train crew relieving an expired passenger train crew en route is not required to be qualified under the emergency preparedness plan, provided that at least one member of the expired passenger train crew remains on board and is available to perform excess service under the Federal hours of service laws in the event of an emergency.

(3) Joint operations

(i) Each railroad hosting passenger train service shall address its specific responsibilities consistent with this part.

(ii) In order to achieve an optimum level of emergency preparedness, each railroad hosting passenger train service shall communicate with each railroad that provides or operates such service and coordinate applicable portions of the emergency preparedness plan. All of the railroads involved in hosting, providing, and operating a passenger train service operation shall jointly adopt one emergency preparedness plan that addresses each entity's specific responsibilities consistent with this part. Nothing in this paragraph shall restrict the ability of the railroads to provide for an appropriate assignment of responsibility for compliance with this part among those railroads through a joint operating agreement or other binding contract. However, the assignor shall not be relieved of responsibility for compliance with this part.

(4) Special circumstances

(i) Tunnels. When applicable, the railroad's emergency preparedness plan shall reflect readiness procedures designed to ensure passenger safety in an emergency situation occurring in a tunnel of 1,000 feet or more in length. The railroad's emergency preparedness plan shall address, as a minimum, availability of emergency lighting, access to emergency evacuation exits, benchwall readiness, ladders for detraining, effective radio or other communication between on-board crewmembers and the control center, and options for assistance from other trains.

(ii) Other operating considerations. When applicable, the railroad's emergency preparedness plan shall address passenger train emergency procedures involving operations on elevated structures, including drawbridges, and in electrified territory.

(iii) Parallel operations. When applicable, the railroad's emergency preparedness plan shall require reasonable and prudent action to coordinate emergency efforts where adjacent rail modes of transportation run parallel to either the passenger railroad or the railroad hosting passenger operations.

(5) Liaison with emergency responders. Each railroad to which this part applies shall establish and maintain a working relationship with the on-line emergency responders by, as a minimum:

(i) Developing and making available a training program for all on-line emergency responders who could reasonably be expected to respond during an emergency situation. The training program shall include an emphasis on access to railroad equipment, location of railroad facilities, and communications interface, and provide information to emergency responders who may not have the opportunity to participate in an emergency simulation. Each affected railroad shall either offer the training directly or provide the program information and materials to state training institutes, firefighter organizations, or police academies;

(ii) Inviting emergency responders to participate in emergency simulations;

(iii) Distributing applicable portions of its current emergency preparedness plan at least once every three years, or whenever the railroad materially changes its plan in a manner that could reasonably be expected to affect the railroad's interface with the on-line emergency responders, whichever occurs earlier, including documentation concerning the railroad's equipment and the physical characteristics of its line, necessary maps, and the position titles and telephone numbers of relevant railroad officers to contact.

(6) On-board emergency equipment

(i) General. Each railroad's emergency preparedness plan shall state the types of emergency equipment to be kept on board and indicate their location(s) on each passenger car that is in service. Effective May 4, 1999, or not more than 120 days after commencing passenger operations, whichever is later, this equipment shall include, at a minimum:

(A) One fire extinguisher per passenger car;

(B) One pry bar per passenger car;

(C) One flashlight per on-board crewmember.

(ii) Effective May 4, 1999, or not more than 120 days after commencing passenger operations, whichever is later, each railroad that provides intercity passenger train service shall also equip each passenger train that is in service with at least one first-aid kit accessible to crewmembers that contains, at a minimum:

(A) Two small gauze pads (at least 4×4 inches);

(B) Two large gauze pads (at least 8×10 inches);

(C) Two adhesive bandages;

(D) Two triangular bandages;

(E) One package of gauge roller bandage that is at least two inches wide;

(F) Wound cleaning agent, such as sealed moistened towelettes;

(G) One pair of scissors;

(H) One set of tweezers;

(I) One roll of adhesive tape;

(J) Two pairs of latex gloves; and

(K) One resuscitation mask.

(iii) On-board emergency lighting. Consistent with the requirements of part 238 of this chapter, auxiliary portable lighting (e.g., a handheld flashlight) must be accessible and provide, at a minimum:

(A) Brilliant illumination during the first 15 minutes after the onset of an emergency situation; and

(B) Continuous or intermittent illumination during the next 60 minutes after the onset of an emergency situation.

(iv) Maintenance. Each railroad's emergency preparedness plan shall provide for scheduled maintenance and replacement of first-aid kits, on-board emergency equipment, and on-board emergency lighting.

(7) Passenger safety information.

(i) General. Each railroad's emergency preparedness plan shall provide for passenger awareness of emergency procedures, to enable passengers to respond properly during an emergency.

(ii) Passenger awareness program activities. Each railroad shall conspicuously and legibly post emergency instructions inside all passenger cars (e.g., on car bulkhead signs, seatback decals, or seat cards) and shall utilize one or more additional methods to provide safety awareness information including, but not limited to, one of the following:

(A) On-board announcements;

(B) Laminated wallet cards;

(C) Ticket envelopes;

(D) Timetables;

(E) Station signs or video monitors;

(F) Public service announcements; or

(G) Seat drops

49 CFR 239 (Section 201): Emergency Prep. Plan Filling and Approval Requirements

(a) Filing. Each passenger railroad to which this part applies and all railroads hosting its passenger train service (if applicable) shall jointly adopt a single emergency preparedness plan for that service and the passenger railroad shall file one copy of that plan with the Associate Administrator for Safety, Federal Railroad Administration, Mail Stop 25, 400 Seventh Street, S.W., Washington, D.C. 20590, not more than 180 days after May 4, 1998, or not less than 45 days prior to commencing passenger operations, whichever is later. The emergency preparedness plan shall include the name, title, address, and telephone number of the primary person on each affected railroad to be contacted with regard to review of the plan, and shall include a summary of each railroad's analysis supporting each plan element and describing how every condition on the railroad's property that is likely to affect emergency response is addressed in the plan. Each subsequent amendment to a railroad's emergency preparedness plan shall be filed with FRA by the passenger railroad not less than 60 days prior to the proposed effective date.

(b) Approval

(1) Preliminary review

(i) Within 90 days of receipt of each proposed emergency preparedness plan, and within 45 days of receipt of each plan for passenger operations to be commenced after the initial deadline for plan submissions, FRA will conduct a preliminary review of the proposed plan to determine if the elements prescribed in Sec. 239.101 are sufficiently addressed and discussed in the railroad's plan submission. FRA will then notify the primary contact person of each affected railroad in writing of the results of the review, whether the proposed plan has been conditionally approved by FRA, and if not conditionally approved, the specific points in which the plan is deficient.

(ii) If a proposed emergency preparedness plan is not conditionally approved by FRA, the affected railroad or railroads shall amend the proposed plan to correct all deficiencies identified by FRA (and provide FRA with a corrected copy) not later than 30 days following receipt of FRA's written notice that the proposed plan was not conditionally approved.

(2) Final review

(i) Within 18 months of receipt of each proposed plan, and within 180 days of receipt of each proposed plan for passenger operations to be commenced after the initial deadline for plan submissions, FRA will conduct a comprehensive review of the conditionally approved plan to evaluate implementation of the elements included. This review will include ongoing dialogues with rail management and labor representatives, and field analysis and verification. FRA will then notify the primary contact person of each affected railroad in writing of the results of the review, whether the conditionally approved

plan has been finally approved by FRA, and if not approved, the specific points in which the plan is deficient.

(ii) If an emergency preparedness plan of a railroad or railroads is not finally approved by FRA, the affected railroad or railroads shall amend the plan to correct all deficiencies (and provide FRA with a corrected copy) not later than 30 days following receipt of FRA's written notice that the plan was not finally approved.

(3) Review of amendments.

(i) FRA will review each proposed plan amendment within 45 days of receipt. FRA will then notify the primary contact person of each affected railroad of the results of the review, whether the proposed amendment has been approved by FRA, and if not approved, the specific points in which the proposed amendment is deficient.

(ii) If the amendment is not approved, the railroad shall correct any deficiencies identified by FRA and file the corrected amendment prior to implementing the amendment.

(4) Reopened review. Following initial approval of a plan, or amendment, FRA may reopen consideration of the plan, or amendment, for cause stated.

Presidential Executive Order 13347 Emergency Preparedness Plan Requirements

(1) Section 1 - Policy. To ensure that the Federal Government appropriately supports safety and security for individuals with disabilities in situations involving disasters, including earthquakes, tornadoes, fires, floods, hurricanes, and acts of terrorism, it shall be the policy of the United States that executive departments and agencies of the Federal Government (agencies):

(a) consider, in their emergency preparedness planning, the unique needs of agency employees with disabilities and individuals with disabilities whom the agency serves;

(b) encourage, including through the provision of technical assistance, as appropriate, consideration of the unique needs of employees and individuals with disabilities served by State, local, and tribal governments and private organizations and individuals in emergency preparedness planning; and

(c) facilitate cooperation among Federal, State, local, and tribal governments and private organizations and individuals in the implementation of emergency preparedness plans as they relate to individuals with disabilities.

(2) Section 2 - Establishment of Council.

(a) There is hereby established, within the Department of Homeland Security for administrative purposes, the Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (the "Council"). The Council shall consist exclusively of the following members or their designees:

(i) the heads of executive departments, the Administrator of the Environmental Protection Agency, the Administrator of General Services, the Director of the Office of Personnel Management, and the Commissioner of Social Security; and

(ii) any other agency head as the Secretary of Homeland Security may, with the concurrence of the agency head, designate.

(b) The Secretary of Homeland Security shall chair the Council, convene and preside at its meetings, determine its agenda, direct its work, and, as appropriate to particular subject matters, establish and direct subgroups of the Council, which shall consist exclusively of Council members.

(c) A member of the Council may designate, to perform the Council functions of the member, an employee of the member's department or agency who is either an officer of the United States appointed by the President, or a full-time employee serving in a position with pay equal to or greater than the minimum rate payable for GS-15 of the General Schedule.

(3) Section 3 - Functions of Council

(a) The Council shall:

(i) coordinate implementation by agencies of the policy set forth in section 1 of this order;

(ii) whenever the Council obtains in the performance of its functions information or advice from any individual who is not a full-time or permanent part-time Federal employee, obtain such information and advice only in a manner that seeks individual advice and does not involve collective judgment or consensus advice or deliberation; and

(iii) at the request of any agency head (or the agency head's designee under section 2(c) of this order) who is a member of the Council, unless the Secretary of Homeland Security declines the request, promptly review and provide advice, for the purpose of furthering the policy set forth in section 1, on a proposed action by that agency.

(b) The Council shall submit to the President each year beginning 1 year after the date of this order, through the Assistant to the President for Homeland Security, a report that describes:

(i) the achievements of the Council in implementing the policy set forth in section 1;

(ii) the best practices among Federal, State, local, and tribal governments and private organizations and individuals for emergency preparedness planning with respect to individuals with disabilities; and

(iii) recommendations of the Council for advancing the policy set forth in section 1.

(4) Section 4c. 4. - General

(a) To the extent permitted by law:

(i) agencies shall assist and provide information to the Council for the performance of its functions under this order; and

(ii) the Department of Homeland Security shall provide funding and administrative support for the Council.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers or employees, or any other person.

Annex D: SEPP template

A template for transit agencies to develop a customized SEPP is provided on the following pages. 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. This blue and red text should be deleted or replaced on completion of the SEPP.

<<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>>

Security and Emergency Preparedness Plan (SEPP)

<<ADD AGENCY LOGO>>.

<<ADD AGENCY NAME>>

<<ADD RELEASE DATE>>

<<ADD VERSION #>>

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:

<<ADD NAME>>
<<ADD TITLE>>
<<ADD MAILING ADDRESS>>
<<ADD E-MAIL ADDRESS>>

<<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>>

Policy statement

Recent worldwide terrorist attacks on transportation systems have created a climate of heightened risk and security awareness. The inherently open and easily accessible nature of transit systems, coupled with this heightened state of alert, has in turn greatly increased the importance of security throughout the transit industry. The Federal Transit Administration (FTA) and Transportation Security Administration (TSA) have recognized and responded to this increased importance by placing their own emphasis on transit security.

The **<<ADD AGENCY NAME>>**, in support of its mission to provide safe and secure transit services, and in response to FTA and TSA's increased 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 as a *condition of employment*. Further, **<<ADD 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, **<<ADD 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 **<<ADD 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 **<<ADD 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

<<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.

<<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>>

Contents

List of exhibits

Security and Emergency Preparedness Plan (SEPP)

1. Overview

The inherently open nature of public transportation systems, the quantities 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. Recent worldwide terrorist attacks have created an environment of heightened risk throughout the nation and have further increased the need for security hardening within the nation's public transportation systems.

The Federal Transit Administration has responded to this heightened level of risk by increasing its 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. The **<<ADD 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, **<<ADD AGENCY NAME>>** has developed this security plan in accordance with the following:

- *TSA/FTA Security and Emergency Management Action Items for Transit Agencies, 2008*
- *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, 2007*

This security plan emphasizes **<<ADD 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 **<<ADD AGENCY NAME>>**'s system safety program establishes mechanisms for identifying and addressing hazards within **<<ADD AGENCY NAME>>**'s operations, this security plan establishes mechanisms through which security-related threats and vulnerabilities can be identified and addressed. It is therefore the intent of **<<ADD 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.

<<ADD 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 **<<ADD 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 **<<ADD 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 **<<ADD 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 **<<ADD AGENCY NAME>>** and its employees, contractors, passengers and other personnel can:

- Appropriately identify and report threats and vulnerabilities within **<<ADD AGENCY NAME>>**'s operations to the correct personnel and/or external parties (emergency response agencies, law enforcement agencies, etc.) so that 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 **<<ADD AGENCY NAME>>**'s security program.
- Satisfy local, state and federal requirements and guidelines, such as those of the city of **<<ADD CITY NAME>>** as applicable.

1.1 Scope

[Insert what the extent of this 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 **<<ADD AGENCY NAME>>** organizational units, employees and contractors. This security plan is to include all current modes of transportation but be scaleable to incorporate any new service if and when it is introduced.

This SEPP provides guidance for all emergency management and security personnel from an *all* hazards approach (criminal activity including terrorism, natural disasters, etc.).

1.2 Goals

[Insert what the overall goals of the SEPP will be. Unlike objectives, goals are more general and broad. Modify as appropriate.]

The overall goal of **<<ADD AGENCY NAME>>**'s Security and Emergency Preparedness Plan is to establish the highest reasonable level of security that can be afforded to all passengers, employees, contractors, equipment and facilities. Through the implementation of an effective security program, **<<ADD AGENCY NAME>>** will plan to provide training for employees and contractors to supply the knowledge and skills necessary to effectively respond to and control security incidents and other major events. Specific goals of the SEPP are to do the following:

- Foster the development of an agencywide security program that complements the agency's 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. Unlike goals, objectives are more specific and focused. 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 do 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 other personnel to identify criminal acts, suspicious activities and occurrences, or other security concerns identified within **<<ADD 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 **<<ADD 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 breaches 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

FTA defines system security 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."

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

<<ADD 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 **<<ADD AGENCY NAME>>**, as developed and approved by the **<<ADD TITLE>>**, is defined as follows:

[Add mission statement]

2. Definitions and acronyms

2.1 Definitions

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

2.1.2 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 (December 17, 2003) used the term "all hazards" to include preparedness for terrorist attacks, major disasters and other emergencies.

2.1.3 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.

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

2.1.5 audit: A formal or official examination and verification.

2.1.6 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.

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

2.1.8 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.

2.1.9 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.

2.1.10 Department of Labor: A Cabinet-level agency that administers a variety of federal labor laws, including those that guarantee workers' rights to safe and healthful working conditions; a minimum hourly wage and overtime pay; freedom from employment discrimination; unemployment insurance; and other income support.

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

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

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

2.1.14 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.

2.1.15 employee: Any person employed by the transit agency.

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

2.1.17 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.

[The titles of frontline employees may vary from agency to agency.]

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

2.1.19 Federal Transit Administration: 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.

2.1.20 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.

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

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

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

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

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

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

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

2.1.28 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.

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

2.1.30 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.

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

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

2.1.33 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.

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

2.1.35 Safety and Security Management Plan: An SSMP is 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.

2.1.36 security: Freedom from intentional harm.

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

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

2.1.39 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.

2.1.40 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.

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

2.1.42 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.

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

2.1.44 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.

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

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

2.1.47 Transportation Security Administration (TSA): An agency within the U.S. Depart-

ment of Homeland Security charged with protecting the U.S. transportation system to ensure freedom of movement for people and commerce.

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

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

2.2 Acronyms

ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
AVL	automatic vehicle location
BASE	Baseline Assessment for Security Enhancement (TSA)
CCTV	closed-circuit television
CFR	Code of Federal Regulations
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security
EOC	Emergency Operation Centers
EOP	Emergency Operating Procedure
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
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
PT-ISAC	Public Transit Intelligence Sharing and Analysis Center
RTSWG	Regional Transit Security Working Group
SMPM	Security Manpower Planning Model
SOP	standard operating procedure
SSI	Sensitive Security Information
SSMP	Safety and Security Management Plan
TSA	Transportation Security Administration

VISAT Vulnerability Identification Self-Assessment Tool
WMD weapon of mass destruction

3. Transit system description

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

3.1 Organizational structure

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

3.2 Operating environment

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

3.3 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.]

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

OPERATING STATISTICS (<<ADD YEAR>>)

Exhibit 1

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

3.4 Facilities description

[Insert information describing 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.]

3.5 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.]

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

3.6 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.]

3.7 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.]

4. Security conditions, trends and capabilities

Since September 11, 2001, transit agencies have placed greater emphasis on mitigating terrorism-related events. Prior to 9/11, emphasis at **<<ADD 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, **<<ADD 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.

4.1 Security incident recording

<<ADD 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. The NTD's guidelines for what activities to report and when are found at http://www.ntdprogram.gov/ntdprogram/safety.htm. **<<ADD 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.

REPORTED TRANSIT CRIMES (<<ADD YEAR>>)

Exhibit 2

Security Incident		Number of Occurrences
Terrorism-related incidents	Bomb threat	
	Bombing	
	Chemical/biological/radiological/nuclear (CBRN) release	
Other system security incidents	Arson	
	Sabotage	
	Hijacking	
	Cyber security event	
Other personal incidents	Aggravated assault	
	Burglary	
	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 arrests.

4.2 Security incidents trend analysis

<<ADD 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, **<<ADD 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.>

TRANSIT CRIME TRENDS (**<<ADD YEAR>>** **to** **<<ADD YEAR>>**)
Exhibit 3

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

1. Report only those incidents that result in arrests.

Each **<<ADD FREQUENCY>>**, **<<ADD 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 Web site at www.transit-safety.volpe.dot.gov.

4.3 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.]

4.3.1 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.]

4.3.2 Security Committee

[Modify as appropriate and if applicable.]

<<ADD AGENCY NAME>>'s main internal security component is its Security Committee. Headed by the **<<ADD TITLE>>**, the Security Committee is represented by all of **<<ADD 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.

4.3.3 Law enforcement

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

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

4.3.4 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.]

4.3.5 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.]

4.3.6 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. **<<ADD 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.

FACILITY SECURITY FEATURES

Exhibit 4

Security Features	<<ADD FACILITY #1 NAME>>	<<ADD FACILITY #2 NAME>>
External		
Fencing		
Lighting		
Sensors		
Guard post		
Gate arms		
Motion detectors		
Burglar systems		
Intrusion alarms		
Closed-circuit TV (CCTV)		
Public address systems		
Panic button (to police or security)		
Card or controlled access		
Law enforcement presence (24/7)		
Security guard presence (off-hours)		
Law enforcement patrol		
Law enforcement canine patrol		
Internal		
Intrusion alarms		
Motion detectors		
Closed-circuit TV (CCTV)		
Card or controlled access		
Public address systems		

4.3.7 Vehicle security

[Modify as appropriate.]

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

<<ADD AGENCY NAME>> has implemented some security features and practices for increasing the safety and security of its vehicles. These features include **<<ADD AND DESCRIBE SECURITY FEATURES>>**. In addition to security equipment, vehicle operators are currently 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 who are responsible for correcting problems. The inspections include but are not limited to identification of suspicious packages.

VEHICLE SECURITY FEATURES
Exhibit 5

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			
Driver's only speakers			
Onboard cameras (audio capable)			
Audio microphones			

4.3.8 Management information systems security

[Modify as appropriate. Ensure section covers how MIS team counters cyber threats.]

<<ADD AGENCY NAME>>'s Management Information Systems (MIS) team maintains a firewall-protected Intranet system for management and other personnel. **<<ADD AGENCY NAME>>** has procured standard virus protection software and firewalls to protect its information technology infrastructure. For security purposes, the MIS team 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 log-in.

4.4 Internal security practices

[In developing internal security procedures/practices, the agency should use applicable APTA standards as well as FTA and TSA guidance

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

documents. Further, the agency should use the TSA/FTA Top 17 document to identify additional security procedures/practices not contained below.]

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 **<<ADD AGENCY NAME>>** has in place, including the source document in which the procedures can be found.

SECURITY PROCEDURES
Exhibit 6

Security Procedures	Security Procedures Exist?	Source Document
Background investigation[1]		
Badging and uniforms		
Communication with passengers		
Identifying suspicious behavior		
Passenger and baggage screening[2]		
Safe mail package handling		
Sensitive Security Information		
Security procurement language checklist		
Termination		
Trash container procurement and placement		
Unattended items		
Vehicle security sweeps		

1. Refer to TSA guidance document titled "Additional Guidance on Background Checks, Redress and Immigration Status" (http://www.tsa.gov/assets/pdf/guidance_employee_background_checks.pdf)
2. Ensure that procedures are ADA compliant and therefore consider and include passengers with disabilities, the elderly and their baggage.

4.5 External security component

The interface between **<<ADD AGENCY NAME>>** and other local, state and federal governmental agencies exists on all levels. These interfaces and relationships ensure that communica-

tions are ongoing and that the development and implementation of various security-related activities occurs, including exercises, simulations, drills and training.

4.5.1 Local law enforcement interface

[Describe interface between transit agency and local police department.]

4.5.2 Local/county/state interface

[Describe interface between transit agency and local/county/state 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.]

4.5.3 Federal interface

[Describe interface between transit agency and federal agencies. Examples may include FBI joint terrorism task force (JTTF), TSA's supported Regional Transit Security Working Groups (RTSWG) teams, civil support teams, etc.]

5. 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 **<<ADD TITLE>>**, the responsibility and authority for the preparation, implementation and enhancement of the plan rests with **<<ADD 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 a top priority 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.
- 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).

5.1 Employees

It is the responsibility of each and every employee to place safety and security as a top priority. 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. **<<ADD 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. **<<ADD 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 of 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 reader 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.

5.2 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.

5.2.1 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.
- Development of an effective notification and reporting system for security incidents and emergencies.
- Communication of security and emergency preparedness as top priorities 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.

5.2.2 Director of security (or equivalent)

[Modify as appropriate. This position may assume some or all of the duties described under 5.2.1]

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.

5.3 Agency divisions

It is the responsibility of each division to place security as a top priority. 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.]

5.3.1 Human resources

[Modify as appropriate.]

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

- Ensuring that all pre-employment screening processes 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.

5.3.2 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.

5.3.3 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.

5.3.4 Legal

[Add as appropriate.]

5.3.5 Operations

[Add as appropriate.]

5.3.6 Paratransit (if applicable)

[Add as appropriate.]

5.3.7 Risk management

[Add as appropriate.]

5.3.8 Safety

[Add as appropriate.]

5.3.9 Engineering

[Add as appropriate.]

5.3.10 Maintenance

[Add as appropriate.]

5.3.11 Enterprise Information and Technology Group

[Add as appropriate.]

5.4 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 **<<ADD 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 the **<<ADD AGENCY NAME>>**'s **<<ADD 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 **<<ADD 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 **<<ADD 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 Federal Bureau of Investigation 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 **<<ADD 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 **<<ADD AGENCY NAME>>**'s control.

In all cases, **<<ADD 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 6, "Threat, vulnerability and consequence identification and resolution."

5.4.1 Internal security incident reporting

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

<<ADD AGENCY NAME>> maintains Security and Emergency Preparedness incident reports **<<ADD 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)
- Probable 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)

5.4.2 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**

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

- **State safety oversight**
- **State and local government**
- **Agency-specific reporting requirements]**

6. Threat, vulnerability and consequence identification and resolution

[NOTE: The threat and vulnerability assessment methodology introduced herein is simply one approach. Other approaches may be just as useful and applicable to a transit agency.]

The inherently open nature of transit systems can be exploited by criminals, terrorists or other adversaries to commit crimes, acts of violence and other malicious and destructive acts. The greatest vulnerability and challenge faced by most transit systems with regard to security is how to maintain an open and inviting environment that is easily accessible to all members of the public while concurrently maintaining a level of security that prevents or minimizes, to the greatest extent possible, the occurrence of such acts throughout the system. Key steps to prevent, minimize and prepare for criminal and/or terrorist acts within or directed toward the agency's operations and services are designed to do the following:

- Identify potential threats facing the agency.
- Identify vulnerabilities within transit operations and services that may be exploited to carry out these threats.
- Analyze the potential impacts of each threat and vulnerability scenario.
- Develop and implement corrective actions and countermeasures to eliminate, minimize or otherwise prepare for attacks.
- Protect against identified threats and vulnerabilities.

6.1 Threat and vulnerability assessment

Threat and vulnerability assessments enable transit agencies to thoroughly evaluate potential threats, targets and vulnerabilities within their systems. The agency's processes for conducting such assessments are based on FTA recommended practices and industry guidelines, such as those detailed in FTA's *Public Transportation System Security and Emergency Preparedness Planning Guide* or that offered by TSA's Vulnerability Identification Self-Assessment Tool (VISAT). Threat and vulnerability assessments are typically completed **<<ADD FREQUENCY>>** or when conditions warrant (e.g., rising crime, raising of the NTAS) or when any new major rail lines or bus route is open, or during the design stage of any new major asset.

<<ADD AGENCY NAME>>'s assessment process entails identifying and evaluating system assets; identifying potential targets or threats within the system; examining the system to identify potential vulnerabilities that may be exploited to carry out threats; developing threat scenarios to

evaluate potential consequences; and developing and implementing countermeasures to eliminate, control or otherwise address identified threats and vulnerabilities to the extent practical.

All findings, recommendations and other information gathered or developed through the assessment process is considered SSI and shall remain under the strict control of the **<<ADD TITLE>>**. The **<<ADD TITLE>>**, with the assistance of other applicable personnel, is responsible for evaluating all assessment findings and proposed countermeasures; for determining if, where and when countermeasures should be implemented; and for tracking through fruition all corrective actions taken to address potential threats and vulnerabilities.

6.2 Asset identification and analysis

Transit system assets can be broadly defined as people (passengers, employees, contractors, visitors, surrounding communities, etc.), information (operations and maintenance procedures, computer network information, passwords and facility access codes, etc.), and property (stations, vehicles, buildings, communications systems, etc.). Asset analysis enables transit systems to quantitatively and qualitatively evaluate their assets to determine which are most significant to the system. **<<ADD AGENCY NAME>>** classifies those assets determined to have the highest level of value and/or criticality within the system as "key assets." This classification is based on the following:

- The value of the asset, including:
  - replacement or repair costs;
  - lost revenues resulting from halting or delaying service because of a loss of that asset; and
  - lost revenue resulting from decreased passenger confidence in utilizing that asset.
- The impact, if the asset is lost, on passengers, employees, public safety organizations, the general public and the agency, including:
  - economic impacts on the surrounding community, state or nation; and
  - the likelihood for mass casualties.
- The value of the asset to a potential adversary, including the level of visibility and prestige that would be gained by the adversary as a result of an attack.
- How, when and by whom the asset will be accessed and used, including the relative ease of access for ingress and egress of personnel and equipment required for an attack.
- Where the asset is located within the system as well as within the surrounding community, including its proximity to:
  - facilities containing chemical, biological, nuclear or radiological materials that could significantly contribute to the level of destruction resulting from an attack;
  - community, state or national structures that can be considered symbolic in nature (e.g., state or national monuments, government complexes or financial institutions, health care facilities, places of worship, sports arenas);

- secluded areas that are not immediately visible to the surrounding public; and
- areas of high crime.

By identifying key assets, **<<ADD AGENCY NAME>>** is able to direct its resources toward hardening security at critical locations, those locations would severely impact the overall system if lost.

6.2.1 All hazards threat and vulnerability identification and analysis

Threat analysis is a process that enables transit systems to "define the level or degree of the threats against a facility by evaluating the intent, motivation, and possible tactics of those who may carry them out." Vulnerability analysis is described by the FTA as a process that can be used by transit systems to identify "specific weaknesses with respect to how they may invite and permit a threat to be accomplished."

Through these forms of analysis, transit systems are able to better identify and evaluate the security-related risks that exist not only within their systems, but also within the operating environments and surrounding communities through which their services are provided. This can be a complex process that may require the involvement of outside parties, including local, state or federal law enforcement and emergency response agency representatives, and/or security experts.

The analysis process involves gathering and evaluating relevant information, including but not limited to the following:

- Security practices, protocols, crime deterrents and other countermeasures currently in place within the system, including an evaluation of their effectiveness.
- Historical data pertaining to past security breaches and other security-related incidents directed toward the system or toward other similar systems.
- Crime rate data in the communities and areas surrounding the system.
- Site layout information, such as the ease of accessibility, location of incoming utilities, hazardous storage materials locations, types of building construction, levels of lighting, etc.
- Existing criminal or terrorist threats that may be present within the system's operating environment or that may be directed toward the surrounding communities, state or nation as a whole and may impact the system.
- The response capabilities of the transit system and local emergency responders, such as police and fire/rescue personnel.

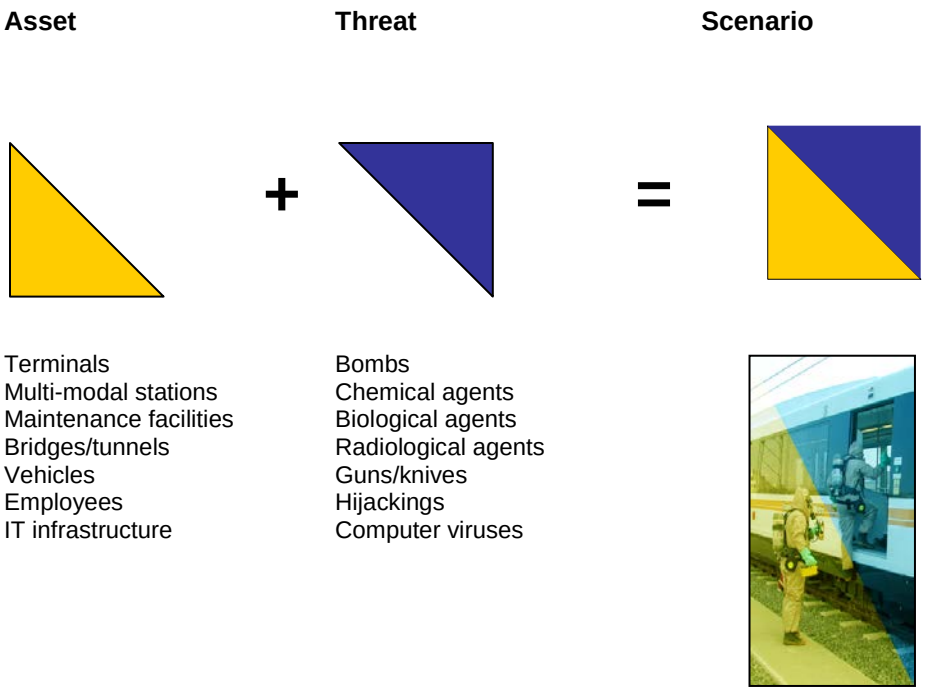
6.2.2 Scenario analysis

[NOTE: The importance of gathering intelligence received from the law enforcement community is not to be underemphasized. Based on intelligence, the type of

scenario being developed may change, as well as the level of priority for a given scenario.]

Once key assets, potential threats and system vulnerabilities have been identified, threat scenarios can be developed to evaluate the types of potential attacks and outcomes that may be waged against and experienced by the transit system. The scenario analysis process combines information gained through each of the other analysis processes, as depicted in Exhibit 7.

THREAT SCENARIO DEVELOPMENT
Exhibit 7



Each threat scenario is then evaluated to determine its likelihood and severity of occurrence, giving consideration to the extent of identified threats and vulnerabilities, and the level of risk associated with its occurrence. This process is depicted in Exhibits 8 and 9. In our process "likelihood" is tied into "vulnerability"; combining vulnerability with impact gives us the level of criticality.

SCENARIO EVALUATION CRITERIA

Exhibit 8

Vulnerability		Impact	
A	Very easy	I	Loss of life
B	Relatively easy	II	Serious injuries, major service impact, >$250,000 damage
C	Difficult	III	Minor injuries, minor service impact, <$250,000 damage
D	Very difficult	IV	No injuries, no service impact
E	Too difficult		

Criticality matrix

	I	II	III	IV
A	H	H	S	S
B	H	H	S	L
C	H	S	L	L
D	S	L	L	L
E	S	L	L	L

H = High
S = Serious
L = Low

LEVELS OF RISK

Exhibit 9

Risk level	Assets/impacts	Threat	Vulnerability
Critical	Loss of life	Definite threat exists Both the capability and intent exist Similar assets are targeted on a frequent or recurring basis	Few effective countermeasures exist Known adversaries could easily exploit the asset
High	Serious injuries Major service impact >$250,000 damage	Credible threat exists Plausible capability and intent exists Related incidents have occurred on similar assets in the past	Some countermeasures exist, but multiple weaknesses still exist Many adversaries could exploit the asset

LEVELS OF RISK
Exhibit 9

Risk level	Assets/impacts	Threat	Vulnerability
Medium	Minor injuries Minor service impact <$250,000 damage	Potential threat exists Adversary's desire to gain capability and intent exists Capability could exist through a third party	Effective countermeasures exist, but at least one weakness still exists Some known adversaries could exploit the asset
Low	No injuries No service impact	Little or no credible evidence of capability or intent exists No history of actual or planned threats	Multiple levels of effective countermeasures exist Few or no known adversaries would be capable of exploiting asset

6.3 Countermeasure development

Countermeasures and corrective actions are developed at the completion of the analysis processes to eliminate or mitigate identified system threats and vulnerabilities. Effective countermeasures will typically include mutually supporting engineering and administrative elements. Examples of engineering countermeasures include the following:

- Installing physical barriers designed to reduce the asset's vulnerability to unauthorized access or explosive or other incendiary attacks.
- Installing integrated intrusion detection and alarm systems throughout key facilities.
- Installing chemical, biological, radiological and/or nuclear detection devices at facility and station locations.

Administrative countermeasures include the following:

- Increasing the frequency of security patrols at key asset locations.
- Increasing security-related training to improve the abilities of employees to identify suspicious packages or activities.
- Conducting drills and tabletop exercises involving security-related scenarios.
- Developing working groups and information exchange committees with local law enforcement and emergency response agencies.

In developing the countermeasures, consideration must be given to not only the initial costs of procurement and implementation, but also to the associated maintenance costs and expected lev-

el of effectiveness at eliminating or controlling the threat or vulnerability. It is also important to take into account that during special events, additional security measures may be required. Such conditions may adversely impact the effectiveness of normal countermeasures.

The **<<ADD TITLE>>**, with the assistance of other applicable personnel, is responsible for developing countermeasures and corrective actions; for determining if, where and when countermeasures should be implemented; and for documenting and tracking through fruition all steps taken to address potential threats and vulnerabilities. Exhibit 10 provides a sample list of typical countermeasures used in the transit industry to eliminate and control threats and vulnerabilities.

[Agency should add checkmarks to the table below as applicable.]

PUBLIC TRANSPORTATION COUNTERMEASURES

Exhibit 10

Countermeasures	Administrative			Physical			
	Planning	Coordination with local responders	Training and drills	Access control	Surveillance	Blast mitigation	WMD protection
Identifying unusual or out-of-place activity							
Security screening and inspection procedures[1]							
Enhancing access control for stations/vehicles							
Securing perimeters for non-revenue areas							
Denying access to authorized-only areas							
Security vulnerable areas (target hardening)							
Removing obstacles to clear line of sight							
Protecting parking lots							
Enhanced access control for control center							
Securing critical functions and backups							
Promoting visibility of uniformed staff							

PUBLIC TRANSPORTATION COUNTERMEASURES

Exhibit 10

Countermeasures	Administrative			Physical			
	Planning	Coordination with local responders	Training and drills	Access control	Surveillance	Blast mitigation	WMD protection
Removing spaces that permit concealment							
Reinforcing natural surveillance							
Procedures for vehicle and station evacuation[2]							
Coordination with community planning efforts							
Backing up critical computer systems							
Revising lost-and-found policies							
Securing tunnels and elevated structures							
Elevating/securing fresh air intakes							
Protecting incoming utilities							
Establishing mail-handling procedures							
Identifying appropriate personal protective equipment and training							
Preparing response folders and notebooks for facilities and vehicles							
Familiarization training for local emergency response agencies							
Planning for scene management and emergency response							

Source: The Public Transportation System Security and Emergency Preparedness Planning Guide, *U.S. Department of Transportation*

1. Screening procedures should include ADA-compliant procedures for the disabled, the elderly and their baggage.
2. Vehicle and station evacuation procedures should consider and include procedures for the disabled and the elderly.

6.4 Security testing and inspections

Security testing and inspection activities are conducted at least once a year or as mandated by federal regulations. Security testing and inspections are performed to do the following:

- Assess the current state of the Security and Emergency Preparedness Program.
- Monitor the effectiveness of countermeasures implemented to eliminate or control threats and vulnerabilities.
- Identify any other potential threats and vulnerabilities within the system.
- Evaluate **<<ADD AGENCY NAME>>**'s state of security preparedness with regard to equipment and resource availability, employee proficiency and levels of training, and local law enforcement and emergency response agency system knowledge and response capabilities.
- Enhance and promote security awareness throughout transit operations and services.

While performing these activities, several levels of equipment deficiencies may be identified. For instance, if a single video camera is used to monitor a bus stop or a parking lot, the camera must be functional at all times to ensure that the bus stop or parking area can be adequately monitored. However, if two cameras are used to monitor the bus stop or parking area, then the loss of one of the cameras may be tolerated for a short period of time. In all cases, any equipment conditions found to be unacceptable during the inspection shall be reported to the appropriate maintenance personnel and corrected immediately.

7. Security design

<<ADD 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, terminal, 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/Volpe Transit Security Design Considerations" document and FTA's Safety and Security Management Plan.

[APTA's Crime Prevention Through Environmental Design (CPTED) Recommended Practice, created by APTA's Infrastructure Security Standards Working Group, is another great resource for the transit agency. At the time of publication of this SEPP, the final version of the document was not yet complete.]

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

7.1 Security design considerations

[This section should reference the FTA/Volpe document.]

<<ADD 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. **<<ADD AGENCY NAME>>** uses the FTA and Volpe's co-developed "Transit Security Design Considerations" report as guidance.

7.2 Crime Prevention Through Environmental Design (CPTED)

[This section should reference the APTA Infrastructure Committee CPTED Recommended Practice.]

<<ADD 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.

7.3 Safety and Security Management Plan (SSMP)

[This section should reference the FTA's SSMP.]

<<ADD 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. For specific details on requirements, visit http://transit-safety.volpe.dot.gov/publications/security/SSMP_FAQs_Final.doc.

8. Threat levels and alerts

<<ADD AGENCY NAME>> recognizes the threat condition designations as defined by the National Terrorism Advisory System (NTAS). **<<ADD 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, **<<ADD AGENCY NAME>>** keeps current of the federal threat level in addition to regularly receiving and monitoring alerts distributed by other organizations, including the FBI.

8.1 National Terrorism Advisory System (NTAS)

In April 2011, DHS introduced NTAS. NTAS replaced the color-coded threat conditions used by DHS, the Homeland Security Advisory System, which had been in place since 2002. Through the NTAS, DHS and other federal entities will issue alerts based on credible threat intelligence. Alerts will be defined in one of two ways:

- Elevated Threat: Warns of a credible terrorist threat against the United States
- Imminent Threat: Warns of a credible, specific, and impending terrorist threat against the United States

SAMPLE NTAS ALERT
Exhibit 11

These alerts may be sent directly to law enforcements agencies, affected stakeholders, or in some cases the general public through official and social media channels. The 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. **<<ADD AGENCY NAME>>** uses the NTAS as a guide for its own preparation and response to alerts.

In addition the FTA, through its *Transit Agency Security and Emergency Management Protective Measures* guidance document (November 2006) provides two additional threat levels and associated protective measures. They are the Active Incident (an actual emergency, which might include a terrorist attack, accident or natural disaster) and the Recovery phase following an incident.

8.1.1 Active incident

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

- Responding to casualties.
- Assisting in evacuations.
- Reporting incident (see Section 5.4)
- Inspecting and securing transit facilities.
- Helping with other tasks directed by local emergency management personnel.

8.1.2 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. **<<ADD 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 inquires about services.
- Undertaking other activities necessary to restore transit service.

8.2 Federal Bureau of Investigation alerts

<<ADD 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. **<<ADD 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 **<<ADD PHONE NUMBER>>** or via the Web at **<<ADD WEB ADDRESS>>**.

[Add name of specific contact, perhaps with JTTF]

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

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

<<ADD AGENCY NAME>> regularly reviews information disseminated by the PT-ISAC. In January 2003, the U.S. Department of Transportation designated the American Public Transportation Association (APTA) as the sector coordinator in the creation of a Public Transit 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 cyber-security 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
1-866-PT-ISAC-1 (784-7221)
www.surfacetransportationisac.org

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

<<ADD AGENCY NAME>> regularly reviews information disseminated by TSA through DHS's HSIN-PT. HSIN-PT 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 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. TSA also uses its emergency notification system, called TSA Alerts, sometimes in conjunction with HSIN-PT, to advise transit agencies of significant threats or terrorist attacks.

9. Training

An important aspect of every employee's job is his or her individual responsibility for safety and security. As a result, **<<ADD AGENCY NAME>>** develops, maintains and updates the security-related training curriculum for all employees. Targeted security training at **<<ADD 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.

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

9.1 General employee training (all employees)

[General employee training may be offered as initial and refresher training. Potential concepts and principles include transit operations and services; general rules, policies, and procedures; how to best utilize 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.]

9.2 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.]

9.3 Vehicle operator training

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

9.4 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.]

9.5 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**

<When transit agency data is added to this document, it must be labeled SENSITIVE SECURITY INFORMATION.>

- **Hazardous materials storage locations**
- **Communications with transit personnel**
- **Transit organizational roles and responsibilities**
- **Coordination of functions/lines of authority (e.g., personnel responsibilities during events)**
- **Relevant transit rules and operating procedures]**

9.6 NIMS training

[National Incident Management System 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 ICS as the national incident management model, when to institute an area command, when to institute a multi-agency coordination system, benefits of using a joint information system (JIS) for public information, managing resources using NIMS, and technology.]

10. Exercises and drills

[This section should be modeled after APTA's drills and standards document developed by the Emergency Management Standards working group. Include here 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 the 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.]

A program for effective joint training exercises and drills involving **<<ADD AGENCY NAME>>** and other external agencies including local police, fire and emergency management agencies is maintained by the **<<ADD TITLE>>** or an appointee. This program includes tabletop exercises and "in-the-field" full-scale mock emergency drills.

Tabletop exercises involve presenting various emergency scenarios to teams of participants with the purpose of allowing the teams to discuss the appropriate response actions. Tabletop exercises are conducted to prepare **<<ADD AGENCY NAME>>**, law enforcement and emergency response personnel to respond to emergencies involving transit passengers and equipment. Drills differ from tabletop exercises in that they involve utilizing actual equipment, facilities and personnel together to form a full-scale mock emergency.

The purpose of these drills is to demonstrate that participants understand their individual roles and responsibilities and are familiar with the equipment and layout of facilities. The results of the drills are fed back into future transit drill scenarios as necessary. Drills 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 **<<ADD AGENCY NAME>>** has participated in and will participate in, see Exhibit 12.

EXERCISE LIST
Exhibit 12

Fiscal year	Description of exercises conducted

11. Public awareness

<<ADD 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
- *Transit Watch* (sponsored and developed by the FTA)

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 al-

ways 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, persons, 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.

12. Evaluation and modification

The evaluation and modification process is an excellent opportunity to ensure that the SEPP effectively eliminates and mitigates security threats. As **<<ADD TRANSIT AGENCY>>**'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 **<<ADD FREQUENCY>>** and updated as needed to ensure that it remains up to date and consistent with all other **<<ADD TRANSIT AGENCY>>** rules, procedures and policies.

12.1 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 suggestions for improvement, either to fine-tune the program or to implement new objectives in a revised plan. The **<<ADD TITLE>>** or designee is responsible for the evaluation or review process.

12.2 Modification

Modifications occur after a significant security breach and after any emergency drill or exercise. 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 **<<ADD TITLE>>** for review.

If system changes occur outside a scheduled review period of the plan, the **<<ADD TITLE>>** ensures that the changes are reviewed and incorporated as necessary. The **<<ADD TITLE>>** has the primary responsibility for reviewing and updating the SEPP. Change bulletins are issued once changes are made to the plan, provided 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 **<<ADD TITLE>>**.

12.3 SEPP control

The **<<ADD 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 **<<ADD TITLES>>** as well as all directors, supervisors and managers.

Appendix A: Common threats identification

Category	Hazard
Natural	drought
	earthquake
	flash flooding
	flooding (river or tidal)
	high winds
	hurricane
	landslide
	tornado
	wildfire
	winter storm
Technological	dam failure
	energy or fuel shortage
	hazmat or oil spill (fixed site or in transport)
	major structural fire
	nuclear facility incident
	power outage
Societal	civil unrest or riot
	strike
	civil panic or looting
Security	violent or other crime
	bomb threats
	chemical, biological or radiological threats
	chemical, biological or radiological device/release
	explosive device/detonation
	hijackings
	sabotage or vandalism
	terrorism
	trespassing
	workplace violence

Source: The Public Transportation System Security and Emergency Preparedness Planning Guide, *U.S. Department of Transportation*

Appendix B: Points of contact list

Contacts					
Name	**Company**	**Title**	**Work phone**	**Cell phone**	**E-mail**

Appendix C: Communication tree

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