The BASE Resource Kit (BRK) is designed to help transit agencies effectively prepare for the BASE review process. The BRK provides direct resources and web-links to TSA, FEMA, FTA and APTA reference documents.
INTRODUCTION

The Baseline Assessment of Security Enhancement (BASE) program is designed to establish a security standard for mass transit rail and bus, and passenger rail system security programs and assess progress. The BASE program is designed to meet requirements identified in the 9/11 Commission Act’s security assessment section, which directs the Transportation Security Administration (TSA) to identify critical assets, infrastructure and systems and their vulnerabilities and assist bus and public transportation authorities to address their security programs. This voluntary review of transit agency security programs focuses on multiple categories identified by the transit community as fundamentals for a sound transit security program.

The BASE review includes a comprehensive evaluation of program elements, which include but are not limited to the transit agency’s security plans, security awareness and emergency response training, drills/exercise programs, public outreach efforts, and background check programs. TSA Surface Transportation Security Inspectors coordinate and conduct BASE reviews; they also perform an in-depth security program analysis for the participating mass transit, passenger rail or bus system, while identifying possible security vulnerabilities, options for consideration and smart practices.

Since 2006, the TSA Surface Inspection program has completed over 500 BASE reviews on large mass transit, passenger rail and bus systems that have higher passenger volumes. These large systems collectively account for over 80 percent of all users of public transportation, and potentially face the greatest risk from terrorist intentions. TSA Transportation Security Inspectors also conduct BASE reviews on smaller transit agencies to assist them on raising their overall security posture.

PURPOSE

The BASE program is intended to elevate the security posture and readiness throughout the mass transit, passenger rail and bus modes of transportation by implementing and sustaining baseline security measures applicable to the operating environment and system characteristics. The Baseline Assessment and Security Enhancement (BASE) Resource Kit (BRK), formerly titled the Performance Improvement Action Plan (PIAP) tool kit, is designed to help transit agencies effectively prepare for BASE reviews, as well as function as follow-up resource tool for providing cost-effective measures in addressing weaknesses identified in the BASE. The BRK shall offer the transit agencies and surface transportation security inspectors reference information necessary to reconnect in the interest of securing identified vulnerabilities. The reference sources contained in BRK are hyperlinks that provide immediate access to templates, security standards and best practices, and other resources made available by federal and industry security partners; FTA, APTA, FEMA and TSA. For additional information related to the BASE
program, contact the TSA Office of Security Operations (OSO), Surface Compliance Branch at STSIP@dhs.gov or Office of Security Policy and Industry Engagement (OSPIE), Mass Transit at tsa.seccoord@tsa.dhs.gov.
CONTENTS

1.000 Establish Written System Security Plans (SSPs) and Emergency Response Plan (ERP) ........... 5
  
1.100 System Security Plan (SSP) .............................................................................................................. 5
  
1.200 Emergency Response Plan (ERP) ............................................................................................................ 9
  
2.000 Define Roles and Responsibilities for Security and Emergency Management .................. 11
  
2.100 System Security Plan (SSP) .................................................................................................................. 11
  
2.200 Emergency Response Plan (ERP) ........................................................................................................ 14
  
3.000 Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control .......................................................... 16
  
4.000 Coordinate Security and Emergency Management Plan(s) with local and regional agencies . 17
  
5.000 Establish and Maintain a Security and Emergency Training Program ................................. 20
  
6.000 Establish plans and protocols to respond to the DHS NTAS .................................................... 27
  
7.000 Implement and reinforce a Public Security and Emergency Awareness program .................. 28
  
8.000 Establish and use a Risk Management Process to assess and manage threats, vulnerabilities and consequences ............................................................................................................... 31
  
9.000 Establish and use an information sharing process for threat and intelligence information .... 33
  
10.000 Conduct Tabletop and Functional Drills .................................................................................... 34
  
11.000 Developing a Comprehensive Cyber Security Strategy ............................................................. 38
  
12.000 Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors ............................................................................................................................. 41
  
13.000 Conduct Physical Security Inspections ...................................................................................... 47
  
14.000 Conduct Background Investigations of Employees and Contractors ........................................ 50
  
15.000 Control Access to documents of security critical systems and facilities ............................... 51
  
16.000 Process for handling and access to Sensitive Security Information (SSI) .............................. 52
  
17.000 Audit Program ................................................................................................................................. 54
## PAGE CONTROL CHART

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/13/2017</td>
<td>Pg. 1, Introduction</td>
<td>Number of BASEs completed changed from 150 to 500.</td>
</tr>
<tr>
<td>10/13/2017</td>
<td>Pg. 14, 2.109</td>
<td>Email to submit Coordinator Information</td>
</tr>
</tbody>
</table>
1.000 Establish Written System Security Plans (SSPs) and Emergency Response Plan (ERP)

The purpose of the SSP (also referred to as Security and Emergency Preparedness Plan) is to ensure a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events.

<table>
<thead>
<tr>
<th>1.100</th>
<th>System Security Plan (SSP)</th>
<th>BASE RESOURCE LIBRARY:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.101</td>
<td>Does the transit agency have a System Security Plan (SSP) which addresses personnel security, facility security, vehicle security and Threat/Vulnerability Management?</td>
<td><strong>Standard:</strong> SSP is a well-developed plan, complete with detailed policies and procedures related to personnel security, facility security, vehicle security and threat/vulnerability management. SSP is missing no key elements and has been completely implemented by the agency.</td>
</tr>
<tr>
<td>1.102</td>
<td>Does the SSP identify and actively monitor the goals and objectives for the security program?</td>
<td><strong>Standard:</strong> Goals and objectives are identified, documented and actively monitored to ensure the SSP is fulfilling its purpose.</td>
</tr>
<tr>
<td>1.103</td>
<td>Does a written policy statement exist that endorses and adopts the policies and procedures of the SSP that is approved and signed by top management, such as the agency's chief executive?</td>
<td><strong>Standard:</strong> Policy statement is a well-developed written statement (memo, mission statement, etc.) that includes all elements: endorsement statement, applicability, authority establishing the plan, and approval signature from the agencies chief executive.</td>
</tr>
<tr>
<td>1.104</td>
<td>Is the SSP separate from the agency’s System Safety Program Plan (SSPP)?</td>
<td><strong>Standard:</strong> SSP is a stand-alone document, separate from the System Safety Program Plan.</td>
</tr>
</tbody>
</table>

**FTA – Model System Security Program Plan (SSP) Template**

**FTA System Security and Emergency Preparedness Plan (SEPP) Template**

**FTA System Security and Emergency Preparedness Plan (SEPP) Appendix G**

**APTA - Security Planning for Public Transit**

**49 CFR 659.21 SSP General Requirements**
1.105  **Do the Security and Emergency Response Plans address protection and response for critical systems?** (i.e., facilities, stations, terminals, offices building, underwater tunnels, underground stations/tunnels and other critical systems)

**Standard:** Security plans address specific policies and procedures related to security and emergency response for underwater/underground infrastructure (if system has any) and/or other critical systems.

1.106  **Does the SSP contain or reference other documents establishing procedures for the management of security incidents by the operations control center (or dispatch center) or other formal process?**

**Standard:** Procedures for the management of security incidents by the OCC (or dispatch center) is identified in the Security Plan. Specific procedures are in place and documented in the SSP. If documented elsewhere, such as in a stand-alone Emergency Response Plan, the SSP references that document.

1.107  **Does the SSP contain or reference other documents establishing plans, procedures, or protocols for responding to security events with external agencies (such as law enforcement, local EMA, fire departments, etc.)?**

**Standard:** Well-developed, *specific* procedures are in place and documented in the SSP or as part of another document and referenced in the SSP.

1.108  **Has the agency partnered with local law enforcement/first responders to develop Active Shooter procedures or protocols?**

**Standard:** Active Shooter procedures and protocols were developed with local law enforcement/first responder input to ensure agency’s response is in concert with law enforcement/first responder’s response to an Active Shooter threat.
<table>
<thead>
<tr>
<th>1.109</th>
<th>Does the SSP contain or reference other documents that establish procedures or protocols for responding to active shooter events?</th>
<th><strong>Active Shooter Pocket Card</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Well-developed, <em>specific</em> procedures or protocols are in place that addresses Active Shooter. These procedures or protocols are documented in the SSP or as part of another document, such as a stand-alone Emergency Response Plan, and referenced in the SSP.</td>
<td></td>
</tr>
<tr>
<td>1.110</td>
<td>Does the SSP contain or reference other documents that establish protocols addressing specific threats from (i) Improvised Explosive Devices (IED) and (ii) Weapons of Mass Destruction (chemical, biological, radiological hazards)?</td>
<td><strong>Model Program for Responding to a Package with Suspicion of a Bio Threat - IAFC Oct. 2008</strong>&lt;br&gt;<strong>Chemical Weapons Improved Response Program (CWIRP)</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Well-developed, <em>specific</em> protocols are in place that addresses IED and WMD. These protocols are documented in the SSP or as part of another document, such as in stand-alone Emergency Response Plan (ERP), and referenced in the SSP.</td>
<td></td>
</tr>
<tr>
<td>1.111</td>
<td>Are visible, random security measures, based on employee type, integrated into security plans to introduce unpredictability into security activities for deterrent effect?</td>
<td><strong>APTA- Random Counterterrorism Measures on Transit Systems (close sign in link and document will automatically open)</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Random, unpredictable measures are well-documented with specific measures assigned by employee-type. Includes both security and non-security personnel.</td>
<td></td>
</tr>
<tr>
<td>1.112</td>
<td>Does the SSP include provisions requiring that security be addressed in extensions, major projects, new vehicles and equipment procurement and other capital projects, and including integration with the transit agency’s safety certification process?</td>
<td><strong>APTA - Security Planning for Public Transit</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Security plays a role in all new projects and procurements and is part of the safety certification process. This is required by the agency and documented in the SSP. There is a formal process in place for planning and implementing a project with security playing a role in various phases, including: planning, engineering, construction, testing, and final implementation.</td>
<td></td>
</tr>
<tr>
<td>1.113</td>
<td>Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?</td>
<td><strong>FEMA - CPTED</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>CPTED principles are addressed in all facilities and fully implemented. These principles are documented in the SSP or other documents (which are referenced in the SSP).</td>
<td>APTA Crime Prevention Through Environmental Design (CPTED (Sign in to APTA’s website or close login screen and document will open))</td>
</tr>
<tr>
<td>1.114</td>
<td>Does the SSP require an annual review?</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Annual review is a written requirement with verification measures in place (signed and dated).</td>
<td></td>
</tr>
<tr>
<td>1.115</td>
<td>Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Reports are produced once per year at a minimum and are detailed and developed regularly to track the agency's progress in meeting the goals and objectives identified in the SSP.</td>
<td></td>
</tr>
<tr>
<td>1.116</td>
<td>Has an annual review of the SSP been performed and documented in the preceding 12 months?</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Annual review is verifiable by document review.</td>
<td></td>
</tr>
<tr>
<td>1.117</td>
<td>Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP?</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Documented process for securing SSO review and approval of SSP is included in writing, or directly referenced, in the SSP.</td>
<td></td>
</tr>
<tr>
<td>1.118</td>
<td>Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Approval (including date of approved) is verifiable through document review.</td>
<td></td>
</tr>
</tbody>
</table>
### 1.200 Emergency Response Plan (ERP)

<table>
<thead>
<tr>
<th>1.201</th>
<th>Does the transit agency have an Emergency Response Plan (ERP) which addresses specific policies and procedures related to emergency response?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>ERP is a well-developed plan, complete with detailed policies and procedures related to emergency response. ERP is missing no key elements and has been completely implemented by the agency.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.202</th>
<th>Does a written policy statement exist that endorses and adopts the policies and procedures of the ERP that is approved and signed by top management, such as the agency's chief executive?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Policy statement is well developed and includes all elements: endorsement statement, applicability, authority establishing the plan, and approval signature from the agencies chief executive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.203</th>
<th>Does the ERP require an annual review to determine if it needs to be updated?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Annual review is a written requirement with verification measures in place (signed and dated).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.204</th>
<th>Has an annual review of the ERP been performed and documented in the preceding 12 months?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Annual review, including date and signature is verifiable by document review.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.205</th>
<th>Does the ERP include a process or review provision to ensure coordination with the transit agency’s SSPP and SSP?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>ERP includes documented provisions that ensure its coordination with the agency's safety and security plans.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.206</th>
<th>Has the transit agency received documentation from the SSO confirming its review and approval of the ERP currently in effect?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Approval (including date of approval) is verifiable.</td>
</tr>
<tr>
<td>1.207</td>
<td>Does the ERP contain or reference other documents establishing plans, procedures, or protocols for responding to emergency events with external agencies? (i.e. law enforcement, local EMA, fire departments, etc.)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Well-developed, <em>specific</em> procedures are in place and documented in the ERP <em>or</em> as part of another document and referenced in the ERP.</td>
</tr>
<tr>
<td>1.208</td>
<td>Does the ERP contain or reference other documents that establish procedures for the management of emergency events, including those to be employed by the operations control center (or dispatch center)?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The responsibility for the management of security incidents has been assigned to the Operations Control Center (or dispatch center). Specific procedures are in place and documented in the ERP. If documented elsewhere, the ERP references that document.</td>
</tr>
<tr>
<td>1.209</td>
<td>Does the ERP contain or reference other documents to provide for Continuity of Operations (COOP) while responding to emergency events?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Continuity of Operations plans exists and are included as part of the ERP (or in another document that is referenced in the ERP).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1.210</td>
<td>Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Business Recovery Plan is a comprehensive plan. Essential business functions (HR, IT, etc.) have been identified, and the agency has taken steps to protect vital business information (records, data, etc.). The plan outlines steps to be taken to return the agency to a &quot;normal&quot; operational status in a timely manner. Policies and procedures (including who activates the plan and how the agency transitions from emergency operations to business recovery) are detailed.</td>
</tr>
</tbody>
</table>
### 1.211 Does the agency have a written Business Continuity Plan and COOP to guide restoration of facilities and services following an emergency event?

**Standard:** Business Continuity Plan is a comprehensive plan. Essential operations functions (bus operations, security infrastructure) and key facilities have been identified. Policies and procedures are detailed and effective in mitigating any disruption to operations. Continuity responsibilities are identified (including who is responsible for activating the plan). Any resulting SOP changes are documented.

- **NFPA 1600: Standard on Disaster-Emergency Management and Business Continuity Programs**
- **Ready.gov: Business Continuity Plan**

### 1.212 Does the agency have a back-up operations control center capability?

**Standard:** The agency has identified a back-up location for operations control. This secondary location can quickly become fully operational and is equipped to function in the same capacity as the primary Operation Control Center.

- **APTA - Creating an Alternate or Backup Operations Control Center**

### 2.000 Define Roles and Responsibilities for Security and Emergency Management

The purpose of this section is to ensure that agency management and employees are knowledgeable of and well-prepared to develop, disseminate and implement written Security and Emergency Management Plans.

#### 2.100 System Security Plan (SSP)

#### 2.101 Does the SSP establish and assign responsibility for implementation of the security program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?

**Standard:** The implementation of the security program has been assigned to a Senior Manager who is a "direct report" to the CEO. This responsibility is documented in the SSP.

- **FTA System Security and Emergency Preparedness Plan (SEPP) Appendix G:**
- **FTA System Security and Emergency Preparedness Plan (SEPP) Template:**
- **APTA Recommended Practice for SEPP**
<table>
<thead>
<tr>
<th>2.102</th>
<th>Has the agency established documented lines of delegated authority and lines of succession of security responsibilities?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has established comprehensive policies and procedures related to &quot;chain of command&quot; and &quot;lines of succession&quot; for security responsibilities. The policy is well documented, and lines of succession include multiple individuals based on the importance of responsibilities (more important roles have longer, multi-personnel lines of succession). This policy is shared with agency managers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.103</th>
<th>Does the SSP or other documents establish roles and responsibilities for security and/or law enforcement personnel based on title and/or position?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Roles and responsibilities of security personnel are assigned by position and documented in the SSP or other documents. Roles are comprehensive and detailed for all position-types, from security managers to supervisors to front-line security personnel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.104</th>
<th>Does the SSP or other documents establish security-related roles and responsibilities for non-security personnel based on title and/or position? (i.e., operators, conductors, maintenance workers and station attendants)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Specific security-related responsibilities have been established for non-security personnel and assigned based on job function for all (or a majority of) employees. Roles and responsibilities are comprehensive and clearly identify the role non-security personnel play in regards to security. These responsibilities are documented in the SSP or other documents.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.105</th>
<th>Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Senior staff and management conduct security meetings on a quarterly basis, at minimum, to review recommendations for changes to plans and processes.</td>
</tr>
<tr>
<td>2.106</td>
<td>Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings?</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>A formal security committee or working group has been established. This group meets multiple times per year at predictable intervals (at least once per quarter) to review security incident reports, trends, and program audit findings. All applicable security items are addressed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.107</th>
<th>Are informational briefings with appropriate personnel held whenever security protocols, threat levels, or protective measures are updated or as security conditions warrant?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Policies and procedures are in place to ensure that frontline personnel are made aware of anything relevant to the security of their transit system. Agency utilizes a variety of message delivery systems for security messages based on message importance: face-to-face verbal, electronic dispersal, written-memo system, and bulletin board postings. The agency has also developed a means of tracking/monitoring who has (or has not) received high-importance informational briefings. (acknowledgement/signature sheet, email receipt, etc.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.108</th>
<th>Have reference guides or other written instructions or procedures, appropriate to job function, been distributed to transit employees to implement the requirements of the SSP?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Individual written guides or reference material based on job function have been provided to employees to assist employees with the implementation of security procedures (ex. Driver’s manual, SOP, etc.).</td>
</tr>
<tr>
<td>2.109</td>
<td>Has the agency appointed a Primary and Alternate Security Coordinator to serve as its primary and immediate 24-hr contact for intelligence and security-related contact with TSA and are the names of those Coordinators on file with TSA OSPIE office correct?</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has appointed a Primary and Alternate Security Coordinator that meet all criteria established by TSA and provided TSA the names of these individuals.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.110</th>
<th>Does the agency maintain a record of security related incidents that are reported within the agency?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Agency maintains a record of security related incidents that are reported within the agency. Agency has the ability to review incidents that have occurred over one year earlier.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.200</th>
<th>Emergency Response Plan (ERP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.201</td>
<td>Does the ERP establish and assign responsibility for implementation of the emergency response program to a Senior Manager who is a &quot;direct report&quot; to the agency's Chief Executive Officer?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The implementation of the security program has been assigned to a Senior Manager who is a &quot;direct report&quot; to the CEO. This responsibility is documented in the ERP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.202</th>
<th>Are detailed, comprehensive emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency takes an all-inclusive, system-wide approach to emergency preparedness. Emergency response roles and responsibilities have been developed and are assigned for all departments. Roles are comprehensive, detailed, and documented.</td>
</tr>
</tbody>
</table>

Submit Security Coordinators contact information to: tsa.seccoord@tsa.dhs.gov

**BASE RESOURCE LIBRARY:**

FTA System Security and Emergency Preparedness Plan (SEPP) Template

FTA System Security and Emergency Preparedness Plan (SEPP) Appendix G:
<table>
<thead>
<tr>
<th>2.203</th>
<th>Does the ERP establish emergency response roles and responsibilities for all front-line personnel based on title and/or position? (i.e. system law enforcement, system security officials, train or vehicle operators, conductors, station attendants, maintenance workers)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Roles and responsibilities of frontline personnel are assigned by position and documented in the ERP. Roles are comprehensive and detailed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.204</th>
<th>Has the ERP been distributed to appropriate departments in the organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency takes a total approach to emergency response, including all departments in the process. All departments have been provided a copy of the ERP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.205</th>
<th>Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the ERP?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Individual written guides or reference material based on job function have been provided to all employees to assist employees with the implementation of emergency procedures.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.206</th>
<th>Are senior staff and middle management ERP coordination meetings held on a regular basis?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Senior staff and management conduct ERP coordination meetings on a monthly basis.</td>
</tr>
<tr>
<td>2.207</td>
<td>Are informational briefings with appropriate personnel held whenever emergency response protocols are substantially changed or updated?</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Standard:</strong> Policies and procedures are in place to ensure that frontline personnel are made aware of anything relevant to the emergency response plan. Agency utilizes a variety of message delivery systems for security messages based on message importance: face-to-face verbal, electronic dispersal, written-memo system, and bulletin board postings. The agency has also developed a means of tracking/monitoring who has (or has not) received high-importance informational briefings (acknowledgement/signature sheet, email receipt, etc.).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.000</th>
<th>Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The purpose of this section is to ensure that agency front-line supervisors and employees are trained, informed and prepared to implement security and emergency response protocols and procedures appropriate to their function.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.101</th>
<th>How frequently do managers and supervisors provide information to front-line personnel where security and emergency response issues are the primary focus?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> Frontline employees receive a weekly briefing from their immediate supervisor regarding security and emergency preparedness. Security and emergency response issues are the primary focus of briefings (or equal to that of safety).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.102</th>
<th>How frequently are supervisor, manager, and/or foreperson security review and coordination briefings held?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> Supervisor/management security review and coordination meetings are held on a monthly basis.</td>
<td></td>
</tr>
<tr>
<td>3.103</td>
<td><strong>Does the agency have a program that actively utilizes a formal process for confirming personnel have a measurable working knowledge of security protocols? (i.e. internal audits, challenge procedures, qualification testing)</strong></td>
</tr>
<tr>
<td>--------</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong> The agency actively engages its workforce to ensure a high rate of security knowledge. Agency utilizes a formal, measurable and on-going system of verification, such as internal audits, challenge procedures, or qualification testing. The program—or procedures/responsibilities related to it—is documented.</td>
<td></td>
</tr>
</tbody>
</table>

| 3.104 | **Does the agency have a written policy requiring managers and/or supervisors to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?** |
|--------|
| **Standard:** There is a written policy that requires leadership to debrief frontline personnel regarding their involvement in or management of any security or emergency incidents. |

| 4.000 | **Coordinate Security and Emergency Management Plan(s) with local and regional agencies** |
|--------|
| The purpose of this section is to enhance and elevate security and emergency preparedness by coordinating, training, exercising and testing agency capabilities with local and regional emergency response agencies. |

| 4.101 | **Have Mutual Aid agreements been established between the transit agency and entities in the area that would be called upon to supplement the agency’s resources in the event of an emergency event?** |
|--------|
| **Standard:** The agency has taken a comprehensive approach to emergency preparedness and has established mutual aid agreements with all outside entities that the agency may need to coordinate with during an emergency situation. This includes: law enforcement entities, other transit agencies that operate in the same area, and first responders. |

APTA - Mutual Aid (Sign in to APTA’s website or close login screen and document will open)
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Standard</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 4.102   | Does the agency participate in a regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and response? | The agency participates in a regional security and emergency preparedness/management working group or committee. *(This is not the same as participation in drills or exercises)* | FEMA State Offices and Agencies of Emergency Management  
APTA Security & Emergency management Aspects of Special Event Service  
DHS State Homeland Security and Emergency Services |
| 4.103   | Have regional incident management protocols been shared with the agency and incorporated into the agency's ERP/SSP/SEPP? | The agency has received--and is knowledgeable of--regional incident management protocols. These protocols have been completely incorporated into the agency's ERP/SSP/SEPP. | |
| 4.104   | Have agency resources been appropriately identified and provided to the regional EMA? | The agency has provided the regional EMA with a detailed list of resources (vehicles, facilities, etc.) that may be utilized in the event of an emergency. | APTA - First Responder Familiarization of Transit Systems  
DHS State Homeland Security and Emergency Services  
FEMA ICS Resource Center  
APTA - Contagious Virus Response  
ICS Forms  
Surface Transportation and Public Transportation Information Sharing and Analysis Center  
The Role of Transit in Emergency Evacuation - Transportation Research Board Special Report |
<p>| 4.105   | Does the agency have a designated point-of-contact or liaison from the local/regional Emergency Operations Center (EOC)? | Agency has established a point-of-contact at the Emergency Operations Center. | |
| 4.106   | Does the agency send a representative to the local/regional EOC, should it be activated? | Agency has officially designated a representative to be sent to the EOC, upon activation. This is documented in SSP/ERP/SEPP. | |</p>
<table>
<thead>
<tr>
<th><strong>4.107</strong></th>
<th>Does the agency have information sharing capabilities with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has developed a formal method of effectively sharing information with the EOC, information flow is two-way (information can be shared and received), and the method of sharing is known by both entities. Capabilities are documented.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>4.108</strong></th>
<th>Has the agency developed internal incident management protocols that comply with the National Response Plan and the National Incident Management System (NIMS)?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has developed a formal method of effectively sharing with the EOC, information flow is two-way (information can be shared and received), and the method of sharing is known by both entities. Capabilities are documented.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>4.109</strong></th>
<th>Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has shared its internal emergency response protocols with the regional EMA and appropriate first response agencies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>4.110</strong></th>
<th>Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency is very proactive in regards to interoperable communication and ensures that its communication systems can communicate with appropriate external agencies across jurisdictional lines. The agency uses compatible radio systems (800mHz, UHF, VHF, etc.), has developed a plan (either documented or trained personnel) for interoperable communication, and has tested its system for compatibility with appropriate external agencies.</td>
</tr>
<tr>
<td>5.00</td>
<td>Establish and Maintain a Security and Emergency Training Program</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>The purpose of this section is to ensure that ALL agency personnel are trained, tested and monitored in the current security and emergency response protocols appropriate to their position.</td>
<td></td>
</tr>
<tr>
<td>5.101</td>
<td>Is initial training provided to all new agency employees regarding security orientation/awareness?</td>
</tr>
<tr>
<td><strong>Standard:</strong> All new employees, regardless of job function, receive initial training, which is focused on general security awareness and orientation. The agency has a well-developed program with an official curriculum and training is provided in a formal environment (classroom or computer-based).</td>
<td></td>
</tr>
<tr>
<td>5.102</td>
<td>Is annual refresher training regarding security orientation/awareness provided to all employees regardless of position or job function in a formal manner?</td>
</tr>
<tr>
<td><strong>Standard:</strong> Annual refresher training is well-developed with an official curriculum, focused on the appropriate subject, and provided in a formal manner (classroom or computer-based).</td>
<td></td>
</tr>
<tr>
<td>5.105</td>
<td>Is ongoing advanced security training focused on job function provided at least annually?</td>
</tr>
<tr>
<td><strong>Standard:</strong> Advanced security training is provided in an ongoing manner, with classes/courses being provided at least once per year. Agency has established an official training curriculum, training is specifically designed based on job function, and training is provided in a formal environment (classroom or computer-based).</td>
<td></td>
</tr>
<tr>
<td>5.106</td>
<td>Is initial training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function, in a formal manner?</td>
</tr>
<tr>
<td><strong>Standard:</strong> All employees, regardless of job function, receive initial training, which is focused on Active Shooter. The agency has a well-developed program with an</td>
<td></td>
</tr>
<tr>
<td>5.107</td>
<td><strong>Is annual refresher training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function?</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Standard:</strong> <em>All</em> employees, regardless of job function, receive annual Active Shooter training. The agency has a well-developed program with an official curriculum and training is provided in a formal environment (classroom or computer-based).</td>
<td></td>
</tr>
</tbody>
</table>

5.108 **Is initial training provided to all new transit employees regarding emergency response?**

**Standard:** All new employees, regardless of job function, receive initial training, which is focused on emergency response. The agency has a well-developed program with an official curriculum and training is provided in a formal environment (classroom or computer-based).

5.109 **Is annual refresher training regarding emergency response provided to all employees regardless of position or job function in a formal manner?**

**Standard:** Annual refresher training is well-developed with an official curriculum, focused on the appropriate subject, and provided in a formal manner (classroom or computer-based).

5.112 **Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System (NIMS)?**

**Standard:** All employees who may have a role in emergency response--frontline personnel and leadership--have received ICS training in accordance with the NIMS. The agency has a well-developed program with an official curriculum and training is provided in a formal environment (classroom or computer-based).
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.113</td>
<td>Has ICS and NIMS training appropriate to the position been provided to Senior Management staff and supervisors? (Describe the frequency of training)</td>
</tr>
</tbody>
</table>

**Standard:** Annual ICS and NIMS training based on job function is provided by the agency to all senior leadership.

FTA Transit Security Training Tools
DHS State Homeland Security and Emergency Services

| 5.114  | Has ICS and NIMS training appropriate to the position been provided to frontline employees? |

**Standard:** Annual ICS and NIMS training based on job function is provided by the agency to all supervisors and managers.

FTA/NTI Sponsored Course Catalog
APTA - Security Awareness Training for Transit Employees (Sign in to APTA’s website or close login screen and document will open)

FEMA Emergency Management Institute

| 5.116  | Has the agency developed a program and provided initial training on its own incident response protocols? |

**Standard:** The agency has developed internal procedures for incident response and a comprehensive training program to support these procedures. Training has an established curriculum, official training materials, and is provided in a formal environment (classroom or computer-based).

<p>| 5.117  | Is annual refresher training on the agency's incident response protocols appropriate to the position been provided to all employees regardless of position or job function? |</p>
<table>
<thead>
<tr>
<th>Standard:</th>
<th>Annual training is provided to all employees regardless of position or job function.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.120</td>
<td>Has the transit system implemented an annual training program for personnel regarding response to terrorism, including (i) Improvised Explosive Devices and ii) Weapons of Mass Destruction (chemical, biological, radiological, nuclear)? If so, summarize the relevant programs in the justification?</td>
</tr>
<tr>
<td>Standard:</td>
<td>Annual training provided regarding response to IEDs and WMD. This is part of an official curriculum, uses effective training materials, and is provided in a formal environment (classroom or computer-based).</td>
</tr>
<tr>
<td>5.121</td>
<td>Has training focused on IEDs and WMDs appropriate to the position been provided to all employees regardless of position or job function at least annually?</td>
</tr>
<tr>
<td>Standard:</td>
<td>Annual training based on job function is provided by the agency to all senior leadership.</td>
</tr>
<tr>
<td>5.124</td>
<td>Do law enforcement/security department personnel, security managers at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.</td>
</tr>
<tr>
<td>Standard:</td>
<td>All personnel in security-related positions receive annual specialized training focused on counter-terrorism. Training is in addition to general training, with materials developed by or instruction led by subject matter experts. Training is part of an established curriculum and</td>
</tr>
</tbody>
</table>

---

**Introduction to Incident Command System - ICS-100**

**FTA Transit Security Training Tools**

**DHS State Homeland Security and Emergency Services**

**FTA/NTI Sponsored Course Catalog**

**APTA Security Awareness Training for Transit Employees (Sign in to APTA’s website or close login screen and document will open)**

**FEMA Emergency Management Institute**

**National Transit Institute**
<table>
<thead>
<tr>
<th>5.125</th>
<th>Do law enforcement/security department personnel at the agency receive specialized training supporting their incident management and emergency response roles at least annually? Summarize program in the justification.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> All personnel in security-related positions receive annual specialized training supporting incident response. This training is in addition to general training, with materials developed by or instruction led by subject matter experts. Training is part of an established curriculum and provided in a formal environment (classroom or computer-based).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.126</th>
<th>Does the agency have an established program to monitor and schedule employee training?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency has developed a formal system of monitoring employee training and scheduling employee training as needed. This includes retaining training records, having the ability of easily determining employee-training status, and having the ability to effectively schedule employee training in an effective manner.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5.127</th>
<th>Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?</th>
</tr>
</thead>
</table>
| **Standard:** The agency has a formal system to **record and track** personnel training for all security-related training, including initial, annual, and periodic. Records for **all** employees contain the following: employee information.
<table>
<thead>
<tr>
<th>Section</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.128</td>
<td>Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has a formal system to <strong>record and track</strong> personnel training for <strong>all emergency response-related training</strong>, including initial, annual, and periodic. Records for <strong>all</strong> employees contain the following: employee name/identifier, training/course identifier, and date of course completion.</td>
</tr>
<tr>
<td>5.129</td>
<td>Does the agency have a program to regularly review and update security awareness and emergency response training materials?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has developed a formal program of reviewing and updating security and emergency response training materials to ensure they are up-to-date, this program is documented (generally or as a &quot;role/responsibility&quot;), and the program ensures materials are reviewed at least annually.</td>
</tr>
<tr>
<td>5.130</td>
<td>Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Appropriate personnel are notified of operational changes--including those related to threat levels and protective measures. Individuals with a &quot;need to know&quot; have been formally identified, and measures are in place to effectively reach <strong>all</strong> appropriate employees.</td>
</tr>
<tr>
<td>Section</td>
<td>Question</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>5.131</td>
<td>Do the agency's security awareness and emergency response training programs cover response and recovery operations in critical facilities and infrastructure? If so, summarize relevant provisions of program in the justification.</td>
</tr>
<tr>
<td>5.132</td>
<td>Has the agency provided training to regional first responders to enable them to operate in critical facilities and infrastructure?</td>
</tr>
<tr>
<td>5.133</td>
<td>Has the agency provided local law enforcement/first responders opportunities to familiarize themselves with agency’s system for response to Active Shooter events?</td>
</tr>
<tr>
<td>5.134</td>
<td>Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?</td>
</tr>
</tbody>
</table>
### 5.135 Has the agency implemented a program to train or orient first responders and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?

**Standard:** The agency has developed and implemented a program to *annually* train or orient first responders and other supporting agencies (TSA VIPR teams) on their system vehicle familiarization. Training is well-developed, and the agency has actively offered it to outside entities.

### 6.000 Establish plans and protocols to respond to the DHS National Terrorism Advisory System (NTAS).

The purpose of establishing plans and protocols to respond to information received about imminent or elevated security threats is to ensure a pre-determined, organized response by the Agency, employees and individuals to prevent, mitigate or respond to the threat.

#### 6.101 Does the SSP contain or reference other documents identifying incremental actions (imminent or elevated) to be implemented for a NTAS threat?

**DHS NTAS**

**Standard:** The agency has identified incremental actions that correlate with NTAS threat level increases. Incremental actions are identified for all threat conditions, well-developed, effective, and documented.

#### 6.102 Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?

**Standard:** The agency has identified possible NTAS alert scenarios and established detailed procedures and protocols to respond to these scenarios. These procedures are well-developed and documented.
### 6.103 Has the agency provided annual training and/or instruction focused on job function regarding the incremental activities to be performed by employees?

**Standard:** Job-specific NTAS training that focuses on incremental activities to be performed by employees has been provided annually by the agency. Training is well-developed, part of an official curriculum, focuses on appropriate individual roles in response to NTAS threats, and is provided in a formal environment (classroom or computer-based).

### 7.000 Implement and reinforce a Public Security and Emergency Awareness program.

The purpose of this section is to ensure that the agency develops and implements programs to engage all passengers, contractors and others who come into contact with the system in a program of security awareness activities so that they serve as “eyes and ears” for the system.

### 7.101 Has the transit agency developed and implemented a public security and emergency awareness program?

**Standard:** Agency has implemented a well-developed public awareness program that addresses specific issues of both security and emergency response.

**FTA Transit Watch Program**

**DHS If-You-See-Something-Say-Something-Campaign**

**FTA Transit Watch Program Toolkit**

### 7.102 Does the agency provide active public outreach for security awareness and emergency preparedness (e.g., Transit Watch, “If You See Something, Say Something”, message boards, brochures, channel cards, posters, fliers)?

**Standard:** The agency's public awareness program covers security and emergency response and is communicated effectively. Program materials—brochures, posters, fliers—are widely distributed and highly visible.

**NTAS Print Materials**

### 7.103 Is the above consistent with agency's overall announcement program?
<table>
<thead>
<tr>
<th>Standard: Public awareness material is consistent with the agency's overall announcement program. All information/instruction/guidance is the same.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.104</strong> Are general security awareness and emergency preparedness messages included in public announcement messages at stations and on board vehicles?</td>
</tr>
<tr>
<td>Standard: The agency includes frequent mentions of general security and emergency preparedness items in its pre-recorded announcement messages at all appropriate areas, including at stations and onboard vehicles.</td>
</tr>
<tr>
<td><strong>7.105</strong> Are passengers urged to report unattended property, suspicious behavior, and security concerns to uniformed crew members, law enforcement or security personnel, and/or a contact telephone number? If so, summarize the type of materials used and content in the justification.</td>
</tr>
<tr>
<td>Standard: Passengers are urged to report unattended property, suspicious behavior, and other security concerns to an identified agency representative (uniformed crew member, law enforcement, etc.) or identified contact number. This is documented in awareness material and readily observable.</td>
</tr>
<tr>
<td><strong>7.106</strong> Does the agency have an appropriate mechanism in place for passengers to communicate a security concern? (e.g., 1-800 number, smart phone applications, social media, etc.)</td>
</tr>
<tr>
<td>Standard: The agency utilizes an effective mechanism in place that can be used by passengers to report security concerns (phone number, smart phone application, social media, etc.). This mechanism is actively monitored by the agency and widely distributed to passengers as part of the awareness program's materials.</td>
</tr>
</tbody>
</table>

FTA Transit Watch Program
APTA - Suspicious Behavior (Sign in to APTA’s website or close login screen and document will open)
<table>
<thead>
<tr>
<th>7.107</th>
<th>Does the agency issue public service announcements or press releases to social media regarding security and emergency protocols? (e.g. Twitter/ Facebook/etc., QRC codes, and/or apps for smart phones)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency utilizes social media to issue public service announcements related to security or emergency response. This method is documented or readily observable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.108</th>
<th>Does the agency issue public service announcements or press releases to local media regarding security or emergency protocols? (e.g. newspaper, radio and/or television)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency issues security- and emergency response-related PSAs or press releases to local media. This method is documented or readily observable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.109</th>
<th>Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response? If so, describe training program and activities.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency conducts training of non-employee volunteers to aid with system evacuations an emergency response. This training program has an official curriculum and provided on a semi-frequent basis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7.110</th>
<th>Does the transit agency conduct an outreach program to enlist members of the public as security awareness volunteers, similar to Neighborhood Watch programs?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has established a volunteer program to enlist an active security awareness volunteer</td>
</tr>
</tbody>
</table>

**Community Emergency Response Team (CERT) Program**
| 7.111 | Do public awareness materials and/or messages inform passengers on the means to evacuate safely from transit vehicles and facilities? |
|-------|---------------------------------------------------------------------------------------------------------------------------------
| **Standard:** The agency has developed awareness material to assist passengers on the means to evacuate safely from transit vehicles and underwater/underground facilities. These materials are readily available or readily visible to passengers. |

<table>
<thead>
<tr>
<th>7.112</th>
<th>Does the agency track and monitor customer complaints reported by passengers?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency has a system in place to actively and effectively monitor and follow up on customer reports.</td>
<td></td>
</tr>
</tbody>
</table>

| 8.000 | Establish and use a Risk Management Process to assess and manage threats, vulnerabilities and consequences. |
|-------|---------------------------------------------------------------------------------------------------------------------------------
| **The purpose of an Agency risk management process is to improve security through a structured, proactive program developed to identify, assess, manage, and mitigate the security risks inherent to the system.** |

| 8.101 | Does the agency have its own risk assessment process, approved by its management, for managing threats and vulnerabilities? If so, summarize the process in the justification. |
|-------|---------------------------------------------------------------------------------------------------------------------------------
| **Standard:** Risk assessment process is developed, documented, specifically addresses threats and vulnerabilities, and is approved by management. |

| 8.102 | Has the agency identified facilities and systems it considers to be its critical assets? |
|-------|---------------------------------------------------------------------------------------------------------------------------------
| **Standard:** The agency has identified facilities and systems it considers critical assets. This is documented (or clearly implied in documentation/procedures). |

| 8.103 | Has the agency had an internal or external vulnerability assessment on its critical assets within the past 3 years? Specify the dates of the |
|-------|---------------------------------------------------------------------------------------------------------------------------------

**DHS - Risk Management Fundamentals**

**FTA - An Introduction to All-Hazards Preparedness for Transit Agencies**

**FEMA – Threat and Hazard Identification and Risk Assessment Guide**
<table>
<thead>
<tr>
<th>Most Recent Assessments and the Entity(ies) that Conducted the Assessment(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> A vulnerability assessment focused on the agency's <em>critical assets</em> has been conducted within the last 3 years.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.104</th>
<th>Has the agency had an internal or external Risk Assessment, analyzing threat, vulnerability, &amp; consequence, for critical assets and infrastructure, and systems within the past 3 years? Have management and staff responsible for the risk assessment process been properly trained to manage the process?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> A risk assessment focused on the agency's critical assets has been conducted within the last 3 years; focuses specifically on threats, vulnerabilities, and consequences; and is documented. The personnel tasked with conducting the assessment have been provided adequate training to effectively conduct such an assessment.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.105</th>
<th>Has the system implemented procedures to limit and monitor access to underground and underwater tunnels? If so, summarize procedures in the justification.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The system has well-developed, well-documented policies and procedures in place to limit and monitor access to underground and underwater tunnels.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.106</th>
<th>Are security investments prioritized using information developed in the risk assessment process?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> Risk assessments play a large role in agency policy and procurement. Security investments are prioritized based on information obtained during risk assessments. This is evident based on the agency's recent security investments that corrected items identified in past risk assessments, or is part of a documented policy.</td>
<td></td>
</tr>
</tbody>
</table>
### 8.107

<table>
<thead>
<tr>
<th>8.107</th>
<th>Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and related documents?</th>
</tr>
</thead>
</table>

**Standard:** The agency has provided TSA with *all* requested documents.

### 9.000

**Establish and use an information sharing process for threat and intelligence information**

The purpose of this section is to ensure enhanced agency security awareness through formalized information receipt processes and incident/information reporting exchanges to ensure that the agency has timely, controlled and predictable responses to various types of emergencies that may occur within the system or nearby locations that may impact the system.

### 9.101

<table>
<thead>
<tr>
<th>9.101</th>
<th>Does the agency have a formalized process and procedures for reporting and exchange of threat and intelligence information with Federal, State, and/or local law enforcement agencies?</th>
</tr>
</thead>
</table>

**Standard:** The entity is actively involved with intelligence sharing and has developed a formalized (documented) method of sharing threat/intel information with multiple entities representing local, State *and* Federal law enforcement.

### 9.102

<table>
<thead>
<tr>
<th>9.102</th>
<th>Does the agency report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?</th>
</tr>
</thead>
</table>

**Standard:** The agency reports threat/intel information *directly* to the JTTF or regional anti-terrorism task force.

### 9.103

<table>
<thead>
<tr>
<th>9.103</th>
<th>Does the agency have policies requiring employees to report (internal or external) suspicious activity to their supervisor or management?</th>
</tr>
</thead>
</table>

**Standard:** The agency has detailed policies and protocols in place to report suspicious activity Internally and externally.
<table>
<thead>
<tr>
<th>9.104</th>
<th>Does the system have a protocol to report threats or significant security concerns to appropriate law enforcement authorities, and TSA's Transportation Security Operations Center (TSOC)?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Standard:</strong> The agency has detailed policies and protocols in place to report real-time threats/significant security concerns to appropriate law enforcement and TSOC. These protocols are documented and include a &quot;time&quot; element (immediately, within &quot;X&quot; hours, etc.).</td>
</tr>
</tbody>
</table>
|        | **TSOC – Freedom Center**  
|        | POC: TSOC Surface Watch Officer  
|        | Telephone: 1-866-615-5150  
|        | E-Mail: TSOC.St@dhs.gov  |

<table>
<thead>
<tr>
<th>9.105</th>
<th>Does the agency routinely receive threat and intelligence information directly from any Federal government agency, State Homeland Security Office, Regional or State Intelligence Fusion Center, PT-ISAC, or other transit agencies? If so, describe frequency.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Standard:</strong> The agency receives threat/intel information at least once per week.</td>
</tr>
</tbody>
</table>
|        | **Homeland Security Information Network**  
|        | **Surface Transportation and Public Transportation Information Sharing and Analysis Center** |

<table>
<thead>
<tr>
<th>9.106</th>
<th>Does the agency report their NTD security data to FTA as required by 49 CFR 659?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Standard:</strong> The agency reports NTD security data to FTA.</td>
</tr>
</tbody>
</table>

| 10.000 | **Conduct Tabletop and Functional Drills**  

The purpose of this section is to develop and prepare a coordinated agency emergency response through the conduct of planning, training, exercising and evaluating of response protocols with local and regional first responders.  

<table>
<thead>
<tr>
<th>10.101</th>
<th>Does the agency have a documented process to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>FTA System Security and Emergency Preparedness Program Plan Template</strong></td>
</tr>
<tr>
<td>Standard</td>
<td>Does the agency’s SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>10.102</strong></td>
<td><strong>APTA – Transit Incident Drills and Exercises</strong></td>
</tr>
<tr>
<td>Standard</td>
<td>The agency has documented roles and responsibilities that detail how it performs its emergency planning activities, including those related to drills and exercises. Furthermore, the agency has established written requirements for emergency drills and exercises (timelines, method of evaluation, personnel required to participate, etc.). All roles, responsibilities, and requirements are documented in the agency's SSPP or SSP--or another documented that is referenced in the SSPP.</td>
</tr>
<tr>
<td><strong>10.103</strong></td>
<td><strong>FTA Emergency Preparedness/ Emergency Management</strong></td>
</tr>
<tr>
<td>Standard</td>
<td>The agency conducts drills and exercises annually with the purpose of evaluating its emergency preparedness procedures.</td>
</tr>
<tr>
<td><strong>10.104</strong></td>
<td><strong>DHS FEMA IS-130 Exercise Evaluation training course</strong></td>
</tr>
<tr>
<td>Standard</td>
<td>The agency has a documented requirement for drills/exercises to be conducted once per year at a minimum.</td>
</tr>
<tr>
<td><strong>10.104</strong></td>
<td><strong>FEMA Emergency Planning Exercises</strong></td>
</tr>
</tbody>
</table>
| 10.105 | Does the agency’s SPP or SSP describe or reference how the agency documents the results of its emergency preparedness evaluations? (i.e., briefings, after action reports and implementation of findings) | FTA Emergency Preparedness/ Emergency Management  
Homeland Security Exercise and Evaluation Program (HSEEP)  
Safety and Security Oversight Program |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The process of drill/exercise evaluation is described and documented in the SSPP, SSP, or another document that is referenced by the SSPP/SSP.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10.106</th>
<th>Does the agency’s SPP or a related document describe or reference its program for providing employee training on emergency response protocols and procedures?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The program for providing employee training on emergency response protocols and procedures is documented.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10.107</th>
<th>Does the agency participate as an active player in full-scale, regional exercises, held at least annually?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency participates as an active player in full-scale, regional exercises held at least annually.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10.108</th>
<th>In the last year, has the agency conducted drills or exercises specifically focus on Active Shooter scenarios with its employees?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> In the last year, the agency has conducted its own drills and/or exercises specific to Active Shooter with all their employees.</td>
<td></td>
</tr>
</tbody>
</table>

**DRILLS AND EXERCISES**
| 10.109 | In the last year, has the agency conducted and/or participated in a drill, tabletop exercise, and/or field exercise including scenarios involving (i) IED's and (ii) WMD (chemical, biological, radiological, nuclear) with other transit agencies and first responders (e.g., NTAS scenarios)?  

**Standard:** In the last year, the agency has been involved in drills/exercises that specifically focus on IEDs **and** WMD with appropriate external entities, to include first responders **and** other transit agencies that operate in the same environment. |
| 10.110 | In the last year, has the agency reviewed results and prepared after-action reports to assess performance and develop lessons learned for all drills, tabletop, and/or field exercises?  

**Standard:** *In the last year*, the agency has reviewed and prepared after-action reports (or other evaluating report) for all drills and exercises. All evaluations are documented. |
| 10.111 | In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings or corrective actions? If so, summarize the actions taken in the justification.  

**Standard:** *In the last year*, the agency has updated plans, protocols, or processes to incorporate after-action report recommendations/findings. |
<p>| 10.112 | Has the agency established a system for objectively measure and assess its performance during emergency exercises and to measure improvements? |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Standard</th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.113</td>
<td><strong>Standard:</strong> The agency has developed a formal, objective system of evaluating drill performance. The agency has identified evaluation <em>criteria</em>, establishes drill/exercise <em>goals</em>, and analyzes the results appropriately. This system is documented.</td>
<td>Does the system conduct drills and exercises of its security and emergency response plans to test capabilities of (i.) employees and (ii.) first responders to operate effectively throughout the agencies system? (i.e., facilities, stations, office buildings, terminals, underwater/underground infrastructure and other critical systems)</td>
<td><strong>APTA – Transit Incident Drills and Exercises</strong></td>
</tr>
<tr>
<td>10.114</td>
<td><strong>Standard:</strong> The agency conducts exercises of its security and emergency response plans to test operational capabilities of employees and first responders in underwater/underground infrastructure and other critical systems.</td>
<td>Does the transit system integrate local and regional first responders in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place?</td>
<td></td>
</tr>
<tr>
<td>11.101</td>
<td><strong>Standard:</strong> The agency actively reaches out to external emergency agencies (local and regional) when planning and conducting exercises. The agency integrates all appropriate entities: fire, medical, and law enforcement.</td>
<td>Has the agency conducted a risk assessment to identify operational control and</td>
<td></td>
</tr>
<tr>
<td>11.000</td>
<td><strong>Developing a Comprehensive Cyber Security Strategy</strong></td>
<td>The purpose of this section is to enhance agency security awareness and preparedness to identify and protect against cyber security threats to the system.</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>11.102 Has the agency implemented protocols to ensure that all IT facilities (e.g., data centers, server rooms, etc.) and equipment are properly secured to guard against internal or external threats or attacks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard:</td>
<td>The agency has identified all critical IT facilities/infrastructure and established procedures and protocols that ensure the security (physical and cyber) of these assets. Procedures are well-developed--specifically referencing IT-facilities/equipment and IT-security--and documented.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>11.103 Has a written strategy been developed and integrated into the overall security program to mitigate the cyber risk identified?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard:</td>
<td>A written IT-security strategy--which includes countermeasures and personnel responsibilities--has been developed to mitigate cyber risk and is part of the overall security program (included as part of the SSP or other appropriate document).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>11.104 Does the agency have a designated representative to secure the internal network through appropriate access controls for employees, a strong authentication (i.e., password) policy, encrypting sensitive data, and employing network security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard:</td>
<td></td>
</tr>
<tr>
<td><strong>infrastructure (example: firewalls, intrusion detection systems, IT security audits, antivirus, etc.)?</strong></td>
<td><strong>Standard:</strong> The agency has formally designated an individual responsible for securing the internal network through appropriate measures. This individual is knowledgeable of the agency's cybersecurity measures, and his/her responsibilities are documented.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>11.105</strong> Does the agency ensure that recurring cyber security training reinforces security roles, responsibilities, and duties of employees at all levels to protect against and recognize cyber threats?</td>
<td><strong>Cyber Security Training &amp; Exercises</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong> The agency provides ongoing, recurrent cyber training that identifies cyber threats and addresses roles, responsibilities, and duties at all levels to mitigate these threats. Training is part of an official curriculum, utilizes well-developed materials, and is provided in a formal environment (classroom or computer-based).</td>
<td></td>
</tr>
<tr>
<td><strong>11.106</strong> Has the agency established a cyber-incident response and reporting protocol?</td>
<td><strong>Standard:</strong> The agency has established cyber-incident response and reporting protocols. These procedures are detailed, documented, and address (a) employee actions to be taken in the event of a cyber-incident and (b) to whom cyber-incidents shall be reported.</td>
</tr>
<tr>
<td><strong>11.107</strong> Is the agency aware of and using available resources (e.g., standards, PT-ISAC, US CERT, National Cyber Security Communication and Integration Center, etc.)?</td>
<td><strong>APTA PT- ISAC (Sign in to APTA’s website or close login screen and document will open)</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong> The agency is aware of and makes use of available resources.</td>
<td><strong><a href="http://transitwireless.org/">http://transitwireless.org/</a></strong></td>
</tr>
<tr>
<td><strong>National Cyber Security Communication and Integration Center</strong></td>
<td></td>
</tr>
</tbody>
</table>
Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors.

The purpose of establishing controlled access to identified security critical facilities is to promote protective measures for critical infrastructure essential to uninterrupted / uncompromised system operation.

<table>
<thead>
<tr>
<th>12.101</th>
<th>Have assets and facilities requiring restricted access been identified?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Restricted areas are identified and documented. Agency personnel are familiar with their location and restricted status.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.102</th>
<th>Are ID badges or other measures employed to restrict access to facilities not open to the public?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>ID badges (or other effective measure) are issued to all employees with access to restricted areas, and the agency has policies in place requiring their use and/or display.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.103</th>
<th>Has the transit agency developed and implemented procedures to monitor, update and document access control (e.g. card key, ID badges, keys, safe combinations, etc.)?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has implemented an access control system that is capable of all of the following: (1) monitoring access; (2) documenting access; and (3) updating access.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.104</th>
<th>Does the agency have documented procedures for issuing ID badges to visitors and contractors?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has documented procedures in place to issue ID badges for visitors and contractors. These procedures are implemented perfectly.</td>
</tr>
</tbody>
</table>

FTA Transit Security Design Considerations - 5.0 Access Management
<table>
<thead>
<tr>
<th>12.105</th>
<th>Does the agency have a documented policy that requires visitors to be escorted when accessing non-public areas.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has a documented policy that requires visitors to be escorted when accessing non-public areas. This policy is implemented <em>perfectly</em>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.106</th>
<th>Is CCTV equipment installed in transit agency facilities?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Effective and capable CCTV systems are installed at all facilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.107</th>
<th>Is CCTV equipment protecting critical assets interfaced with an access control system?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>CCTV equipment protecting critical assets are completely integrated with other access control measures (door breach triggers automated CCTV functions, etc.).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.108</th>
<th>Is CCTV equipment installed on transit vehicles?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>Effective and capable CCTV systems are installed on a vast majority of vehicle fleet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.209</th>
<th>Are Crime Prevention through Environmental Design (CPTED) and technology (e.g., CCTV, access control, intrusion detection, bollards, etc.) incorporated into design criteria for all new and/or existing capital projects?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>CPTED is incorporated in the design of all projects. CPTED-related vulnerabilities are identified and corrected promptly using technological solutions or other solutions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.110</th>
<th>Does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has installed physical barriers or intrusion detection systems to prevent unauthorized access</td>
</tr>
<tr>
<td>FACILITY SECURITY AND ACCESS CONTROLS</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--</td>
</tr>
<tr>
<td>12.111</td>
<td><strong>Has the system implemented protective measures to secure high risk/high consequence assets and critical systems?</strong> (i.e., CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems)</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has identified high risk/high consequence assets and has implemented additional security measures for <em>all</em> such assets. Additional measures are documented.</td>
</tr>
<tr>
<td>12.112</td>
<td><strong>Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has a means of effectively monitoring a network of alarms, including intrusion, life-safety, and other security-related alarms. The agency has plans and procedures in place for responding to such alarms.</td>
</tr>
<tr>
<td>12.113</td>
<td><strong>Does the agency provide a method for passengers and visitors to report security and safety concerns from within the agency's system?</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Call boxes are <em>consistently</em> installed throughout the agency’s system; specifically in stations, terminals,</td>
</tr>
</tbody>
</table>

APTA - Chain Link, Mesh, or Woven Metal Fencing (Sign in to APTA’s website or close login screen and document will open)

APTA - Gates to Control Access (Sign in to APTA’s website or close login screen and document will open)

APTA - Ornamental Fencing (Sign in to APTA’s website or close login screen and document will open)

FTA - Transit Security Design Considerations - 6.3 Security Approaches for Types of Transit Infrastructure

DHS If-You-See-Something-Say-Something-Campaign
<table>
<thead>
<tr>
<th>12.114</th>
<th><strong>Does the transit agency administer an automated employee access control system and perform corrective analysis of security breaches?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency uses an automated access control system and performs a corrective analysis of all security breaches to prevent future occurrences of a similar nature. This corrective analysis is documented as part of an overarching policy or as part of an identified employee's responsibilities.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.115</th>
<th><strong>Does the agency have policies and procedures for screening of mail and/or outside deliveries?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency has documented policies and specific, well-developed procedures that address the screening of mail or outside deliveries. Procedures are completely implemented.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.116</th>
<th><strong>Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency uses multiple methods of breach prevention (locks, anti-frag materials, bullet resistant materials, etc.) at all critical locations.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12.117</th>
<th><strong>Does the agency use National Fire Protection Association (NFPA) Standard 130 or equivalent to evaluate fire/life safety in station design or modifications? (including fire detection systems, firewalls and flame-resistant materials, back-up powered emergency lighting, defaults in turnstile and other systems supporting emergency exists, and pre-recorded public announcements)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>National Fire Protection Association (NFPA) Standard List of Codes and Standards</strong></td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>12.118 Is directional signage with adequate lighting provided in a consistent manner throughout their system, both to provide orientation and to support emergency evacuation?</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard:</td>
<td>Directional signage and lighting is consistent throughout the system and is installed in a manner that supports security, safety, and emergency operations.</td>
</tr>
<tr>
<td>12.119</td>
<td>Are gates and locks used on all facility doors to prevent unauthorized access during operating hours?</td>
</tr>
<tr>
<td>Standard:</td>
<td>The agency uses gates and locks to prevent unauthorized access at all facilities. Policies and procedures are in place to effectively utilize locks and gates.</td>
</tr>
<tr>
<td>12.120</td>
<td>Are keys controlled through an established program that is documented?</td>
</tr>
<tr>
<td>Standard:</td>
<td>The agency has a documented key control program that specifically assigns management responsibility to a specific individual or department.</td>
</tr>
<tr>
<td>12.121</td>
<td>Are gates and locks used to close down system facilities after operating hours?</td>
</tr>
<tr>
<td>Standard:</td>
<td>Gates and locks are used at all facilities that are closed down. Policies and procedures are in place to effectively utilize locks and gates.</td>
</tr>
<tr>
<td>12.122</td>
<td>Do transit vehicles have radios, silent alarms, and/or passenger communication systems?</td>
</tr>
</tbody>
</table>

**Standard:** NFPA 130 or equivalent is used in station design or modification criteria. Access Control systems do not interfere with safety or emergency operations.

**Standard:** The agency uses gates and locks to prevent unauthorized access at all facilities. Policies and procedures are in place to effectively utilize locks and gates.

**Standard:** The agency has a documented key control program that specifically assigns management responsibility to a specific individual or department.

**Standard:** Gates and locks are used at all facilities that are closed down. Policies and procedures are in place to effectively utilize locks and gates.

**APTA - Security Lighting for Transit Passenger Facilities**
(Sign in to APTA’s website or close login screen and document will open)

**APTA - Fencing Systems to Control Access to Transit Facilities**
(Sign in to APTA’s website or close login screen and document will open)

**APTA - Chain Link, Mesh, or Woven Metal Fencing**
(Sign in to APTA’s website or close login screen and document will open)

**APTA - Gates to Control Access**
(Sign in to APTA’s website or close login screen and document will open)

**APTA - Ornamental Fencing**
(Sign in to APTA’s website or close login screen and document will open)
<table>
<thead>
<tr>
<th>Standard: All transit vehicles are equipped with radios, silent alarms, and/or passenger communication systems. Policies and procedures are in place to effectively utilize these measures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.123 Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?</td>
</tr>
<tr>
<td>Standard: Graffiti-resistant/etch-resistant materials are used at all (or a vast majority of) facilities.</td>
</tr>
<tr>
<td>12.124 Are Uninterruptible Power Supply (UPS) or redundant power sources provided for safety and security of critical equipment, fire detection, alarm and suppression systems; public address; call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?</td>
</tr>
<tr>
<td>Standard: Uninterruptible Power Supplies are provided for all safety- and security-critical equipment.</td>
</tr>
<tr>
<td>12.125 Has the agency removed non-explosive resistant trash receptacles from platform areas of terminals and stations?</td>
</tr>
<tr>
<td>Standard: The agency has removed non-explosive resistant trash receptacles from platform areas of terminals and stations.</td>
</tr>
<tr>
<td>12.126 Does the agency employ specific protective measures for all critical infrastructure (e.g., tunnels, bridges, stations, control centers, etc.) identified through the risk assessment particularly at access points and ventilation infrastructure?</td>
</tr>
</tbody>
</table>

*National Infrastructure Protection Plan (NIPP), DHS, 2013*

*APTA - Operational Strategies for Emergency Smoke Ventilation in Tunnels*
| Standard: | The agency has formally identified critical infrastructure and deployed specific, effective protective measures, which are maintained and implemented appropriately, at all identified areas. |
| 12.127 | Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available through mutual aid agreements with other law enforcement agencies? |
| Standard: | The agency utilizes explosive detection canine teams (with appropriate mutual aid agreements established, if necessary) and has established documented policies and procedures regarding their use. |

| 13.000 | Conduct Physical Security Inspections |
| The purpose of conducting frequent and consistent inspections of security critical facilities, equipment and other critical assets is to ensure prompt identification and resolution of security issues, gaps or conditions. |
| 13.101 | Does the agency conduct frequent inspections of key facilities, stations, terminals, trains and vehicles, or other critical assets for persons, materials, and items that do not belong? Describe frequency of inspection. |
| Standard: | The agency has procedures in place to conduct security inspections of facilities and vehicles for suspicious items and persons at multiple times per day. These procedures are appropriately documented and implemented perfectly. |

| 13.102 | Has the transit agency established procedures for inspecting/sweeping vehicles and stations to identify and manage suspicious items, based on HOT characteristics (hidden, obviously suspicious, not typical) or equivalent system? |
| Standard: | TSA/FTA – Conduct Physical Security Inspections |
| APTA - Identifying Suspicious Behavior in Mass Transit (Sign in to APTA’s website or close login screen and document will open) |

<p>| Standard: | APTA - Recognizing and Responding to Unattended Packages, Objects and Baggage (Sign in to APTA’s website or close login screen and document will open) |</p>
<table>
<thead>
<tr>
<th>Standard: Documented security procedures reflect HOT characteristics.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>13.103</strong> Has the transit agency developed a form or quick reference guide for operations and personnel to conduct pre-trip, post-trip, and within-trip inspections?</td>
<td>APTA - Conducting Revenue Vehicle Security Inspections (Sign in to APTA’s website or close login screen and document will open)</td>
</tr>
<tr>
<td>Standard: The agency utilizes a checklist or other widely distributed document that specifically addresses security to assist personnel conducting pre-, post-, and within-trip security inspections.</td>
<td></td>
</tr>
<tr>
<td><strong>13.104</strong> Has the transit agency developed a form or quick reference guide for station attendants and others regarding station and facility inspections?</td>
<td>APTA - Conducting Nonrevenue Vehicle Security Inspections (Sign in to APTA’s website or close login screen and document will open)</td>
</tr>
<tr>
<td>Standard: The agency utilizes a checklist or other widely distributed document that specifically addresses security to assist personnel conducting station/facility inspections.</td>
<td></td>
</tr>
<tr>
<td><strong>13.105</strong> Does the system document the results of inspections and implement any changes to policies and procedures or implement corrective actions, based on the findings? Describe specific examples where improvements to policy or procedures have occurred.</td>
<td></td>
</tr>
<tr>
<td>Standard: Inspection results are documented and the agency implements corrective actions or other modifications based on these results. This is readily observable in changes made by the agency or is a documented policy.</td>
<td></td>
</tr>
<tr>
<td><strong>13.106</strong> Does the agency conduct frequent inspections of its critical systems access points, ventilation systems, and the interior of underground/underwater assets for indications of suspicious activity?</td>
<td></td>
</tr>
<tr>
<td><strong>Standard:</strong> The agency conducts security inspections of non-normal areas (access points, ventilation systems, interior of underground/underwater assets) for indications of suspicious activity multiple times per week. These procedures are documented appropriately and implemented to perfection.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>13.107</strong></th>
<th>Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect?</th>
<th><a href="https://www.apta.org/programs/counterterrorism/counterterrorism-measures-on-transit-systems">APTA - Random Counterterrorism Measures on Transit Systems</a> (Sign in to APTA’s website or close login screen and document will open)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Standard:</strong> Security activities are conducted at random times and at random intervals and these procedures are documented.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>13.108</strong></th>
<th>Is there a process in place to ensure that in-service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Standard:</strong> The agency has documented policies and procedures in place to ensure that all in-service vehicles are inspected at multiple times per day for suspicious or unattended items. Personnel receive training to properly conduct these inspections.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>13.109</strong></th>
<th>Is there a process in place, with necessary training provided to personnel, to ensure that all critical infrastructures are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.</th>
<th></th>
</tr>
</thead>
</table>

<p>| <strong>Standard:</strong> The agency has documented policies and procedures in place to ensure that all critical infrastructure areas are inspected at multiple times per day for suspicious or unattended items. Personnel receive training to properly conduct these inspections. |</p>
<table>
<thead>
<tr>
<th>14.000</th>
<th>Conduct Background Investigations of Employees and Contractors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The purpose of this element is to enhance system security through the conduct and documentation of employee and contractor background investigations based upon identified and verified critical system access requirement levels.</td>
</tr>
</tbody>
</table>

14.101 | Does the agency conduct background investigations on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities, and systems? (i.e., criminal history and motor vehicle records) |
|        | APTA - Conducting Background Investigations (Sign in to APTA’s website or close login screen and document will open) |
|        | Standard: The agency conducts an appropriate level of background check on all frontline employees, maintenance employees, and employees with access to sensitive security information/facilities/systems. |
|        | ASIS International – Pre-employment Background Screening |

14.102 | To the extent allowed by agency policy or law, does the agency conduct background investigations on contractors, including vendors, with access to critical facilities, sensitive security systems, and sensitive security information? |
|        | Standard: The agency (a) conducts an appropriate level of background check on relevant contract employees or (b) the agency builds appropriate background check criteria into the bid process and has established a method of verifying/auditing background checks. |

14.103 | Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations? |
|        | Standard: The agency’s process for conducting background investigations has been reviewed by a legal professional. |

14.104 | Does the agency have a documented process for conducting background investigations? |
### Control Access to documents of security critical systems and facilities

**The purpose of this element is to enhance system security through the identification and protection of employee and contractor document access to critical systems and facilities based upon verified need-to-know access requirements.**

<table>
<thead>
<tr>
<th>15.101</th>
<th>Does the agency keep documentation of its security critical systems, such as tunnels, bridges, HVAC systems and intrusion alarm detection systems (i.e. plans, schematics, etc.) protected from unauthorized access?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong> The agency has well-developed document control procedures that protect security-critical documentation from unauthorized access. All documents are appropriately protected: plans, schematics, etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15.102</th>
<th>Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td>A person or department has been formally tasked with administering the access control policy with respect to agency documents.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>15.103</strong></td>
<td>Does the security review committee or other designated group review document control practices, assess compliance applicable procedures, and identify discrepancies and necessary corrective action?</td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>A security review committee actively reviews document control practices, assess compliance-applicable procedures, and identifies discrepancies and corrective action regularly.</td>
</tr>
</tbody>
</table>

### 16.000 Process for handling and access to Sensitive Security Information (SSI)

The purpose of this element is to enhance system security through the identification and documentation of critical systems and facility access based upon employee and contractor verified access needs requirements.

| **16.101** | Does the agency have a documented policy for identifying and controlling the distribution of and access to documents it considers to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520? |
| **Standard:** | The agency has a fully-developed policy for identifying and controlling the distribution of and access to SSI documents. This policy is documented and includes all of the following: (1) what materials are considered SSI; (2) how SSI is marked; (3) who has access to SSI; and (4) how SSI is shared or distributed. |
| **16.102** | Does the agency have a documented policy for proper handling, control, and storage of documents labeled as or otherwise |

**FTA - Sensitive Security Information (SSI)**

**TCRP - RECONCILING SECURITY, DISCLOSURE, AND RECORD-RETENTION REQUIREMENTS IN TRANSIT PROCUREMENTS**
<table>
<thead>
<tr>
<th>Standard:</th>
<th>The agency has a fully-developed policy for identifying and controlling the distribution of and access to SSI documents. This policy is documented and includes all of the following: (1) proper handling of SSI (how distribution is tracked, how SSI should be treated once received by employees, etc.); (2) how SSI is stored and secured (locked, encrypted, etc.); and (3) how SSI is destroyed/disposed of.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>16.103</strong></td>
<td><strong>Are employees who may be provided SSI materials per 49 CFR Part 15 or 1520) familiar with the documented policy for the proper handling of such materials?</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>Based on a random sampling of frontline personnel interviews, all employees who may be provided SSI materials have a working knowledge of the agency's SSI policy—including (a) what constitutes SSI, (b) how it is controlled, (c) how it is handled, and (d) how it is stored.</td>
</tr>
<tr>
<td><strong>16.104</strong></td>
<td><strong>Have employees provided access to SSI material per 49 CFR Part 15 or 1520 received training on proper labeling, handling, dissemination, and storage (such as through the TSA on-line SSI training program)?</strong></td>
</tr>
<tr>
<td><strong>Standard:</strong></td>
<td>The agency has established official SSI training (with appropriate materials), and based on a sampling of frontline personnel interviews, all</td>
</tr>
</tbody>
</table>
employees who may be provided access to SSI have been provided the training.

<table>
<thead>
<tr>
<th>17.000 Audit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>The purpose of this element is to assess the effectiveness of the agency’s Security Program as related to the inspection, monitoring, auditing and documentation processes and procedures established for all agency functions as well as all of its contractors.</td>
</tr>
</tbody>
</table>

| 17.101 | Has the agency established a schedule for conducting its internal security audit process? |
|---------|
| **Standard:** The agency has a documented schedule for conducting internal security audits in an ongoing manner over a three-year period. |

| 17.102 | Does the SSP contain a description of the process used by the agency to audit its implementation of the SSP over the course of the agency's published schedule? |
|---------|
| **Standard:** The agency has a detailed, well-documented process for conducting internal security reviews. This process is described in the SSP and includes the following: (1) what activities and documents are audited; (2) how these items are audited (methods of verification); and (3) the extent/depth/level of the audit. |

| 17.103 | Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process? |
|---------|
| **Standard:** The agency has well-developed procedures for conducting internal security audits and uses checklists/forms to properly and consistently conduct audits. |

| 17.104 | Is the transit agency complying with its internal security audit schedule? |

- APTA - Security Planning for Public Transit
- FTA – Recommended Best Practices for States Conducting Three-Year Safety Reviews
- APTA - Random Counterterrorism Measures on Transit Systems (Sign in to APTA’s website or close login screen and document will open)
- APTA - Security Program Considerations for Public Transit
<table>
<thead>
<tr>
<th>Standard: The agency is conducting internal security audits in a manner that reflects its established schedule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>17.105</strong> Is each internal security audit documented in a written report, which includes evaluation of the adequacy and effectiveness of the SSP element and applicable implementing procedures audited, needed corrected actions, needed recommendations, an implementation schedule for corrective actions and status reporting?</td>
</tr>
<tr>
<td>Standard: All internal security audits are documented in a written report, which include all of the following: (1) evaluation of all audited items, including a policy and its implementation; and (2) corrective/recommended actions.</td>
</tr>
<tr>
<td><strong>17.106</strong> In the last 12 months, has the Security Review Committee (or other designated group) addressed the findings and recommendations from the internal security audits, and updated plans, protocols and processes as necessary?</td>
</tr>
<tr>
<td>Standard: In the last 12 months, the Security Review Committee has reviewed audit reports, addressed findings, and updated plans and protocols as necessary.</td>
</tr>
<tr>
<td><strong>17.107</strong> Does the transit agency’s internal security audit process ensure that auditors are independent from those responsible for the activity being audited?</td>
</tr>
<tr>
<td>Standard: Auditors are independent from the individuals they are tasked with auditing to prevent any conflicts of interest.</td>
</tr>
<tr>
<td><strong>17.108</strong> Has the agency made its internal security audit schedule available to the SSO agency?</td>
</tr>
<tr>
<td>Standard:</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>17.109</strong></td>
</tr>
<tr>
<td>Standard:</td>
</tr>
<tr>
<td><strong>17.110</strong></td>
</tr>
<tr>
<td>Standard:</td>
</tr>
<tr>
<td><strong>17.111</strong></td>
</tr>
<tr>
<td>Standard:</td>
</tr>
<tr>
<td><strong>17.112</strong></td>
</tr>
<tr>
<td>Standard:</td>
</tr>
</tbody>
</table>
17.113 Was that certification included with the most recent annual report submitted to the SSO agency?

Standard: The previously mentioned certification was included with the most recent annual report submitted to the SSO agency.

17.114 If the agency's chief executive was not able to certify to the SSO agency that the agency is in compliance with its SSP, was a corrective action plan developed and made available to the SSO?

Standard: A corrective action plan was developed and made available to the SSO.

**ADDITIONAL RESOURCES**

Lessons Learned Information Sharing (LLIS.gov) is a U.S. Department of Homeland Security/Federal Emergency Management Agency program. This information and collaboration resource helps first responders, emergency managers, and homeland security officials prepare for, protect against, respond to, recover from, and mitigate terrorist attacks, natural disasters, and other emergencies. LLIS.gov provides Federal, State, local, tribal, and territorial responders and managers from all disciplines with a wealth of information and front-line expertise on effective planning, training, and operational practices.

https://emilms.fema.gov/IS0921a/CIPP0104280text1.htm

The APTA Resource Library offers a comprehensive collections of reports, studies, and publications for and about public transportation – from statistics to committee – guidance documents and much more

http://www.apta.com/resources/Pages/Default.aspx
http://www.apta.com/resources/standards/Pages/default.aspx
<p>| The Federal Transit Administration (FTA), through the Office of Safety and Oversight, oversees a host of programs focused on achieving the highest level of safety in America’s public transit systems. The Office of Safety and Oversight is responsible for guiding the development and implementation of programs and initiatives to continually improve the safety of passengers, employees, and the community. A cornerstone in meeting this mission is the re-engineered and revitalized Transit Bus Safety Program. | <a href="https://www.transit.dot.gov/regulations-and-guidance/safety/transit-safety-oversight-tso">https://www.transit.dot.gov/regulations-and-guidance/safety/transit-safety-oversight-tso</a> |
| DHS provides security grants to mass transit and passenger rail systems, intercity bus companies, freight railroad carriers, ferries and the trucking industry to help protect the public and nation’s critical transportation infrastructure against acts of terrorism and other large-scale events. The grants support high-impact security projects that have a high efficacy in reducing the most risk to our nation’s transportation systems. | <a href="https://www.grants.gov/web/grants/learn-grants/grant-making-agencies/department-of-homeland-security.html">https://www.grants.gov/web/grants/learn-grants/grant-making-agencies/department-of-homeland-security.html</a> |</p>
<table>
<thead>
<tr>
<th>Document</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>APTA Chain Link, Mesh, or Woven Fencing Systems to Control Access, APTA-SS-SIS-RP004-10, 2010</td>
<td></td>
</tr>
<tr>
<td>APTA Crime Prevention through Environmental Design (CPTED), APTA-SS-SIS-RP-00710, 2010</td>
<td></td>
</tr>
<tr>
<td>APTA Developing a Contagious Virus Response Plan, APTA-SS-SEM-S-005-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Fencing Systems to Control Access, APTA-SS-SIS-RP-003-10, 2010</td>
<td></td>
</tr>
<tr>
<td>APTA Gates to Control Access, APTA-SS-SIS-RP-005-10, 2010</td>
<td></td>
</tr>
<tr>
<td>APTA Recognizing and Responding to Unattended Packages, Objects and Baggage, APTASS-SRM-RP-007-12, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice Conducting Nonrevenue Vehicle Security Inspections, APTASS-SRM-RP-003-009, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice Conducting Revenue Vehicle Security Inspections, APTA-SSSRM-RP-012-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice Creating an Alternate or Backup OCC, APTA-SS-SEM-RP007-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice for Conducting Background Investigations, APTA-SS-SRMRP-004-11, 2011</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice for First Responder Familiarization of Transit Systems, APTA-SS-SEM-RP-002-08, 2008</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice for Participating in Mutual Aid, APTA-SS-SEM-RP-011-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Recommended Practice Identifying Suspicious Behavior in Mass Transit, APTA-SSSRM-RP-009-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Safe Mail and Package Handling, APTA-SS-SEM-RP-008-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Security Awareness Training for Transit Employees, APTA-SS-SRM-RP-005-12, 2012</td>
<td></td>
</tr>
<tr>
<td>APTA Security Considerations for Public Transit, APTA-SS-SIS-S-010-13, 2013</td>
<td></td>
</tr>
<tr>
<td>APTA Shelter of Transit Vehicles and Nonrevenue Equipment During Emergencies, APTASS-SEM-S-006-09, 2009</td>
<td></td>
</tr>
<tr>
<td>APTA Standard for Security &amp; Emergency Management Aspects of Special Events Service</td>
<td></td>
</tr>
<tr>
<td>APTA Transit Incident Drills and Exercises, APTA-SS-SM-S-004-9, 2009</td>
<td></td>
</tr>
<tr>
<td>DHS</td>
<td>Homeland Security Exercise and Evaluation Program (HSEEP), Volume 1: HSEEP Overview and Exercise Program Management, DHS, 2007</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DHS</td>
<td>National Disaster Recovery Framework (NDRF), DHS, 2011</td>
</tr>
<tr>
<td>DHS</td>
<td>National Incident Management System, DHS, 2008</td>
</tr>
<tr>
<td>DHS</td>
<td>National Infrastructure Protection Plan (NIPP), DHS, 2013</td>
</tr>
<tr>
<td>DHS</td>
<td>National Response Framework (NRF), DHS, 2013</td>
</tr>
<tr>
<td>DHS</td>
<td>Roadmap to Secure Control Systems in the Transportation Sector, DHS, 2012</td>
</tr>
<tr>
<td>DHS</td>
<td>See Something, Say Something, NYCMTA, endorsed by DHS</td>
</tr>
<tr>
<td>FTA</td>
<td>An Introduction to All-hazards Preparedness for Transit Agencies, FTA, 2010</td>
</tr>
<tr>
<td>FTA</td>
<td>Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel Systems, FTA, 2010</td>
</tr>
<tr>
<td>FTA</td>
<td>Handbook for Transit Safety and Security Certification, FTA, 2000</td>
</tr>
<tr>
<td>FTA</td>
<td>National Transit Database (NTD), Safety and Security Reporting Manual, FTA, 2013</td>
</tr>
<tr>
<td>FTA</td>
<td>Response and Recovery for Declared Emergencies and Disasters, A Resource Document for Transit Agencies</td>
</tr>
<tr>
<td>FTA</td>
<td>Transit Security Design Considerations, FTA, 2004</td>
</tr>
<tr>
<td>FTA</td>
<td>Transit Watch, FTA</td>
</tr>
<tr>
<td>NIST</td>
<td>NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, NIST, 2012</td>
</tr>
<tr>
<td>NIST</td>
<td>NIST Special Publication 800-64, Revision 2, Security Considerations in the System Development Life Cycle</td>
</tr>
<tr>
<td>NIST</td>
<td>NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS) and other control system configurations such as Programmable Logic Controllers (PLC), NIST, 2011</td>
</tr>
<tr>
<td>NIST</td>
<td>NIST Special Publication 800-94, Revision 1 (Draft), Guide to Intrusion Detection and Prevention Systems</td>
</tr>
</tbody>
</table>
### DOCUMENT LIST

| TRB     | NCHRP Report 525, Volume 14, Security 101: A Physical Security Primer for Transportation Agencies |
| TRB     | NCHRP Report 525, Volume 15, Costing Asset Protection: An All Hazards Guide for Transportation Agencies |
| TRB     | TCRP Report 86, Volume 12, Making Transportation Tunnels Safe and Secure, TRB/TCRP, 2006 |
| TRB     | TCRP Report 86, Volume 6, Applicability of Portable Explosive Detection Devices in Transit Environments, |
| TRB     | TCRP Report 86, Volume 8, Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies, TRB/TCRP, 2005 |
| TRB     | TCRP Report 86, Volume 9, Guidelines for Transportation Emergency Training Exercises, TRB/TCRP, 2006 |
| TRB     | The Role of Transit in Emergency Evacuation, TRB SF-294, 2008 |
| TSA     | Additional Guidance on Background Checks, Redress and Immigration Status, TSA, 2006 |
| TSA     | Sensitive Security Information (SSI) Best Practices Guide for non-DHS Employees and Contractors, |
| TSA     | TSA Mass Transit, Bus and Passenger Rail Security Awareness Message, Protective Measures |
| USCG    | Navigation and Vessel Inspection Circular (NVIC) No. 11-02, Recommended Security Guidelines for Facilities |

### Appendix A - FY16 BASE Changes
<table>
<thead>
<tr>
<th>BASE Question #</th>
<th>Changes to BASE Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>