

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.

# BASE Resource Kit (BRK)



Transportation  
Security  
Administration

Office of Security Operations (OSO), Surface Compliance  
Office of Security Policy & Industry Engagement (OSPIE)  
601 S. 12th Street, Arlington, VA 20528

---

## 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

**Revision: 4.1**

**Date of Revision: 13 October 2017**

---

program, contact the TSA Office of Security Operations (OSO), Surface Compliance Branch at [STSIP@dhs.gov](mailto:STSIP@dhs.gov) or Office of Security Policy and Industry Engagement (OSPIE), Mass Transit at [tsa.seccoord@tsa.dhs.gov](mailto:tsa.seccoord@tsa.dhs.gov).

## CONTENTS

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



<b>1.000</b>		<b>Establish Written System Security Plans (SSPs) and Emergency Response Plan (ERP)</b>	
<p>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.</p>			
<b>MANAGEMENT AND ACCOUNTABILITY</b>	<b>1.100</b>	<b>System Security Plan (SSP)</b>	<b>BASE RESOURCE LIBRARY:</b>
	<b>1.101</b>	<b>Does the transit agency have a System Security Plan (SSP) which addresses personnel security, facility security, vehicle security and Threat/Vulnerability Management?</b>	
	<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>FTA – Model System Security Program Plan (SSP) Template</u></a></p>
	<b>1.102</b>	<b>Does the SSP identify and actively monitor the goals and objectives for the security program?</b>	<p><a href="#"><u>FTA System Security and Emergency Preparedness Plan (SEPP) Template</u></a></p>
	<p><b>Standard:</b> Goals and objectives are identified, documented and actively monitored to ensure the SSP is fulfilling its purpose.</p>		<p><a href="#"><u>FTA System Security and Emergency Preparedness Plan (SEPP) Appendix G</u></a></p>
	<b>1.103</b>	<b>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?</b>	<p><a href="#"><u>APTA - Security Planning for Public Transit</u></a></p>
	<p><b>Standard:</b> 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.</p>		
	<b>1.104</b>	<b>Is the SSP separate from the agency's System Safety Program Plan (SSPP)?</b>	<p><a href="#"><u>49 CFR 659.21 SSP General Requirements</u></a></p>
<p><b>Standard:</b> SSP is a stand-alone document, separate from the System Safety Program Plan.</p>			

<p><b>1.105</b></p>	<p><b>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)</b></p>	<p><a href="#"><u>APTA Security and Emergency Preparedness Plan Template</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>FTA System Security and Emergency Preparedness Program Plan Template</u></a></p>
<p><b>1.106</b></p>	<p><b>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?</b></p>	<p><a href="#"><u>FTA System Security and Emergency Preparedness Program Plan Template</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>FTA-Standard Protocol for Managing Security Incident Involving Surface Transit Vehicles</u></a></p>
<p><b>1.107</b></p>	<p><b>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.)?</b></p>	<p><a href="#"><u>National Incident Management System</u></a> <a href="#"><u>FTA Emergency Preparedness / Emergency Management</u></a></p>
<p><b>Standard:</b> Well-developed, <i>specific</i> procedures are in place and documented in the SSP <i>or</i> as part of another document and referenced in the SSP.</p>		
<p><b>1.108</b></p>	<p><b>Has the agency partnered with local law enforcement/ first responders to develop Active Shooter procedures or protocols?</b></p>	<p><a href="#"><u>Active Shooter Preparedness</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>FBI – Run, Hide, Fight</u></a></p>

MANAGEMENT AND ACCOUNTABILITY	1.109	<b>Does the SSP contain or reference other documents that establish procedures or protocols for responding to active shooter events?</b>	<a href="#"><u>Active Shooter Pocket Card</u></a>
	<b>Standard:</b> Well-developed, <i>specific</i> procedures or protocols are in place that addresses Active Shooter. These procedures or protocols are documented in the SSP <i>or</i> as part of another document, such as a stand-alone Emergency Response Plan, and referenced in the SSP.		
	1.110	<b>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)?</b>	<a href="#"><u>Model Program for Responding to a Package with Suspicion of a Bio Threat - IAFC Oct. 2008</u></a>
	<b>Standard:</b> Well-developed, <i>specific</i> protocols are in place that addresses IED <i>and</i> WMD. These protocols are documented in the SSP <i>or</i> as part of another document, such as in stand-alone Emergency Response Plan (ERP), and referenced in the SSP.		<a href="#"><u>Chemical Weapons Improved Response Program (CWIRP)</u></a>
	1.111	<b>Are visible, random security measures, based on employee type, integrated into security plans to introduce unpredictability into security activities for deterrent effect?</b>	<a href="#"><u>APTA- Random Counterterrorism Measures on Transit Systems (close sign in link and document will automatically open)</u></a>
	<b>Standard:</b> Random, unpredictable measures are well-documented with specific measures assigned by employee-type. Includes both security and non-security personnel.		
1.112	<b>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?</b>	<a href="#"><u>APTA - Security Planning for Public Transit</u></a>	
<b>Standard:</b> 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.			

<p><b>1.113</b></p>	<p><b>Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?</b></p>	<p><a href="#"><u>FEMA - CPTED</u></a></p> <p><a href="#"><u>APTA Crime Prevention Through Environmental Design (CPTED) (Sign in to APTA's website or close login screen and document will open)</u></a></p>
<p><b>Standard:</b> 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).</p>		
<p><b>1.114</b></p>	<p><b>Does the SSP require an annual review?</b></p>	
<p><b>Standard:</b> Annual review is a written requirement with verification measures in place (signed and dated).</p>		
<p><b>1.115</b></p>	<p><b>Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>1.116</b></p>	<p><b>Has an annual review of the SSP been performed and documented in the preceding 12 months?</b></p>	
<p><b>Standard:</b> Annual review is verifiable by document review.</p>		
<p><b>1.117</b></p>	<p><b>Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP?</b></p>	
<p><b>Standard:</b> Documented process for securing SSO review and approval of SSP is included in writing, or directly referenced, in the SSP.</p>		
<p><b>1.118</b></p>	<p><b>Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?</b></p>	
<p><b>Standard:</b> Approval (including date of approved) is verifiable through document review.</p>		

		BASE RESOURCE LIBRARY:	
MANAGEMENT AND ACCOUNTABILITY	<b>1.200</b>	<b>Emergency Response Plan (ERP)</b>	<a href="#"><u>APTA Security and Emergency Preparedness Plan Template</u></a>  <a href="#"><u>APTA - Emergency Response and Preparedness Program (ERPP)</u></a>  <a href="#"><u>APTA - Development of a SEPP</u></a>
	<b>1.201</b>	<b>Does the transit agency have an Emergency Response Plan (ERP) which addresses specific policies and procedures related to emergency response?</b>	
	<b>Standard:</b> 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.		
	<b>1.202</b>	<b>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?</b>	
	<b>Standard:</b> Policy statement is well developed and includes all elements: endorsement statement, applicability, authority establishing the plan, and approval signature from the agencies chief executive.		
	<b>1.203</b>	<b>Does the ERP require an annual review to determine if it needs to be updated?</b>	
	<b>Standard:</b> Annual review is a written requirement with verification measures in place (signed and dated).		
	<b>1.204</b>	<b>Has an annual review of the ERP been performed and documented in the preceding 12 months?</b>	
	<b>Standard:</b> Annual review, including date and signature is verifiable by document review.		
	<b>1.205</b>	<b>Does the ERP include a process or review provision to ensure coordination with the transit agency's SSPP and SSP?</b>	
<b>Standard:</b> ERP includes documented provisions that ensure its coordination with the agency's safety and security plans.			
<b>1.206</b>	<b>Has the transit agency received documentation from the SSO confirming its review and approval of the ERP currently in effect?</b>		
<b>Standard:</b> Approval (including date of approval) is verifiable.			

<p><b>1.207</b></p>	<p><b>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.)</b></p>	<p><a href="#"><u>National Incident Management System</u></a></p>
<p><b>Standard:</b> Well-developed, <i>specific</i> procedures are in place and documented in the ERP <i>or</i> as part of another document and referenced in the ERP.</p>		
<p><b>1.208</b></p>	<p><b>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)?</b></p>	<p><a href="#"><u>APTA – Emergency Communication Strategies for Transit Agencies</u></a></p>
<p><b>Standard:</b> 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.</p>		
<p><b>1.209</b></p>	<p><b>Does the ERP contain or reference other documents to provide for Continuity of Operations (COOP) while responding to emergency events?</b></p>	<p><a href="#"><u>APTA - Standard for a Continuity of Operations Plan for Transit Agencies</u></a></p> <p><a href="#"><u>FEMA COOP Plan</u></a></p>
<p><b>Standard:</b> Continuity of Operations plans exists and are included as part of the ERP (or in another document that is referenced in the ERP).</p>		<p><a href="#"><u>FEMA COOP Plan Template</u></a></p> <p><a href="#"><u>Continuity of Operations Planning Guidelines for Transportation Agencies</u></a></p>
<p><b>1.210</b></p>	<p><b>Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event?</b></p>	<p><a href="#"><u>APTA COOP</u></a></p>
<p><b>Standard:</b> 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 "normal" 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.</p>		

	1.211	<b>Does the agency have a written Business Continuity Plan and COOP to guide restoration of facilities and services following an emergency event?</b>	
	<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>NFPA 1600: Standard on Disaster-Emergency Management and Business Continuity Programs</u></a></p> <p><a href="#"><u>Ready.gov: Business Continuity Plan</u></a></p>
	1.212	<b>Does the agency have a back-up operations control center capability?</b>	
	<p><b>Standard:</b> 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.</p>		
<p><b>2.000 Define Roles and Responsibilities for Security and Emergency Management</b></p>			
<b>MANAGEMENT AND ACCOUNTABILITY</b>	<p>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.</p>		
	2.100	System Security Plan (SSP)	<b>BASE RESOURCE LIBRARY:</b>
	2.101	<p><b>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?</b></p>	<p><a href="#"><u>FTA System Security and Emergency Preparedness Plan (SEPP) Appendix G:</u></a></p> <p><a href="#"><u>FTA System Security and Emergency Preparedness Plan (SEPP) Template:</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>APTA Recommended Practice for SEPP</u></a></p>	

2.102	<b>Has the agency established documented lines of delegated authority and lines of succession of security responsibilities?</b>	
<p><b>Standard:</b> The agency has established comprehensive policies and procedures related to "chain of command" <i>and</i> "lines of succession" 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.</p>		
2.103	<b>Does the SSP or other documents establish roles and responsibilities for security and/or law enforcement personnel based on title and/or position?</b>	
<p><b>Standard:</b> 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.</p>		
2.104	<b>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)</b>	
<p><b>Standard:</b> 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.</p>		
2.105	<b>Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes?</b>	
<p><b>Standard:</b> Senior staff and management conduct security meetings on a quarterly basis, at minimum, to review recommendations for changes to plans and processes.</p>		

<p><b>2.106</b></p>	<p><b>Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>2.107</b></p>	<p><b>Are informational briefings with appropriate personnel held whenever security protocols, threat levels, or protective measures are updated or as security conditions warrant?</b></p>	
<p><b>Standard:</b> 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.)</p>		
<p><b>2.108</b></p>	<p><b>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?</b></p>	
<p><b>Standard:</b> 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.).</p>		

<b>MANAGEMENT AND ACCOUNTABILITY</b>	2.109	<b>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?</b>	Submit Security Coordinators contact information to: <a href="mailto:tsa.seccoord@tsa.dhs.gov">tsa.seccoord@tsa.dhs.gov</a>
	<b>Standard:</b> 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.		
	2.110	<b>Does the agency maintain a record of security related incidents that are reported within the agency?</b>	
	<b>Standard:</b> 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.		
	2.200	<b>Emergency Response Plan (ERP)</b>	<b>BASE RESOURCE LIBRARY:</b>
	2.201	<b>Does the ERP establish and assign responsibility for implementation of the emergency response program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?</b>	<a href="#"><u>FTA System Security and Emergency Preparedness Plan (SEPP) Template</u></a>
	<b>Standard:</b> 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 ERP.		
	2.202	<b>Are detailed, comprehensive emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?</b>	
<b>Standard:</b> 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.		<a href="#"><u>FTA System Security and Emergency Preparedness Plan (SEPP) Appendix G:</u></a>	

2.203	<b>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)</b>	
<b>Standard:</b> Roles and responsibilities of frontline personnel are assigned by position and documented in the ERP. Roles are comprehensive and detailed.		
2.204	<b>Has the ERP been distributed to appropriate departments in the organization?</b>	
<b>Standard:</b> 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.		
2.205	<b>Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the ERP?</b>	
<b>Standard:</b> 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.		
2.206	<b>Are senior staff and middle management ERP coordination meetings held on a regular basis?</b>	
<b>Standard:</b> Senior staff and management conduct ERP coordination meetings on a monthly basis.		

	<p><b>2.207 Are informational briefings with appropriate personnel held whenever emergency response protocols are substantially changed or updated?</b></p>	
	<p><b>Standard:</b> 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.).</p>	
<p><b>3.000</b></p>	<p><b>Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control</b></p>	
<p><b>MANAGEMENT AND ACCOUNTABILITY</b></p>	<p><b>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.</b></p>	
	<p><b>3.101 How frequently do managers and supervisors provide information to front-line personnel where security and emergency response issues are the primary focus?</b></p>	
	<p><b>Standard:</b> 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).</p>	
	<p><b>3.102 How frequently are supervisor, manager, and/or foreperson security review and coordination briefings held?</b></p>	
<p><b>Standard:</b> Supervisor/management security review and coordination meetings are held on a monthly basis.</p>		

	<p><b>3.103 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)</b></p>	
	<p><b>Standard:</b> 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.</p>	
	<p><b>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?</b></p>	
	<p><b>Standard:</b> There is a written policy that requires leadership to debrief frontline personnel regarding their involvement in or management of any security or emergency incidents.</p>	
<p><b>4.000</b></p>	<p><b>Coordinate Security and Emergency Management Plan(s) with local and regional agencies</b></p>	
<p><b>MANAGEMENT AND ACCOUNTABILITY</b></p>	<p><b>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.</b></p>	
	<p><b>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?</b></p> <p><b>Standard:</b> 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.</p>	<p><a href="#"><u>APTA - Mutual Aid (Sign in to APTA's website or close login screen and document will open)</u></a></p>

<p><b>4.102</b></p>	<p><b>Does the agency participate in a regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and response?</b></p>	<p><a href="#"><u>FEMA State Offices and Agencies of Emergency Management</u></a></p> <p><a href="#"><u>APTA Security &amp; Emergency management Aspects of Special Event Service</u></a></p>
<p><b>Standard:</b> The agency participates in a regional security and emergency preparedness/management working group or committee. <i>(This is not the same as participation in drills or exercises)</i></p>		<p><a href="#"><u>DHS State Homeland Security and Emergency Services</u></a></p>
<p><b>4.103</b></p>	<p><b>Have regional incident management protocols been shared with the agency and incorporated into the agency's ERP/SSP/SEPP?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>4.104</b></p>	<p><b>Have agency resources been appropriately identified and provided to the regional EMA?</b></p>	<p><a href="#"><u>APTA - First Responder Familiarization of Transit Systems</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>DHS State Homeland Security and Emergency Services</u></a></p> <p><a href="#"><u>FEMA ICS Resource Center</u></a></p>
<p><b>4.105</b></p>	<p><b>Does the agency have a designated point-of-contact or liaison from the local/regional Emergency Operations Center (EOC)?</b></p>	<p><a href="#"><u>APTA - Contagious Virus Response</u></a></p> <p><a href="#"><u>ICS Forms</u></a></p>
<p><b>Standard:</b> Agency has established a point-of-contact at the Emergency Operations Center.</p>		<p><a href="#"><u>Surface Transportation and Public Transportation Information Sharing and Analysis Center</u></a></p> <p><a href="#"><u>The Role of Transit in Emergency Evacuation - Transportation Research Board Special Report</u></a></p>
<p><b>4.106</b></p>	<p><b>Does the agency send a representative to the local/regional EOC, should it be activated?</b></p>	
<p><b>Standard:</b> Agency has officially designated a representative to be sent to the EOC, upon activation. This is documented in SSP/ERP/SEPP.</p>		

<p><b>4.107</b></p>	<p><b>Does the agency have information sharing capabilities with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>4.108</b></p>	<p><b>Has the agency developed internal incident management protocols that comply with the National Response Plan and the National Incident Management System (NIMS)?</b></p>	<p><a href="#"><u>FEMA EMI Incident Command System Resource Center</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>FEMA NIMS Training</u></a></p> <p><a href="#"><u>Quick Reference Guide for the National Response Plan</u></a></p>
<p><b>4.109</b></p>	<p><b>Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?</b></p>	
<p><b>Standard:</b> The agency has shared its internal emergency response protocols with the regional EMA and appropriate first response agencies.</p>		
<p><b>4.110</b></p>	<p><b>Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?</b></p>	<p><a href="http://transitwireless.org/"><u>http://transitwireless.org/</u></a></p>
<p><b>Standard:</b> 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.</p>		

<b>5.00 0</b>	<b>Establish and Maintain a Security and Emergency Training Program</b>	
<b>SECURITY AND EMERGENCY RESPONSE TRAINING</b>	<b>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.</b>	
	<b>5.101</b>	<b>Is initial training provided to all new agency employees regarding security orientation/awareness?</b>
	<b>Standard:</b> 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).	
	<b>5.102</b>	<b>Is annual refresher training regarding security orientation/awareness provided to all employees regardless of position or job function in a formal manner?</b>
	<b>Standard:</b> 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).	
	<b>5.105</b>	<b>Is ongoing advanced security training focused on job function provided at least annually?</b>
	<b>Standard:</b> 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).	
	<b>5.106</b>	<b>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?</b>
<b>Standard:</b> <u>All</u> employees, regardless of job function, receive initial training, which is focused on Active Shooter. The agency has a well-developed program with an		
		<p><a href="#"><u>DHS State Homeland Security and Emergency Services</u></a></p> <p><a href="#"><u>Transportation Safety Institute - Transit Safety and Security Training</u></a></p> <p><a href="#"><u>FTA Transit Security Training Tools</u></a></p> <p><a href="#"><u>Online SAR Training</u></a></p> <p><a href="#"><u>FTA/NTI Sponsored Course Catalog</u></a></p> <p><a href="#"><u>National Transit Institute</u></a></p> <p><a href="#"><u>APTA - Security Awareness Training for Transit Employees (Sign in to APTA's website or close login screen and document will open)</u></a></p> <p><a href="#"><u>Active Shooter Pocket Card</u></a></p>

<p>official curriculum and training is provided in a formal environment (classroom or computer-based).</p>	<p><a href="#"><u>FBI – Run, Hide, Fight</u></a></p>
<p><b>5.107</b> 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?</p>	<p><a href="#"><u>FEMA Emergency Management Institute</u></a></p> <p><a href="#"><u>Active Shooter Preparedness</u></a></p>
<p><b>Standard:</b> <u>All</u> 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).</p>	<p><a href="#"><u>FBI – Run, Hide, Fight</u></a></p> <p><a href="#"><u>Rural Domestic Preparedness Consortium (RDPC) - First Responder Training Material</u></a></p>
<p><b>5.108</b> Is initial training provided to all new transit employees regarding emergency response?</p>	<p><a href="#"><u>Land Transportation Anti-Terrorism Training Program (LTATP)</u></a></p>
<p><b>Standard:</b> 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).</p>	
<p><b>5.109</b> Is annual refresher training regarding emergency response provided to all employees regardless of position or job function in a formal manner?</p>	
<p><b>Standard:</b> 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).</p>	
<p><b>5.112</b> Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System (NIMS)?</p>	<p><a href="#"><u>FEMA EMI Incident Command System Resource Center</u></a></p> <p><a href="#"><u>FEMA ICS and NIMS Training</u></a></p> <p><a href="#"><u>FEMA NIMS Training</u></a></p>
<p><b>Standard:</b> 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</p>	

	curriculum and training is provided annually in a formal environment (classroom or computer-based).	
	<b>5.113</b> Has ICS and NIMS training appropriate to the position been provided to Senior Management staff and supervisors? (Describe the frequency of training)	
	<b>Standard:</b> Annual ICS and NIMS training based on job function is provided by the agency to all senior leadership.	<a href="#">FTA Transit Security Training Tools</a>
	<b>5.114</b> Has ICS and NIMS training appropriate to the position been provided to frontline employees?	<a href="#">DHS State Homeland Security and Emergency Services</a>
	<b>Standard:</b> Annual ICS and NIMS training based on job function is provided by the agency to all supervisors and managers.	<a href="#">FTA/NTI Sponsored Course Catalog</a>
	<b>5.116</b> Has the agency developed a program and provided initial training on its own incident response protocols?	<a href="#">APTA - Security Awareness Training for Transit Employees (Sign in to APTA's website or close login screen and document will open)</a>
	<b>Standard:</b> 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).	<a href="#">FEMA Emergency Management Institute</a>
<b>SECURITY AND</b>	<b>5.117</b> 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?	

<b>Standard:</b> Annual training is provided to all employees regardless of position or job function.		
<b>5.120</b>	<b>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?</b>	<a href="#"><u>Introduction to Incident Command System - ICS-100</u></a>
<b>Standard:</b> 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).		<a href="#"><u>FTA Transit Security Training Tools</u></a> <a href="#"><u>DHS State Homeland Security and Emergency Services</u></a>
<b>5.121</b>	<b>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?</b>	<a href="#"><u>FTA/NTI Sponsored Course Catalog</u></a> <a href="#"><u>APTA Security Awareness Training for Transit Employees (Sign in to APTA’s website or close login screen and document will open)</u></a>
<b>Standard:</b> Annual training based on job function is provided by the agency to all senior leadership.		<a href="#"><u>FEMA Emergency Management Institute</u></a>
<b>5.124</b>	<b>Do law enforcement/security department personnel, security managers at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.</b>	<a href="#"><u>National Transit Institute</u></a>
<b>Standard:</b> 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		

<p>provided in a formal environment (classroom or computer-based).</p>	
<p><b>5.125 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.</b></p>	<p><a href="#"><u>New Mexico Tech, Incident Response to Terrorist Bombings (IRTB), Prevention of and Response to Suicide Bombing Incidents</u></a></p>
<p><b>Standard:</b> 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).</p>	
<p><b>5.126 Does the agency have an established program to monitor and schedule employee training?</b></p>	
<p><b>Standard:</b> 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.</p>	
<p><b>5.127 Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?</b></p>	
<p><b>Standard:</b> The agency has a formal system to <u>record and track</u> personnel training for <u>all security-related training</u>, including initial, annual, and periodic. Records for <u>all</u> employees contain the following: employee</p>	

<p>name/identifier, training/course identifier, and date of course completion. Must be verified by Document Review.</p>		
<p><b>5.128</b></p>	<p><b>Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?</b></p>	
<p><b>Standard:</b> The agency has a formal system to <i><b>record and track</b></i> personnel training for <i><b>all emergency response-related training</b></i>, including initial, annual, and periodic. Records for <i><b>all</b></i> employees contain the following: employee name/identifier, training/course identifier, and date of course completion.</p>		
<p><b>5.129</b></p>	<p><b>Does the agency have a program to regularly review and update security awareness and emergency response training materials?</b></p>	
<p><b>Standard:</b> 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 "role/responsibility"), and the program ensures materials are reviewed at least annually.</p>		
<p><b>5.130</b></p>	<p><b>Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?</b></p>	
<p><b>Standard:</b> Appropriate personnel are notified of operational changes--including those related to threat levels and protective measures. Individuals with a "need to know" have been formally identified, and measures are in place to effectively reach <i><b>all</b></i> appropriate employees.</p>		

<b>SECURITY AND EMERGENCY RESPONSE TRAINING</b>	<p><b>5.131 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.</b></p>	
	<p><b>Standard:</b> The agency's security and emergency response training covers response and recovery operations in critical facilities and infrastructure (including COOP-related procedures). Training is part of an official curriculum, utilizes effective training materials, and is provided in a formal environment (classroom or computer-based).</p>	
	<p><b>5.132 Has the agency provided training to regional first responders to enable them to operate in critical facilities and infrastructure?</b></p>	<p><a href="#"><u>DHS State Homeland Security and Emergency Services</u></a></p> <p><a href="#"><u>FEMA NIMS Training</u></a></p> <p><a href="#"><u>FTA Transit Security Training Tools</u></a></p> <p><a href="#"><u>FTA/NTI Sponsored Course Catalog</u></a></p> <p><a href="#"><u>DHS NTAS</u></a></p>
	<p><b>Standard:</b> The agency has provided training to regional first responders to enable them to operate in critical facilities and infrastructure. The training is well-developed, and the agency has actively offered it to outside entities.</p>	
	<p><b>5.133 Has the agency provided local law enforcement/first responders opportunities to familiarize themselves with agency's system for response to Active Shooter events?</b></p>	<p><a href="#"><u>TSA I-STEP Program</u></a></p> <p><a href="#"><u>TCRP Rept. 86v13 Public Transportation Passenger Security Inspections- Chapter 3 (Collaboration with Local Law Enforcement)</u></a></p> <p><a href="#"><u>Active Shooter Preparedness</u></a></p>
	<p><b>Standard:</b> The agency has developed and implemented a program to orient local law enforcement and first responders on their system specifically for response to Active Shooter events. The agency actively offers this familiarization separate from drills or exercises.</p>	
<p><b>5.134 Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?</b></p>	<p><a href="#"><u>Operation Lifesaver - Rail Safety for Emergency Responders training request</u></a></p> <p><a href="#"><u>APTA - First Responder Familiarization (Sign in to APTA's website or close login screen and document will open)</u></a></p>	
<p><b>Standard:</b> The concept and employment of visible, unpredictable, and random security measures is included as part of the training curriculum for <i>all</i> personnel in security-related positions. This is documented in training materials.</p>		

	<p><b>5.135</b> 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?</p>	
	<p><b>Standard:</b> The agency has developed and implemented a program to <i>annually</i> 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.</p>	
<p><b>6.000</b> Establish plans and protocols to respond to the DHS National Terrorism Advisory System (NTAS).</p>		
<p>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.</p>		
<p><b>NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)</b></p>	<p><b>6.101</b> Does the SSP contain or reference other documents identifying incremental actions (imminent or elevated) to be implemented for a NTAS threat?</p>	<p><a href="#"><u>DHS NTAS</u></a></p>
	<p><b>Standard:</b> 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.</p>	
	<p><b>6.102</b> Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?</p>	
	<p><b>Standard:</b> 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.</p>	

	<p><b>6.103</b> Has the agency provided annual training and/or instruction focused on job function regarding the incremental activities to be performed by employees?</p>	
	<p><b>Standard:</b> 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).</p>	
<b>7.000</b>	<b>Implement and reinforce a Public Security and Emergency Awareness program.</b>	
	<p>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.</p>	
<b>PUBLIC AWARENESS</b>	<p><b>7.101</b> Has the transit agency developed and implemented a public security and emergency awareness program?</p>	<p><a href="#">FTA Transit Watch Program</a></p>
	<p><b>Standard:</b> Agency has implemented a well-developed public awareness program that addresses specific issues of both security <u>and</u> emergency response.</p>	
	<p><b>7.102</b> 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)?</p>	<p><a href="#">DHS If-You-See-Something-Say-Something-Campaign</a></p>
	<p><b>Standard:</b> 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.</p>	<p><a href="#">FTA Transit Watch Program Toolkit</a></p>
	<p><b>7.103</b> Is the above consistent with agency's overall announcement program?</p>	<p><a href="#">NTAS Print Materials</a></p>

<p><b>Standard:</b> Public awareness material is consistent with the agency's overall announcement program. All information/instruction/guidance is the same.</p>	
<p><b>7.104</b> Are general security awareness and emergency preparedness messages included in public announcement messages at stations and on board vehicles?</p>	
<p><b>Standard:</b> The agency includes frequent mentions of general security <i>and</i> emergency preparedness items in its pre-recorded announcement messages at all appropriate areas, including at stations and onboard vehicles.</p>	
<p><b>7.105</b> 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.</p>	<p><a href="#"><u>FTA Transit Watch Program</u></a></p> <p><a href="#"><u>APTA - Suspicious Behavior (Sign in to APTA's website or close login screen and document will open)</u></a></p>
<p><b>Standard:</b> Passengers are urged to report unattended property, suspicious behavior, and other security concerns to an identified agency representative (uniformed crewmember, law enforcement, etc.) or identified contact number. This is documented in awareness material and readily observable.</p>	
<p><b>7.106</b> 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.)</p>	
<p><b>Standard:</b> 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.</p>	

<b>PUBLIC AWARENESS</b>	<b>7.107</b>	<b>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)</b>	
	<b>Standard:</b> The agency utilizes social media to issue public service announcements related to security or emergency response. This method is documented or readily observable.		
	<b>7.108</b>	<b>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)</b>	
	<b>Standard:</b> The agency issues security- and emergency response-related PSAs or press releases to local media. This method is documented or readily observable.		
	<b>7.109</b>	<b>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.</b>	
	<b>Standard:</b> 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.		<a href="#"><u>Community Emergency Response Team (CERT) Program</u></a>
<b>7.110</b>	<b>Does the transit agency conduct an outreach program to enlist members of the public as security awareness volunteers, similar to Neighborhood Watch programs?</b>		
<b>Standard:</b> The agency has established a volunteer program to enlist an active security awareness volunteer			

	force. This program (including how passengers can get involved) is documented.	
	<b>7.111 Do public awareness materials and/or messages inform passengers on the means to evacuate safely from transit vehicles and facilities?</b>	
	<b>Standard:</b> 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.	
	<b>7.112 Does the agency track and monitor customer complaints reported by passengers?</b>	
	<b>Standard:</b> The agency has a system in place to actively and effectively monitor and follow up on customer reports.	
<b>8.000</b>	<b>Establish and use a Risk Management Process to assess and manage threats, vulnerabilities and consequences.</b>	
	<b>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.</b>	
<b>ESTABLISH A RISK ASSESSMENT AND INFORMATION SHARING PROCESS</b>	<b>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.</b>	<a href="#"><u>DHS - Risk Management Fundamentals</u></a>
	<b>Standard:</b> Risk assessment process is developed, documented, specifically addresses threats and vulnerabilities, and is approved by management.	<a href="#"><u>FTA - An Introduction to All-Hazards Preparedness for Transit Agencies</u></a>
	<b>8.102 Has the agency identified facilities and systems it considers to be its critical assets?</b>	<a href="#"><u>FEMA – Threat and Hazard Identification and Risk Assessment Guide</u></a>
	<b>Standard:</b> The agency has identified facilities and systems it considers critical assets. This is documented (or clearly implied in documentation/procedures).	
	<b>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</b>	

	<p><b>most recent assessments and the entity(ies) that conducted the assessment(s).</b></p>	
	<p><b>Standard:</b> A vulnerability assessment focused on the agency's <i>critical assets</i> has been conducted within the last 3 years.</p>	
<b>8.104</b>	<p><b>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?</b></p>	
	<p><b>Standard:</b> 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.</p>	
<b>8.105</b>	<p><b>Has the system implemented procedures to limit and monitor access to underground and underwater tunnels? If so, summarize procedures in the justification.</b></p>	<p><a href="#"><u>APTA - Operational Strategies for Emergency Smoke Ventilation in Tunnels (Sign in to APTA's website or close login screen and document will open)</u></a></p>
	<p><b>Standard:</b> The system has well-developed, well-documented policies and procedures in place to limit and monitor access to underground and underwater tunnels.</p>	<p><a href="#"><u>NCHRP Report 525, Volume 12: Making Transportation Tunnels Safe and Secure</u></a></p>
<b>8.106</b>	<p><b>Are security investments prioritized using information developed in the risk assessment process?</b></p>	
	<p><b>Standard:</b> 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.</p>	

	<p><b>8.107</b> Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and <u>related documents</u>?</p>	
	<p><b>Standard:</b> The agency has provided TSA with <u>all</u> requested documents.</p>	
<p><b>9.000</b> Establish and use an information sharing process for threat and intelligence information</p>		
<p>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.</p>		
<p style="writing-mode: vertical-rl; transform: rotate(180deg);"><b>ESTABLISH A RISK ASSESSMENT AND INFORMATION SHARING PROCESS</b></p>	<p><b>9.101</b> 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?</p>	<p><a href="#">Homeland Security Information Network</a> <a href="#">Surface Transportation and Public Transportation Information Sharing and Analysis Center</a>  <a href="#">Infragard Website</a></p>
	<p><b>Standard:</b> 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 <u>and</u> Federal law enforcement.</p>	
	<p><b>9.102</b> Does the agency report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?</p>	
	<p><b>Standard:</b> The agency reports threat/intel information <u>directly</u> to the JTTF or regional anti-terrorism task force.</p>	
	<p><b>9.103</b> Does the agency have policies requiring employees to report (internal or external) suspicious activity to their supervisor or management?</p>	
<p><b>Standard:</b> The agency has detailed policies and protocols in place to report suspicious activity Internally and externally</p>		

	<p><b>9.104</b> 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)?</p>	<p><b><u>TSOC – Freedom Center</u></b>                  POC: TSOC Surface Watch Officer                  Telephone: 1-866-615-5150                  E-Mail: <a href="mailto:TSOC.St.@dhs.gov">TSOC.St.@dhs.gov</a></p>
<p><b>Standard:</b> 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 "time" element (immediately, within "X" hours, etc.).</p>		<p><b><u>Homeland Security Information Network</u></b>   <b><u>Surface Transportation and Public Transportation Information Sharing and Analysis Center</u></b></p>
	<p><b>9.105</b> 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.</p>	
<p><b>Standard:</b> The agency receives threat/intel information <i>at least once per week</i>.</p>		
	<p><b>9.106</b> Does the agency report their NTD security data to FTA as required by 49 CFR 659?</p>	
<p><b>Standard:</b> The agency reports NTD security data to FTA.</p>		
<p><b>10.000</b></p>	<p><b>Conduct Tabletop and Functional Drills</b></p>	
<p>The purpose of this section is 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.</p>		
<p><b>DRILLS AND EXERCISES</b></p>	<p><b>10.101</b> 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?</p>	<p><b><u>FTA System Security and Emergency Preparedness Program Plan Template</u></b></p>

<p><b>Standard:</b> The agency has developed a <i>detailed</i> process of developing an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills. This is documented in the System Safety Program Plan (SSPP) or another document that is referenced in the SSPP.</p>	<p><a href="#"><u>APTA – Transit Incident Drills and Exercises</u></a></p>
<p><b>10.102</b> Does the agency’s SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?</p>	<p><a href="#"><u>FTA Emergency Preparedness/ Emergency Management</u></a></p>
<p><b>Standard:</b> 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 or SSP.</p>	
<p><b>10.103</b> Does the agency evaluate its emergency preparedness by using annual field exercises, tabletop exercises, and/or drills? If so, please summarize the exercise events held in the past year.</p>	<p><a href="#"><u>DHS FEMA IS-130 Exercise Evaluation training course</u></a></p> <p><a href="#"><u>FEMA Emergency Planning Exercises</u></a></p>
<p><b>Standard:</b> The agency conducts drills and exercises <i>annually</i> with the purpose of <i>evaluating</i> its emergency preparedness procedures.</p>	
<p><b>10.104</b> Does the agency's SPP or a related document include a requirement for annual field exercises, tabletops and drills?</p>	
<p><b>Standard:</b> The agency has a <i>documented requirement</i> for drills/exercises to be conducted <i>once per year</i> at a minimum.</p>	

<b>DRILLS AND EXERCISES</b>	<b>10.105</b>	<b>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)</b>	<a href="#"><u>FTA Emergency Preparedness/ Emergency Management</u></a> <a href="#"><u>Homeland Security Exercise and Evaluation Program (HSEEP)</u></a> <a href="#"><u>Safety and Security Oversight Program</u></a>
	<b>Standard:</b> The process of drill/exercise evaluation is described and documented in the SSPP, SSP, or another document that is referenced by the SSPP/SSP.		
	<b>10.106</b>	<b>Does the agency’s SPP or a related document describe or reference its program for providing employee training on emergency response protocols and procedures?</b>	
	<b>Standard:</b> The program for providing employee training on emergency response protocols and procedures is <u>documented</u> .		
	<b>10.107</b>	<b>Does the agency participate as an active player in full-scale, regional exercises, held at least annually?</b>	<a href="#"><u>FEMA State Offices and Agencies of Emergency Management</u></a>
	<b>Standard:</b> The agency participates as an <u>active player</u> in full-scale, regional exercises held <u>at least annually</u> .		
<b>10.108</b>	<b>In the last year, has the agency conducted drills or exercises specifically focus on Active Shooter scenarios with its employees?</b>	<a href="#"><u>Active Shooter Pocket Card</u></a>  <a href="#"><u>Active Shooter Preparedness</u></a>	
<b>Standard:</b> In the last year, the agency has conducted its own drills and/or exercises specific to Active Shooter with <u>all</u> their employees.			

<p><b>10.109</b></p>	<p><b>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)?</b></p>	
<p><b>Standard:</b> In the last year, the agency has been involved in drills/exercises that specifically focus on IEDs <b><i>and</i></b> WMD with appropriate external entities, to include first responders <b><i>and</i></b> other transit agencies that operate in the same environment.</p>		
<p><b>10.110</b></p>	<p><b>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?</b></p>	
<p><b>Standard:</b> <i>In the last year</i>, the agency has reviewed and prepared after-action reports (or other evaluating report) for all drills and exercises. All evaluations are documented.</p>		<p><a href="#"><u>APTA – Transit Incident Drills and Exercises</u></a></p>
<p><b>10.111</b></p>	<p><b>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.</b></p>	
<p><b>Standard:</b> <i>In the last year</i>, the agency has updated plans, protocols, or processes to incorporate after-action report recommendations/findings.</p>		
<p><b>10.112</b></p>	<p><b>Has the agency established a system for objectively measure and assess its performance during emergency exercises and to measure improvements?</b></p>	

	<p><b>Standard:</b> The agency has developed a formal, objective system of evaluating drill performance. The agency has identified evaluation <u>criteria</u>, establishes drill/exercise <u>goals</u>, and analyzes the results appropriately. This system is documented.</p>	
10.113	<p><b>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)</b></p>	<p><a href="#"><u>APTA – Transit Incident Drills and Exercises</u></a></p>
	<p><b>Standard:</b> The agency conducts exercises of its security <u>and</u> emergency response plans to test operational capabilities of employees <u>and</u> first responders in underwater/underground infrastructure and other critical systems.</p>	
10.114	<p><b>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 too place?</b></p>	
	<p><b>Standard:</b> The agency actively reaches out to external emergency agencies (local and regional) when planning <u>and</u> conducting exercises. The agency integrates <u>all</u> appropriate entities: fire, medical, <u>and</u> law enforcement.</p>	
11.000	<p><b>Developing a Comprehensive Cyber Security Strategy</b></p>	
	<p><b>The purpose of this section is to enhance agency security awareness and preparedness to identify and protect against cyber security threats to the system.</b></p>	
CY BE R	11.101	<p><b>Has the agency conducted a risk assessment to identify operational control and</b></p>

	<p><b>communication/business enterprise IT assets and potential vulnerabilities?</b></p>	<p><a href="#"><u>APTA - Securing Control and Communications Systems (Sign in to APTA’s website or close login screen and document will open)</u></a></p>
<p><b>Standard:</b> The agency has conducted a risk assessment focused on IT systems as they relate to operational control, communication, and business enterprise. The assessment is documented and addresses threats, vulnerabilities, and consequences.</p>		
<p><b>11.102</b></p>	<p><b>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?</b></p>	<p><a href="#"><u>FEMA 452- Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks</u></a></p> <p><a href="#"><u>Control Systems Security Program (CSSP)</u></a></p>
<p><b>Standard:</b> 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.</p>		<p><a href="#"><u>ICS-CERT Recommended Practices</u></a></p> <p><a href="#"><u>Industrial Control System Cyber Emergency Response Team</u></a></p>
<p><b>11.103</b></p>	<p><b>Has a written strategy been developed and integrated into the overall security program to mitigate the cyber risk identified?</b></p>	<p><a href="#"><u>NIST – Guide to Intrusion Detection and Prevention Systems</u></a></p>
<p><b>Standard:</b> 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).</p>		
<p><b>11.104</b></p>	<p><b>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</b></p>	<p><a href="#"><u>DHS/CERT Password Security, Protection &amp; Management</u></a></p>

	<p><b>infrastructure (example: firewalls, intrusion detection systems, IT security audits, antivirus, etc.)?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>11.105</b></p>	<p><b>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?</b></p>	<p><a href="#">Cyber Security Training &amp; Exercises</a></p>
<p><b>Standard:</b> 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).</p>		
<p><b>11.106</b></p>	<p><b>Has the agency established a cyber-incident response and reporting protocol?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>11.107</b></p>	<p><b>Is the agency aware of and using available resources (e.g., standards, PT-ISAC, US CERT, National Cyber Security Communication and Integration Center, etc.)?</b></p>	<p><a href="#">APTA PT- ISAC (Sign in to APTA's website or close login screen and document will open)</a></p> <p><a href="http://transitwireless.org/">http://transitwireless.org/</a></p> <p><a href="#">National Cyber Security Communication and Integration Center</a></p>
<p><b>Standard:</b> The agency is aware of and makes use of available resources.</p>		

<b>12.000 Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors.</b>			
<p>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.</p>			
<b>FACILITY SECURITY AND ACCESS CONTROLS</b>	<b>12.101</b>	<b>Have assets and facilities requiring restricted access been identified?</b>	<p><a href="#"><u>FTA Transit Security Design Considerations - 5.0 Access Management</u></a></p>
	<p><b>Standard:</b> Restricted areas are identified and documented. Agency personnel are familiar with their location and restricted status.</p>		
	<b>12.102</b>	<b>Are ID badges or other measures employed to restrict access to facilities not open to the public?</b>	
	<p><b>Standard:</b> 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.</p>		
	<b>12.103</b>	<b>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.)?</b>	
	<p><b>Standard:</b> 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.</p>		
	<b>12.104</b>	<b>Does the agency have documented procedures for issuing ID badges to visitors and contractors?</b>	
	<p><b>Standard:</b> The agency has documented procedures in place to issue ID badges for visitors and contractors. These procedures are implemented perfectly.</p>		

12.105	<b>Does the agency has a documented policy that requires visitors to be escorted when accessing non-public areas.</b>	
<b>Standard:</b> The agency has a documented policy that requires visitors to be escorted when accessing non-public areas. This policy is implemented <i>perfectly</i> .		
12.106	<b>Is CCTV equipment installed in transit agency facilities?</b>	
<b>Standard:</b> Effective and capable CCTV systems are installed at all facilities.		
12.107	<b>Is CCTV equipment protecting critical assets interfaced with an access control system?</b>	
<b>Standard:</b> CCTV equipment protecting critical assets are completely integrated with other access control measures (door breach triggers automated CCTV functions, etc.).		<a href="#"><u>APTA - Crime Prevention Through Environmental Design</u></a>
12.108	<b>Is CCTV equipment installed on transit vehicles?</b>	
<b>Standard:</b> Effective and capable CCTV systems are installed on a vast majority of vehicle fleet.		
12.209	<b>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?</b>	
<b>Standard:</b> CPTED is incorporated in the design of <i>all</i> projects. CPTED-related vulnerabilities are identified and corrected promptly using technological solutions or other solutions.		
12.110	<b>Does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?</b>	<a href="#"><u>APTA - Fencing Systems to Control Access to Transit Facilities (Sign in to APTA’s website or close login screen and document will open)</u></a>
<b>Standard:</b> The agency has installed physical barriers or intrusion detection systems to prevent unauthorized access		

FACILITY SECURITY AND ACCESS CONTROLS	at <i>all</i> appropriate stations, facilities, and critical infrastructure.		<a href="#">APTA - Chain Link, Mesh, or Woven Metal Fencing (Sign in to APTA’s website or close login screen and document will open)</a>  <a href="#">APTA - Gates to Control Access (Sign in to APTA’s website or close login screen and document will open)</a>  <a href="#">APTA - Ornamental Fencing (Sign in to APTA’s website or close login screen and document will open)</a>
	12.111	Has the system implemented protective measures to secure high risk/high consequence assets and critical systems? (i.e., CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems)	<a href="#">FTA - Transit Security Design Considerations - 6.3 Security Approaches for Types of Transit Infrastructure</a>
	<b>Standard:</b> The agency has identified high risk/high consequence assets and has implemented additional security measures for <i>all</i> such assets. Additional measures are documented.		
	12.112	Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?	<a href="#">DHS If-You-See-Something-Say-Something-Campaign</a>
	<b>Standard:</b> 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.		
	12.113	Does the agency provide a method for passengers and visitors to report security and safety concerns from within the agency's system?	
<b>Standard:</b> Call boxes are <i>consistently</i> installed throughout the agency’s system; specifically in stations, terminals,			

<p>appropriate facilities and all conveyances. Call boxes are fully functional.</p>	
<p><b>12.114</b> Does the transit agency administer an automated employee access control system and perform corrective analysis of security breaches?</p>	
<p><b>Standard:</b> The agency uses an automated access control system <i>and</i> 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.</p>	
<p><b>12.115</b> Does the agency have policies and procedures for screening of mail and/or outside deliveries?</p>	<p><a href="#"><u>APTA - Safe Mail and Package Handling</u></a></p>
<p><b>Standard:</b> The agency has documented policies and specific, well-developed procedures that address the screening of mail or outside deliveries. Procedures are completely implemented.</p>	
<p><b>12.116</b> Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?</p>	
<p><b>Standard:</b> The agency uses <i>multiple</i> methods of breach prevention (locks, anti-frag materials, bullet resistant materials, etc.) at all critical locations.</p>	
<p><b>12.117</b> 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)</p>	<p><a href="#"><u>National Fire Protection Association (NFPA) Standard List of Codes and Standards</u></a></p>

FACILITY SECURITY AND ACCESS CONTROLS	<b>Standard:</b> NFPA 130 or equivalent is used in station design or modification criteria. Access Control systems do not interfere with safety or emergency operations.		
	12.118	<b>Is directional signage with adequate lighting provided in a consistent manner throughout their system, both to provide orientation and to support emergency evacuation?</b>	<a href="#"><u>APTA - Security Lighting for Transit Passenger Facilities (Sign in to APTA’s website or close login screen and document will open)</u></a>
	<b>Standard:</b> Directional signage and lighting is consistent throughout the system and is installed in a manner that supports security, safety, and emergency operations.		
	12.119	<b>Are gates and locks used on all facility doors to prevent unauthorized access during operating hours?</b>	<a href="#"><u>APTA - Fencing Systems to Control Access to Transit Facilities (Sign in to APTA’s website or close login screen and document will open)</u></a>
	<b>Standard:</b> The agency uses gates and locks to prevent unauthorized access at <u>all</u> facilities. Policies and procedures are in place to effectively utilize locks and gates.		<a href="#"><u>APTA - Chain Link, Mesh, or Woven Metal Fencing (Sign in to APTA’s website or close login screen and document will open)</u></a>
	12.120	<b>Are keys controlled through an established program that is documented?</b>	<a href="#"><u>APTA - Gates to Control Access (Sign in to APTA’s website or close login screen and document will open)</u></a>
	<b>Standard:</b> The agency has a documented key control program that specifically assigns management responsibility to a specific individual or department.		<a href="#"><u>APTA - Ornamental Fencing (Sign in to APTA’s website or close login screen and document will open)</u></a>
	12.121	<b>Are gates and locks used to close down system facilities after operating hours?</b>	
	<b>Standard:</b> Gates and locks are used at <u>all</u> facilities that are closed down. Policies and procedures are in place to effectively utilize locks and gates.		
12.122	<b>Do transit vehicles have radios, silent alarms, and/or passenger communication systems?</b>		

		<b>Standard:</b> <u>All</u> transit vehicles are equipped with radios, silent alarms, and/or passenger communication systems. Policies and procedures are in place to effectively utilize these measures.
12.123	<b>Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?</b>	
		<b>Standard:</b> Graffiti-resistant/etch-resistant materials are used at all (or a vast majority of) facilities.
12.124	<b>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.?</b>	
		<b>Standard:</b> Uninterruptible Power Supplies are provided for <u>all</u> safety- and security-critical equipment.
12.125	<b>Has the agency removed non-explosive resistant trash receptacles from platform areas of terminals and stations?</b>	
		<b>Standard:</b> The agency has removed non-explosive resistant trash receptacles from platform areas of terminals and stations.
12.126	<b>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?</b>	
		<a href="#"><u>National Infrastructure Protection Plan (NIPP), DHS, 2013</u></a>
		<a href="#"><u>APTA - Operational Strategies for Emergency Smoke Ventilation in Tunnels</u></a>

<b>FACILITY SECURITY AND ACCESS CONTROLS</b>	<b>Standard:</b> 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	<b>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?</b>	
	<b>Standard:</b> 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.		
<b>13.000</b>	<b>Conduct Physical Security Inspections</b>		
<b>FACILITY SECURITY AND ACCESS CONTROLS</b>	<b>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.</b>		
	13.101	<b>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.</b>	<a href="#"><u>TSA/FTA – Conduct Physical Security Inspections</u></a> <a href="#"><u>APTA - Identifying Suspicious Behavior in Mass Transit (Sign in to APTA’s website or close login screen and document will open)</u></a>
	<b>Standard:</b> 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	<b>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?</b>	<a href="#"><u>APTA - Recognizing and Responding to Unattended Packages, Objects and Baggage (Sign in to APTA’s website or close login screen and document will open)</u></a>	

<b>Standard:</b> <i>Documented</i> security procedures reflect HOT characteristics.		
<b>13.103</b>	<b>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?</b>	<a href="#"><u>APTA - Conducting Revenue Vehicle Security Inspections (Sign in to APTA's website or close login screen and document will open)</u></a>
<b>Standard:</b> 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.		<a href="#"><u>APTA - Conducting Nonrevenue Vehicle Security Inspections (Sign in to APTA's website or close login screen and document will open)</u></a>
<b>13.104</b>	<b>Has the transit agency developed a form or quick reference guide for station attendants and others regarding station and facility inspections?</b>	
<b>Standard:</b> The agency utilizes a checklist or other widely distributed document that specifically addresses security to assist personnel conducting station/facility inspections.		
<b>13.105</b>	<b>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.</b>	
<b>Standard:</b> Inspection results are documented <i>and</i> 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.		
<b>13.106</b>	<b>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?</b>	

	<p><b>Standard:</b> 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.</p>	
<p>13.107</p>	<p><b>Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect?</b></p>	<p><a href="#"><u>APTA - Random Counterterrorism Measures on Transit Systems (Sign in to APTA's website or close login screen and document will open)</u></a></p>
	<p><b>Standard:</b> Security activities are conducted at random times and at random intervals and these procedures are documented.</p>	
<p>13.108</p>	<p><b>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.</b></p>	
	<p><b>Standard:</b> The agency has documented policies and procedures in place to ensure that <i>all</i> in-service vehicles are inspected at multiple times per day for suspicious or unattended items. Personnel receive training to properly conduct these inspections.</p>	
<p>13.109</p>	<p><b>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.</b></p>	
	<p><b>Standard:</b> 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>	

<b>14.000 Conduct Background Investigations of Employees and Contractors</b>																
<b>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.</b>																
<b>BACKGROUND INVESTIGATIONS</b>	<table border="1"> <tr> <td style="background-color: #d9e1f2;"><b>14.101</b></td> <td><b>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)</b></td> </tr> <tr> <td colspan="2" style="background-color: #d9e1f2;"><b>Standard:</b> 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.</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>14.102</b></td> <td><b>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?</b></td> </tr> <tr> <td colspan="2" style="background-color: #d9e1f2;"><b>Standard:</b> The agency (a) conducts an appropriate level of background check on relevant contract employees <i><b>or</b></i> (b) the agency builds appropriate background check criteria into the bid process <i><b>and</b></i> has established a method of verifying/auditing background checks.</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>14.103</b></td> <td><b>Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?</b></td> </tr> <tr> <td colspan="2" style="background-color: #d9e1f2;"><b>Standard:</b> The agency's process for conducting background investigations has been reviewed by a legal professional.</td> </tr> <tr> <td style="background-color: #d9e1f2;"><b>14.104</b></td> <td><b>Does the agency have a documented process for conducting background investigations?</b></td> </tr> </table>	<b>14.101</b>	<b>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)</b>	<b>Standard:</b> 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.		<b>14.102</b>	<b>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?</b>	<b>Standard:</b> The agency (a) conducts an appropriate level of background check on relevant contract employees <i><b>or</b></i> (b) the agency builds appropriate background check criteria into the bid process <i><b>and</b></i> has established a method of verifying/auditing background checks.		<b>14.103</b>	<b>Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?</b>	<b>Standard:</b> The agency's process for conducting background investigations has been reviewed by a legal professional.		<b>14.104</b>	<b>Does the agency have a documented process for conducting background investigations?</b>	<p><a href="#"><u>APTA - Conducting Background Investigations (Sign in to APTA's website or close login screen and document will open)</u></a></p> <p><a href="#"><u>ASIS International – Pre-employment Background Screening</u></a></p>
	<b>14.101</b>	<b>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)</b>														
	<b>Standard:</b> 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.															
	<b>14.102</b>	<b>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?</b>														
	<b>Standard:</b> The agency (a) conducts an appropriate level of background check on relevant contract employees <i><b>or</b></i> (b) the agency builds appropriate background check criteria into the bid process <i><b>and</b></i> has established a method of verifying/auditing background checks.															
	<b>14.103</b>	<b>Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?</b>														
	<b>Standard:</b> The agency's process for conducting background investigations has been reviewed by a legal professional.															
<b>14.104</b>	<b>Does the agency have a documented process for conducting background investigations?</b>															

	<p><b>Standard:</b> The process for conducting background checks is documented. This includes the following: the method/type of background check utilized, positions that require background checks, who is responsible for conducting the investigation, and other factors of consideration (such as policies restricting the commencement of employment until after the investigation is complete).</p>	
	<p><b>14.105</b> Is the criteria for background investigations based on employee type and responsibility, and is access documented?</p>	
	<p><b>Standard:</b> Background screening criteria (disqualifying conditions) are based on job-function, required level of access, and/or responsibility. Criteria covers all functions that may require a background check. This is documented.</p>	
<b>15.000</b>	<b>Control Access to documents of security critical systems and facilities</b>	
	<p>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.</p>	
<b>DOCUMENT CONTROL</b>	<p><b>15.101</b> 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?</p>	
	<p><b>Standard:</b> The agency has well-developed document control procedures that protect security-critical documentation from unauthorized access. All documents are appropriately protected: plans, schematics, etc.</p>	
	<p><b>15.102</b> Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?</p>	

	<p><b>Standard:</b> A person or department has been formally tasked with administering the access control policy with respect to agency documents.</p>	
	<p><b>15.103</b> Does the security review committee or other designated group review document control practices, assess compliance applicable procedures, and identify discrepancies and necessary corrective action?</p>	
	<p><b>Standard:</b> A security review committee actively reviews document control practices, assess compliance-applicable procedures, and identifies discrepancies and corrective action regularly.</p>	
<b>16.000</b>	<b>Process for handling and access to Sensitive Security Information (SSI)</b>	
	<p>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.</p>	
<b>DOCUMENT CONTROL</b>	<p><b>16.101</b> 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?</p>	<p><a href="#">FTA - Sensitive Security Information (SSI)</a></p> <p><a href="#">TCRP - RECONCILING SECURITY, DISCLOSURE, AND RECORD-RETENTION REQUIREMENTS IN TRANSIT PROCUREMENTS</a></p>
	<p><b>Standard:</b> 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.</p>	
	<p><b>16.102</b> Does the agency have a documented policy for proper handling, control, and storage of documents labeled as or otherwise</p>	

	<p><b>determined to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>16.103</b></p>	<p><b>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?</b></p>	
<p><b>Standard:</b> 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.</p>		
<p><b>16.104</b></p>	<p><b>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)?</b></p>	
<p><b>Standard:</b> The agency has established official SSI training (with appropriate materials), and based on a sampling of frontline personnel interviews, all</p>		

	employees who may be provided access to SSI have been provided the training.	
<b>17.000</b>	<b>Audit Program</b>	
<p><b>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.</b></p>		
<b>17.101</b>	<b>Has the agency established a schedule for conducting its internal security audit process?</b>	<p><a href="#"><u>APTA - Security Planning for Public Transit</u></a></p> <p><a href="#"><u>FTA – Recommended Best Practices for States Conducting Three-Year Safety Reviews</u></a></p> <p><a href="#"><u>FTA - The Public Transportation System Security and Emergency Preparedness Planning Guide</u></a></p> <p><a href="#"><u>APTA - Random Counterterrorism Measures on Transit Systems (Sign in to APTA’s website or close login screen and document will open)</u></a></p> <p><a href="#"><u>APTA - Security Program Considerations for Public Transit</u></a></p>
<p><b>Standard:</b> The agency has a documented schedule for conducting internal security audits in an ongoing manner over a three-year period.</p>		
<b>17.102</b>	<b>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?</b>	
<p><b>Standard:</b> 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.</p>		
<b>17.103</b>	<b>Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process?</b>	
<p><b>Standard:</b> The agency has well-developed procedures for conducting internal security audits and uses checklists/forms to properly and consistently conduct audits.</p>		
<b>17.104</b>	<b>Is the transit agency complying with its internal security audit schedule?</b>	

SECURITY PROGRAM AUDITS

<p><b>Standard:</b> The agency is conducting internal security audits in a manner that reflects its established schedule.</p>	
<p><b>17.105</b></p>	<p><b>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?</b></p>
<p><b>Standard:</b> 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.</p>	
<p><b>17.106</b></p>	<p><b>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?</b></p>
<p><b>Standard:</b> In the last 12 months, the Security Review Committee has reviewed audit reports, addressed findings, and updated plans and protocols as necessary.</p>	
<p><b>17.107</b></p>	<p><b>Does the transit agency’s internal security audit process ensure that auditors are independent from those responsible for the activity being audited?</b></p>
<p><b>Standard:</b> Auditors are independent from the individuals they are tasked with auditing to prevent any conflicts of interest.</p>	
<p><b>17.108</b></p>	<p><b>Has the agency made its internal security audit schedule available to the SSO agency?</b></p>

	<b>Standard:</b> The agency has made its internal security audit schedule available to the SSO agency.	
	<b>17.109</b> Has the agency made checklists and procedures used in its internal security audits available to the SSO agency?	
<b>SECURITY PROGRAM AUDITS</b>	<b>Standard:</b> The agency has made checklists and procedures used in its internal security audits available to the SSO agency.	
	<b>17.110</b> Has the agency notified the SSO agency 30 days prior to the conduct of an internal security audit?	
	<b>Standard:</b> The agency has notified the SSO agency 30 days prior to the conduct of an internal security audit.	
	<b>17.111</b> Has a report documenting internal security audit process and the status of findings and corrective actions been made available to the SSO agency within the previous 12 months?	
	<b>Standard:</b> A report documenting internal security audit process and the status of findings and corrective actions have been made available to the SSO agency within the previous 12 months.	
	<b>17.112</b> Has the agency's chief executive certified to the SSO agency that the agency is in compliance with its SSP?	
	<b>Standard:</b> The agency's chief executive has certified to the SSO agency that the agency is in compliance with its SSP.	

<b>17.113</b>	<b>Was that certification included with the most recent annual report submitted to the SSO agency?</b>	
<b>Standard:</b> The previously mentioned certification was included with the most recent annual report submitted to the SSO agency.		
<b>17.114</b>	<b>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?</b>	
<b>Standard:</b> A corrective action plan was developed and made available to the SSO.		

<b>ADDITIONAL RESOURCES</b>		
<b>ADDITIONAL RESOURCES</b>	Lessons Learned Information Sharing ( <i>LLIS.gov</i> ) 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. <i>LLIS.gov</i> 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.	<a href="https://emilms.fema.gov/IS0921a/CIPP0104280text1.htm">https://emilms.fema.gov/IS0921a/CIPP0104280text1.htm</a>
	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	<a href="http://www.apta.com/resources/Pages/Default.aspx">http://www.apta.com/resources/Pages/Default.aspx</a> <a href="http://www.apta.com/resources/standards/Pages/default.aspx">http://www.apta.com/resources/standards/Pages/default.aspx</a>

<p><b>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.</b></p>	<p><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></p>
<p><b>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.</b></p>	<p><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>

**DOCUMENT LIST**

## DOCUMENT LIST

APTA	Anti-Vehicle Barriers for Public Transit, APTA-SS-SIS-RP-009-12, 2012
APTA	Chain Link, Mesh, or Woven Fencing Systems to Control Access, APTA-SS-SIS-RP004-10, 2010
APTA	Crime Prevention through Environmental Design (CPTED), APTA-SS-SIS-RP-00710, 2010
APTA	Developing a Contagious Virus Response Plan, APTA-SS-SEM-S-005-09, 2009
APTA	Emergency Communication Strategies for Transit Agencies, APTA-SS-SEM-RP-00909, 2009
APTA	Fencing Systems to Control Access, APTA-SS-SIS-RP-003-10, 2010
APTA	Gates to Control Access, APTA-SS-SIS-RP-005-10, 2010
APTA	Ornamental Fencing Systems to Control Access, APTA-SS-SIS-RP-006-10, 2010
APTA	Physical Security for Public Transit, APTA-SS-SIS-RP-013-13, 2013
APTA	Random Counterterrorism Measures on Transit Systems, APTA-SS-SRM-RP-00611, 2011
APTA	Recognizing and Responding to Unattended Packages, Objects and Baggage, APTASS-SRM-RP-007-12,
APTA	Recommended Practice Conducting Nonrevenue Vehicle Security Inspections, APTASS-SRM-RP-003-009,
APTA	Recommended Practice Conducting Revenue Vehicle Security Inspections, APTA-SSSRM-RP-012-09, 2009
APTA	Recommended Practice Creating an Alternate or Backup OCC, APTA-SS-SEM-RP007-09, 2009
APTA	Recommended Practice for Conducting Background Investigations, APTA-SS-SRM-RP-004-11, 2011
APTA	Recommended Practice for First Responder Familiarization of Transit Systems, APTA-SS-SEM-RP-002-08, 2008
APTA	Recommended Practice for Participating in Mutual Aid, APTA-SS-SEM-RP-011-09,
APTA	Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP), APTA-SS-SRM-RP-001-09, Rev. 1, 2012
APTA	Recommended Practice Identifying Suspicious Behavior in Mass Transit, APTA-SSSRM-RP-009-09, 2009
APTA	Safe Mail and Package Handling, APTA-SS-SEM-RP-008-09, 2009
APTA	Securing Control and Communications Systems in Rail Transit Environments Part 2, APTA-SS-CCS-RP-002-13, 2013
APTA	Securing Control and Communications Systems in Transit Environments, Part 1: Elements, Organization and Risk Assessment/Management, APTA-SS-CCS-RP-001-10, 2010
APTA	Security Awareness Training for Transit Employees, APTA-SS-SRM-RP-005-12, 2012
APTA	Security Considerations for Public Transit, APTA-SS-SIS-S-010-13, 2013
APTA	Security Lighting for Nonrevenue Transit Facilities, APTA-SS-SIS-RP-002-10, 2010
APTA	Security Lighting for Revenue Transit Facilities, APTA-SS-SIS-RP-001-10, 2010
APTA	Security Operations for Public Transit, APTA-SS-SIS-RP-012-13, 2013
APTA	Security Planning for Public Transit, APTA-SS-SIS-RP-011-13, 2013
APTA	Shelter of Transit Vehicles and Nonrevenue Equipment During Emergencies, APTASS-SEM-S-006-09, 2009
APTA	Standard for a Continuity of Operations Plan, APTA-SS-SEM-S-001-08, 2008
APTA	Standard for Security & Emergency Management Aspects of Special Events Service
APTA	Transit Incident Drills and Exercises, APTA-SS-SEM-S-004-9, 2009
APTA	White Paper on Random Inspections of Carry-on Items in Transit Systems, APTASS- SRM-WP-002-10, 2010
APTA	Operational Strategies for Emergency Smoke Ventilation in Tunnels, APTA-SS-SEM-WP-013-10, 2010

**DOCUMENT LIST**

DHS	Homeland Security Exercise and Evaluation Program (HSEEP), Volume 1: HSEEP Overview and Exercise Program Management, DHS, 2007
DHS	National Disaster Recovery Framework (NDRF), DHS, 2011
DHS	National Incident Management System, DHS, 2008
DHS	National Infrastructure Protection Plan (NIPP), DHS, 2013
DHS	National Response Framework (NRF), DHS, 2013
DHS	National Terrorism Advisory System Public Guide, DHS, 2011
DHS	Risk Management Fundamentals, Homeland Security Risk Management Doctrine, DHS, 2011
DHS	Roadmap to Secure Control Systems in the Transportation Sector, DHS, 2012
DHS	See Something, Say Something, NYCTMA, endorsed by DHS
DHS	Threat and Hazard Identification and Risk Assessment Guide, (CPG) 201, First Edition, DHS, 2012
FEM/	Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (CPG) 101, Version 2.0, FEMA, 2010
FEM/	Risk Assessment, A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, FEMA 452, 2005
FTA	An Introduction to All-hazards Preparedness for Transit Agencies, FTA, 2010
FTA	Bus Safety and Security Program, Safety, Security, and Emergency Preparedness Excellence – A Roadmap, FTA, 2012
FTA	Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel Systems, FTA,
FTA	Handbook for Transit Safety and Security Certification, FTA, 2000
FTA	Immediate Actions for Transit Employees: Protecting Against Life-Threatening Emergencies, A Resource Document for Transit Agencies, FTA, 2011
FTA	National Transit Database (NTD), Safety and Security Reporting Manual, FTA, 2013
FTA	Response and Recovery for Declared Emergencies and Disasters, A Resource Document for Transit Agencies
FTA	Sensitive Security Information (SSI): Designation, Markings, and Control, Resource Document for Transit
FTA	The Public Transportation System Security and Emergency Preparedness Planning Guide, FTA, 2003
FTA	Transit Security Design Considerations, FTA, 2004
FTA	Transit Watch, FTA
NIST	NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers, NIST, 2006
NIST	NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, NIST, 2012
NIST	NIST Special Publication 800-64, Revision 2, Security Considerations in the System Development Life Cycle
NIST	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
NIST	NIST Special Publication 800-94, Revision 1 (Draft), Guide to Intrusion Detection and Prevention Systems

DOCUMENT LIST

<b>DOCUMENT LIST</b>	
<b>DOCUMENT LIST</b>	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/NCHRP, 2009
	TRB TCRP Report 160, Paratransit Emergency Preparedness and Operations Handbook, TRB/TCRP, 2013
	TRB TCRP Report 86, Volume 12, Making Transportation Tunnels Safe and Secure, TRB/TCRP, 2006
	TRB TCRP Report 86, Volume 4, Intrusion Detection for Public Transportation Facilities Handbook, TRB/TCRP
	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. 10-02, Security Guidelines for Vessels, USCG, 2002
	USCG Navigation and Vessel Inspection Circular (NVIC) No. 11-02, Recommended Security Guidelines for Facilities USCG, 2003

## Appendix A - FY16 BASE Changes

