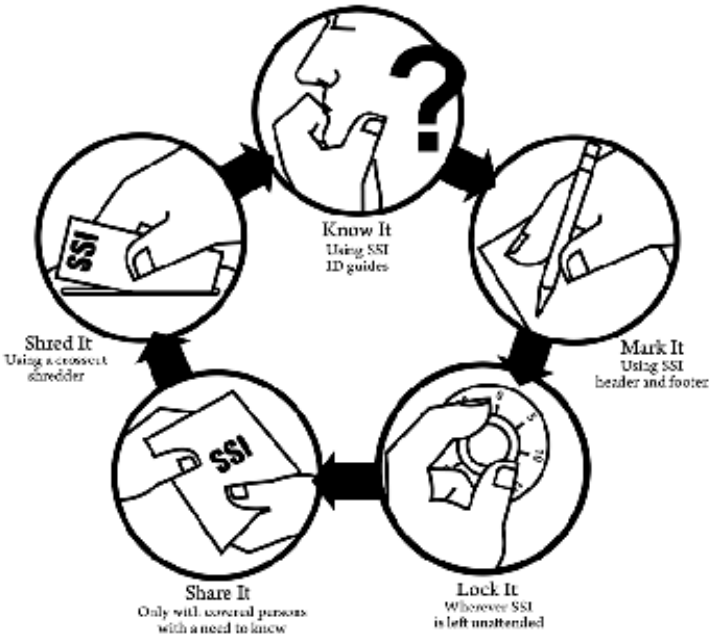
DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet



For more information on handling SSI, contact SSI@dhs.gov.

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

DHS Form 11054 (8/10) Reference: 49 CFR § 1520.13, Marking SSI

M

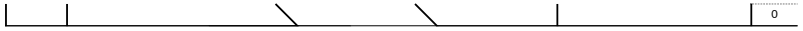
As gener
“0” Security eleme
“1” Security element exists, but doe
“2” Security element is in place with all essential c
“3” Security element is in place and practiced but
“4” Security element is in place, fully implemented and regularl
“N/A” Checked - Securi

Line Element		SIDoT	Comments	Items of Interest	
	Establish Wr				
1.101	Does the transit agency have a System Security Plan (SSP)? Document Review		Inspectors should refer to the MT BASE Guidance, Pg12.	Policies and procedures related to *security*--including personnel security, vehicle security, facility security, and threat/vulnerability management.	4 3 2 1 0
1.102	Does the SSP identify the goals and objectives for the security program? Document Review			Documented method of effectively assessing and monitoring security program's purpose and progress.	4 2 1 0
1.103	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, including the agency's chief executive? Document Review		Justification should include at least two management and implementation statements	Policy statement including: endorsement statement/signature, applicability, and authority/background of the plan.	4 2 1 0
1.104	Is the SSP separate from the agency's System Safety Program Plan (SSPP)? Document Review			"Yes" or "No."	4 0
1.105 T1	Do the Security and Emergency Response Plans address protection and response for critical underwater tunnels, underground stations/ tunnels and other critical systems, where applicable? Document Review		In addition to underwater tunnels, underground stations/ tunnels, this question also applies to other critical systems.	Review SSP to determine if items are address effectively.	4 2 0
1.106	Does the SSP contain or reference other documents establishing procedures for the management of security incidents by the operations control center (or dispatch center)? Document Review			Operation Control Center: managing incidents	4 3 2 1 0
1.107	Does the SSP contain or reference other documents establishing plans, procedures, or protocols for responding to security events with external agencies (such as law enforcement, local EMA, fire departments, etc.)? Document Review		In Justification, describe plans, procedures or protocols.	Documented plans for coordinating with external agencies.	4 2 0
1.108	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)? Document Review			Protocols for IED ***and*** WMD	4 2 0

1.109 T3	Are visible, random security measures integrated into security plans to introduce unpredictability into security activities for deterrent effect? Document Review		Agency should strive to implement and document their own unpredictable security measures using their own resources.	Random or unpredictable security measures that are documented in security plans.	4 2 1 0
1.110	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? Document Review			Project/procurement planning, engineering, design, construction, and testing.	4 3 2 1 0
1.111	Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices? Document Review			Project design, engineering, and construction.	4 3 2 1 0
1.112	Does the SSP require an annual review? Document Review		Reference date of last review in justification.	Annual review ***requirement. A review is focused on written policy and ensuring policies are sufficient.***	4 2 1 0
1.113	Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives? Document Review			An example of periodic reports reviewing SSP progress	4 3 2 1 0
1.114	Has an annual review of the SSP been performed and documented in the preceding 12 months? Document Review			Documented evidence of a annual review. A review is focused on written *policy* and ensuring policies are sufficient.	4 2 0
1.115	Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP? Document Review		49 CFR PART 659 SSO Only Question	"Yes" or "No." Documented process for SSO approval. N/A for entities not regulated under 49 CFR § 659.	4 0
1.116	Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect? Document Review		49 CFR PART 659 SSO Only Question If yes, indicate the approval date in evidence.	Current SSP has been approved by SSO. N/A for entities not regulated under 49 CFR § 659.	4 2 0

1.201	Does the transit agency have an Emergency Response Plan (ERP)? Document Review	Inspectors should refer to the MT BASE Guidance, Pg13.	Emergency response procedures	4 3 2 1 0
1.202	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, including the agency's chief executive? Document Review		Policy statement including: endorsement statement/signature, applicability, and authority/background of the plan.	4 3 2 1 0
1.203	Does the ERP require an annual review to determine if it needs to be updated? Document Review		Documented requirement for annual review.	4 2 1 0
1.204	Has an annual review of the ERP been performed and documented in the preceding 12 months? Document Review	Reference date of last review in justification.	Documented evidence of a annual review.	4 2 0
1.205	Does the ERP include a process or review provision to ensure coordination with the rail transit agency's SSPP and SSMP? Document Review		Emergency response procedures coordinated with security and safety procedures. (Emergency procedures do not hinder safety or security.)	4 3 2 1 0
1.206	Has the transit agency received documentation from the SSO confirming its review and approval of the ERP currently in effect? SSO Review	49 CFR PART 659 SSO Only Question	SSO approval of current ERP. N/A for entities not regulated under 49 CFR § 659.	4 2 0
1.207	Does the ERP contain or reference other documents establishing plans, procedures, or protocols for responding to emergency events with external agencies (such as law enforcement, local EMA, fire departments, etc.)? Document Review		Documented plans for coordinating with external agencies.	4 2 0
1.208	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)? Document Review		Management of emergency events	4 3 2 1 0

1.209	Does the ERP contain or reference other documents to provide for Continuity of Operations while responding to emergency events? Document Review	Verify COOP addresses 5 main goals outlined in the MT BASE Guidance, Pg13.	Continuity of Operations plan.	4 2 0
1.210	Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event? Document Review		Procedures to recover from an event and resume normal operations.	4 3 2 1 0
1.211	Does the agency have a written Business Continuity Plan and COOP to guide restoration of facilities and services following an emergency event? Document Review		Procedures to continue essential operations during emergency.	4 3 2 1 0
1.212	Does the agency have a back-up operations control center capability? Document Review	indicate last time this was tested (if applicable) in Justification.	Secondary site of Operations Control.	4 2 0
				Define
2.101	Does the SSP establish and assign responsibility for implementation of the security program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer? Document Review	Inspectors should refer to the MT BASE Guidance, Pg14.	Documented evidence assigning implementation of security program in the SSP.	4 3 2 1 0
2.102	Has the agency established lines of delegated authority/succession of security responsibilities and, if so, has that information been distributed to agency managers? Document Review		Chain of Command ***and*** Lines of Succession for security responsibilities.	4 3 2 1 0
2.103	Are roles and responsibilities for security and/or law enforcement personnel assigned by title and/or position established in the SSP or other documents? Document Review		Security roles and responsibilities of Security Personnel.	4 3 2 1 0
2.104	Are security-related roles and responsibilities for non-security and/or law enforcement personnel (i.e., operators, conductors, maintenance workers and station attendants) established in the SSP or other documents? Document Review		Security roles and responsibilities of non-security personnel.	4 3 2 1 0
2.105 TSF 2	Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes? Interview / Document Review	Security should be the primary focus of these meetings and briefings	Management meetings for security recommendations. Operational.	4 2 0
2.106	Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings? Interview	Security should be the primary focus of these meetings and briefings	Security Review Committee	4 3 2 1


0

2.107	Are informational briefings with appropriate personnel held whenever security protocols, threat levels, or protective measures are updated or as security conditions warrant?	Document Review / Interview	Security Briefings (written or verbal), means of acknowledgement. Operational.	4 3 2 1 0
2.108	Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the SSP?	Document Review / Interview	Reference guides for transit personnel	4 3 2 1 0
2.109	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?	Document Review / Interview	This question applies to both Regulated and Non-Regulated entities.	Security Coordinator	4 2 0
2.110	Does the agency maintain a record of security related incidents that are reported within the agency?	Document Review		Incident recording (may be document retention or summary archives)	4 3 2 1 0
2.201	Does the ERP 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?	Document Review / Interview	Inspectors should refer to the MT BASE Guidance, Pg14.	Documented evidence assigning implementation of security program in the ERP.	4 3 2 1 0
2.202	Are emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?	Document Review / Interview		Documented emergency response responsibilities.	4 3 2 1 0
2.203 TSF 5	Are roles and responsibilities for front-line personnel (i.e. system law enforcement, system security officials, trainer, vehicle operators, conductors, station attendants, maintenance workers) described in the system's Emergency Response Plan (ERP)?	Document Review / Interview		Frontline Personnel Responsibilities.	4 3 2 1 0
2.204	Has the ERP been distributed to appropriate departments in the organization?	Interview		ERP Distribution	4 3 2 1 0
2.205	Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the ERP?	Document Review / Interview		Reference guides for transit personnel	4 3 2 1 0
2.206	Are senior staff and middle management ERP coordination meetings held on a regular	Document Review / Interview	Emergency response should be the primary focus of these	Management meetings for ERP coordination. Operational.	4 3 2

	basis?	meetings and briefings		1 0
2.207	Are informational briefings with appropriate personnel held whenever emergency response protocols are substantially changed or updated?	Document Review Interview	Briefings related to emergency response. Operational.	4 3 2 1 0
Ensure that operations and maintenanc				
3.101	Do managers and supervisors routinely provide information to front-line personnel regarding security and emergency response issues?	Interview front-line personnel Document Review Observation/ Verification	Inspectors should refer to the MT BASE Guidance, Pg16.	Frontline Personnel Briefings	4 3 2 1 0
3.102	Are regular supervisor, manager, and/or foreperson security review and coordination briefings held? If so, detail frequency and subjects covered in the justification.	Interview		Supervisor Briefings	4 3 2 1 0
3.103	Does the agency have a program for confirming that personnel have a working knowledge of security protocols? If so, summarize program in the justification.	Interview Document Review	Possible follow-up questions needed. Summarize program in justification.	Internal verification of knowledge	4 3 2 1 0
3.104	Are managers and/or supervisors required to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?	Interview Document Review		Debriefing Requirement	4 3 2 1 0
Coordinate Se				
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?	Interview Document Review	Inspectors should refer to the MT BASE Guidance, Pg16.	MOUs involving law enforcement, other transit agencies, and first responders	4 3 2 1 0
4.102	Does the agency participate in a regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and response?	Interview		Regional Emergency Management Group. "Yes" or "No."	4 0
4.103	Have regional incident management protocols been shared with the agency and incorporated into the agency's ERP/SSP/SEPP?	Document Review Interview		Regional Incident Management Protocols	4 3 2 1 0
4.104	Have agency resources been appropriately identified and provided to the regional Emerg...	Interview		Agency Resources. "Yes" or "No."	4 0

4.105	Does the agency have a designated point of contact or liaison with the local/regional Emergency Operations Center (EOC)?	Interview / Document Review	POC identified from EOC. "Yes" or "No."	4 0
4.106	Does the agency send a representative to the local/regional EOC, should it be activated?	Interview / Review / Assessment	Agency Representative sent to EOC. "Yes" or "No."	4 2 0
4.107	Does the agency have information sharing capabilities with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?	Interview / Document Review	Information Sharing Capabilities	4 2 1 0
4.108	Has the agency developed internal incident management protocols that comply with the National Response Plan and the National Incident Management System (NIMS)?	Document Review / Interview / Verification	Internal Incident Management Protocols. "Yes" or "No."	4 0
4.109	Have the agency's emergency response protocols been shared with the EMS and appropriate first responder agencies?	Interview	Internal Emergency Response Protocols. "Yes" or "No."	4 2 0
4.110 TSF 5	Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?	Review / Interview	Interoperability	4 3 2 1 0
4.111	If the agency's communications systems are NOT inter-operable with appropriate emergency response agencies, have alternate communication protocols been established? Describe the alternate communication protocols in the justification.	Interview / Document Review	Interoperability Substitute	4 2 0
				Est
5.101 TSF 4	Is initial training provided to all new agency employees regarding security orientation/awareness?	Document Review / Verification / Interview / Frontline	Training records, training material Inspectors should refer to the MT BASE Guidance, Pg18.	4 2 0
5.102 TSF 4	Is annual refresher training provided regarding security orientation/awareness to Senior Management staff, managers and supervisors?	Interview / Review / Assessment	Training records, training material	4 2 0
5.103 TSF 4	Is annual refresher training provided regarding security orientation/awareness to managers and supervisors?	Interview / Review / Document	Training records, training material	4 2 0
5.104 TSF 4	Is annual refresher training provided regarding security orientation/awareness to front-line employees?	Document Review / Frontline / Verification	Training records, training material	4 2 0
5.105	Is ongoing advanced security training focused on job function provided at least annually?	Interview / Frontline / Verification	Training records, training material	4 2 0

5.106 TSF 4	Is initial training provided to all new transit employees regarding emergency response?	Interview / Verification / Frontline	General emergency response / awareness training	Training records, training material	4 2 0
5.107	Is annual refresher training provided regarding emergency response to Senior Management staff, supervisors, and managers?	Interview / Review / Document		Training records, training material	4 2 0
5.108 TSF 4	Is annual refresher training provided regarding emergency response to Managers and Supervisors?	Interview / Review / Document		Training records, training material	4 2 0
5.109 TSF 4	Is annual refresher training provided regarding emergency response to front-line Employees?	Interview / Verification / Frontline		Training records, training material	4 2 0
5.110 TSF 4	Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System at least annually?	Interview / Verification / Frontline		Training records, training material	4 2 0
5.111	Has ICS and NIMS training appropriate to the position been provided to Senior Management staff, supervisors, and managers at least annually?	Interview / Review / Document		Training records, training material	4 2 0
5.112	Has ICS and NIMS training appropriate to the position been provided to managers and supervisors at least annually?	Interview / Review / Document		Training records, training material	4 2 0
5.113	Has ICS and NIMS training appropriate to the position been provided to front-line employees at least annually?	Interview / Verification / Frontline		Training records, training material	4 2 0
5.114	Has the agency developed a program and provided annual training on its own incident response protocols?	Document Review / Interview		Training records, training material	4 2 0
5.115 TSF 4	Has training on the agency's incident response protocols appropriate to the position been provided to Senior Management staff, managers and supervisors at least annually?	Interview / Document Review		Training records, training material	4 2 0
5.116 TSF 4	Has training on the agency's incident response protocols appropriate to the position been provided to managers and supervisors?	Interview / Review / Document		Training records, training material	4 2 0
5.117 TSF 4	Has training on the agency's incident response protocols appropriate to the position been provided to front-line employees at least annually?	Interview / Verification / Frontline / Document Review /		Training records, training material	4 2 0
5.118 TSF 4	Has the transit system implemented an annual training program for personnel regarding response to terrorism, including (1) Improvised Explosive Devices and (2) Weapons of Mass Destruction (chemical, biological, radiological, nuclear)? If so, summarize the relevant programs in the justification?	Document Review / Interview		Training records, training material	4 2 0

5.119	Has training focused on IEDs and WMDs appropriate to the position been provided to Senior Management staff, managers, and supervisors at least annually?	Document Review / Interview		Training records, training material	4 2 0
5.120	Has training focused on IEDs and WMDs appropriate to the position been provided to manager and supervisors?	Document Review / Interview		Training records, training material	4 2 0
5.121	Has training focused on IEDs and WMDs appropriate to the position been provided to front-line employees at least annually?	Document Review / Interview / Observation		Training records, training material	4 2 0
5.122	Do law enforcement/security department personnel at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.	Document Review / Interview	in justification, provide description of specialized training or provider.	Training records, training material	4 2 0
5.123	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.	Document Review / Interview	in justification, provide description of specialized training or provider.	Training records, training material	4 2 0
5.124	Does the agency have an established program to monitor employee training and to schedule employees for training?	Document Review	General training review. This does not have to revolve around Security Training but establishes if they have an active system.	Training Scheduling (General)	4 2 0
5.125	Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?	Document Review	This question asks specifically about security-related courses.	Training Recording (Security) (ex. 30-day file)	4 2 0
5.126	Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?	Document Review	This question asks specifically about emergency response related courses.	Training Recording (Emergency Response) (ex. 30-day file)	4 2 0
5.127	Does the agency have a program to regularly review and update security awareness and emergency response training materials?	Interview / Review of Document		Security Review and Updating	4 2 0
5.128 TSF 4	Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat conditions, protective measures or the employee watch programs?	Document Review / Interview		Operational Changes	4 3 2 1 0

5.129 TSF 1	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.	Document Review		Response and recovery operations in critical facilities and infrastructure.	4 2 0
5.130 TSF1	Has the agency provided training to regional first responders (law enforcement agencies, firefighters, and emergency medical response teams) to enable them to operate in critical facilities and infrastructure?	Document Review	During interview, dates or frequency of training should be documented to receive full score. Also, describe scope of training.	Training program for external agencies.	4 2 0
5.131 TSF 3	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?	Interview Reference Document Review		Training program featuring concepts of random and highly visible countermeasures.	4 2 0
5.132 TSF 4	Has the agency implemented a program to train or orient first responders (law enforcement, firefighters, emergency medical teams) and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?	Interview Reference Document Review	During interview, dates or frequency of training should be documented to receive full score. Also, describe scope of training.	Training program for external agencies.	4 2 0
Establish plans a					
6.101	Does the SSP contain or reference other documents identifying incremental actions (imminent or elevated) to be implemented for a NTAS threat?	Document Review	Inspectors should refer to the MT BASE Guidance, Pg19.	Incremental actions based on NTAS threat	4 2 0
6.102 TSF 2	Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?	Document Review		Response protocols for specific threat scenarios based on NTAS	4 2 0
6.103	Has the agency provided annual training and/or instruction focused on job function regarding the incremental activities to be performed by employees?	Interview Document Review		Job-specific NTAS training	4 2 1 0

					Implement
7.101	Has the transit agency developed and implemented a public security and emergency awareness program?	Interview, Document Review	Inspectors should refer to the MT BASE Guidance, P20. In justification, provide description of agency's emergency awareness program.	Outreach program	4 3 2 1 0
7.102 TSF 6	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)?	Document Review, Observation		Active outreach, utilizes program materials	4 2 0
7.103 TSF 6	Is the above consistent with agency's overall announcement program?	Document Review / Observation		Appropriate outreach material. "Yes" or "no."	4 0
7.104 TSF 6	Are general security awareness and emergency preparedness messages included in public announcement messages at stations and on board vehicles?	Observation		Public announcements (Pre-recorded voice announcements)	4 3 2 1 0
7.105 TSF 6	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.	Document Review, Observation		Materials specifically mention reporting unattended property, suspicious behavior and security concerns.	4 2 0
7.106 TSF 6	Does the agency have an appropriate mechanism in place for passengers to communicate an (e.g., 1-800 number, smart phone applications, social media, etc.) that can be called or used to report security concerns? If so, is this information indicated in public awareness materials and messages?	Document Review, Observation		Effective reporting mechanism	4 2 0
7.107	Does the agency issue public service announcements or press releases to social media (e.g. Twitter/ Facebook, etc., QRC codes, and/or apps for smart phones) regarding security and emergency protocols?	Interview, Observation, Document Review	In justification, provide description of social media utilized.	**Social Media** Announcements for Security and Emergency. "Yes" or "No."	4 0
7.108 TSF 6	Does the agency issue public service announcements or press releases to local media (e.g. newspaper, radio and/or television) regarding security or emergency protocols?	Interview, Observation, Document Review	In Justification, describe the most recent public announcement or press release to local media.	**Local Media** Announcements for Emergency Response. "Yes" or "No."	4 0
7.109	Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response?	Interview, Observation, Document Review		Training for non-employee volunteers for emergency response	4 2 0
7.110	Does the transit agency conduct an outreach program to enlist members of the public as security awareness volunteers, similar to Neighborhood Watch programs?	Interview, Document Review		Active volunteer program (not the same as "See Something, Say Something")	4 2 0

7.111 TSF 1	Do public awareness materials and/or messages inform passengers of the means to evacuate safely from transit vehicles and underwater/underground facilities?	Interview / Observation / Document Review	If agency has no underwater/underground facilities question applies to transit vehicles.	Passenger evacuation guidance material	4 2 0
7.112	Does the agency track and monitor customer complaints reported by passengers?	Interview		Customer complaint tracking system	4 2 0
Establish and use a Risk M					
8.101 TSF 2	Does the agency have a risk assessment process approved by its management for managing threats and vulnerabilities? If so, summarize the process in the justification.	Document Review / Interview	Inspectors should refer to the MT BASE Guidance, Pg20.	Process of Risk Assessment	4 2 0
8.102	Has the agency identified facilities and systems it considers to be its critical assets?	Interview / Review / Document	In Justification, describe the critical assets identified by the agency.	Identification of Critical Assets	4 2 0
8.103 TSF 2	Has the agency had an internal or external vulnerability assessment on its critical assets within the past 3 years? Specify the dates of the most recent assessments and the entity(ies) that conducted the assessment(s).	Interview / Document Review	Scoring Justification should list at a minimum: date of assessment, identify critical assets, who conducted the assessment, etc.	Date of last vulnerability assessment (General). "Yes" or "no."	4 2 0
8.104 TSF 1	Has the agency had an internal or external Risk Assessment, analyzing threat, vulnerability, & 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?	Interview / Document Review	Scoring Justification should list at a minimum: date of assessment, identify critical assets, who conducted the assessment, etc.	Recent Risk Assessment (specifically ***threat***, ***vulnerability***, and ***consequence*** analyzed), appropriate personnel trained.	4 2 0
8.105 TSF 2	Has the system implemented procedures to limit and monitor authorized access to underground and underwater tunnels? If so, summarize procedures in the justification.	Interview / Observation / Document Review		Access to underground and underwater tunnels. N/A if the system does not have underground/underwater tunnels.	4 2 0
8.106	Are security investments prioritized using information developed in the risk assessment process?	Interview	In justification, examples of improvements based off of risk assessment results should be provided.	Security Investments, examples of security investment prioritization	4 2 0
8.107 TSF 1	Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and related documents?	Document Review / Observation		Inspector was able to review ***all*** requested documents, including assessments and Security Plans. "Yes" or "no."	4 0
Establish and					
9.101	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?	Document Review / Interview	Inspectors should refer to the MT BASE Guidance, Pg22.	Formalized process of intelligence sharing with Federal, State, and local law enforcement agencies.	4 2 0
9.102 TSF 2	Does the system report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?	Document Review / Interview / Observation		Reporting ***directly*** to JTTF or regional anti-terrorism body. "Yes" or "no."	4 0
9.103 TSF2	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)?	Document Review / Interview	This question applies to both Regulated and Non-Regulated entities.	Reporting threats and significant security concerns to TSOC ***and*** local law enforcement.	4 2 1 0

9.104	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?	Document Review		Documented evidence of intel receiving (Daily Report, etc.).	4 3 2 1 0
9.105	Does the agency report their NTA security data to FTA as required by 49 CFR 659?	Interview	49 CFR PART 659 SSO Only Question	NTA Security Data (***regulation***)	4 0
10.101	Does the agency's System Safety Program Plan (SSPP) contain or reference a document describing the process used by the agency to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills?	Document Review, Observation	Inspectors should refer to the MT BASE Guidance, P22. In Justification, describe agencies approved coordinated schedule for all emergency management program activities	Process for developing/ coordinating/ scheduling emergency management activities.	4 2 0
10.102	Does the agency's SSPP or SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?	Document Review		Emergency planning responsibilities and drills/exercises general requirements	4 2 0
10.103 TSF 5	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.	Document Review	Agency driven	Agency conducting functional drills and exercises. "Yes" or "no."	4 0
10.104	Does the agency's SSPP or a related document include a requirement for annual field exercises, tabletops and drills?	Document Review		Annual Requirement. "Yes" or "no."	4 0
10.105	Does the agency's SSPP 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)?	Document Review		Results of drills/ exercises/ evaluations, documentation of results. "Yes" or "no."	4 0
10.106	Does the agency's SSPP or a related document describe or reference its program for providing employee training on emergency response protocols and procedures?	Document Review		Documented training. "Yes" or "no."	4 0
10.107	Does the agency participate as an active player in full-scale, regional exercises held at least annually?	Interview	Region driven	Active-player participation. "Yes" or "no."	4 0
10.108 TSF 5	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)?	Document Review, Observation	In Justification, describe the drill/exercise and include date.	Drills: Specific Focus. Participants: other transit agencies, first responders.	4 2 0
10.109 TSF 5	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?	Interview, Document Review		Evaluation of results	4 2 0

10.110 TSF 5	In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings and corrective actions? If so, summarize the actions taken in the justification. Interview / Document Review		In Justification, summarize the actions taken in the justification.	Evaluation of results, plan modifications. "Yes" or "no."	4 0
10.111	Has the agency established metrics to assess its performance during emergency exercises and to measure improvements? Interview / Review / Document			Method of analysis	4 2 0
10.112 TSF 1	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 in underwater/underground infrastructure and other critical systems? Interview / Document Review		In addition to underwater/underground infrastructure, this question applies to other critical systems as identified by the entity.	Drills in underwater/underground infrastructure and other critical systems.	4 2 0
10.113 TSF 5	Does the transit system integrate local and regional first responders (law enforcement, firefighters, emergency medical teams) in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place. Document Review		In justification, summarize each joint event and state when it took place.	Drills with external agencies	4 2 0
11.101	Has the agency conducted a risk assessment to identify operational control and communication/business enterprise IT assets and potential vulnerabilities? Document Review / Interview		Inspectors should refer to the MT BASE Guidance, Pg24.	Risk assessment focused on ***IT SECURITY***	4 2 0
11.102	Has the agency implemented protocols to ensure that all IT facilities (e.g., data center, server rooms, etc.) and equipment are properly secured to guard against internal or external threats or attacks? Document Review / Interview			Security measures for critical IT facilities/equipment	4 2 0
11.103	Has a written strategy been developed and integrated into the overall security program to mitigate the cyber risk identified? Document Review			Written IT security measures	4 2 0

11.104	Does the agency have a designated representative to secure the internal network through appropriate access controls for employees, a strong authentication (i.e., password) policy, encrypting sensitive data, and employing network security infrastructure (example: firewalls, intrusion detection systems, IT security audits, antivirus, etc.)?	Review of Policy		IT Security Coordinator	4 3 2 1 0
11.105	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?	Review of Policy		Recurrent cybersecurity training	4 2 0
11.106	Has the agency established a cyber-incident response and reporting protocol?	Document review / Interview		Cyber-incident response and reporting protocols	4 2 0
11.107	Is the agency aware of and using available resources (e.g., standards, MT-ISAC, US CERT, National Cyber Security Communication and Integration Center, etc.)?	Review of Policy	In Justification, describe resources used by agency.	Available resources. "Yes" or "no."	4 0
12.101	Have assets and facilities requiring restricted access been identified?	Interview / Review of Document	Inspectors should refer to the MT BASE Guidance, Pg26.	Restricted Areas	4 2 0
12.102	Are ID badges or other measures employed to restrict access to facilities not open to the public?	Frontline Interview / Observation		ID Badges	4 2 0
12.103 TSF 2	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.)?	Review of Policy		Access Control Monitoring/Updating	4 2 0
12.104	Does the agency have procedures to issue ID badges for visitors and contractors?	Interview / Frontline Observation		ID Badges for contractors and visitors	4 2 0
12.105	Does the agency require escorts for visitors accessing non-public areas?	Interview		Escorts Policy	4 2 0
12.106	Is CCTV equipment installed in transit agency facilities?	Interview / Observation / Frontline		CCTV: Facilities	4 2 0
12.107	Is CCTV equipment protecting critical assets interfaced with an access control system?	Interview		CCTV: Access Control	4 2 0
12.108	Is CCTV equipment installed on transit vehicles?	Interview		CCTV: Vehicles	4 2 0
12.109	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?	Interview		CPTED; Design/Engineering Representative interview	4 2 0

12.110	Based on the risk assessment, does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?	Document review	Physical barriers	4 2 0
12.111 TSF 2	Has the system implemented protective measures to secure high risk/high consequence assets and systems identified in risk assessments? Examples of protective measures include but are not limited to, CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems. If protective measures for this infrastructure are employed, summarize type and location in the justification.	Document review	Additional measures for high-risk assets	4 2 0
12.112	Does the transit agency monitor a network of security, fire, duress, intrusion, facility and internal 911 alarm systems?	Document review	Alarm monitoring	4 3 2 1 0
12.113	Are emergency call boxes provided to passengers?	Physical Observation / Interview	Call boxes	4 2 0
12.114	Do transit agency personnel administer an automated employee access control system and perform corrective analysis of security breaches?	Document review	Automated Access Control (employee-controlled badge/keycard entry)	4 3 2 1 0
12.115	Does the agency have policies and procedures for screening of mail and/or outside deliveries?	Document review	Mail screening	4 2 1 0
12.116	Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?	Document review	Breach preparedness at critical location	4 2 0
12.117	Does the agency use National Fire Protection Association (NFPA) Standard 130 or equivalent to evaluate fire/life safety in station design or modification (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)?	Document review	Access Control does not interfere with Safety or Emergency Operations. "Yes" or "no."	4 0
12.118	Is directional signage with adequate lighting provided in a consistent manner in all stations, both to provide orientation and to support emergency evacuation?	Physical Observation	Lighting	4 2 0
12.119	Are gates and locks used on all facility doors to prevent unauthorized access?	Interview / Observation / Physical	Methods of restricting access	4 2 0

12.120	Are keys controlled through an established program managed by the security/police function?	Key control program	4 2 0
12.121	Are gates and locks also used to close down system facilities after operating hours?	Methods of securing facilities	4 2 0
12.122	Do transit vehicles have radios, silent alarms, and/or passenger communication systems?	Means of communication	4 2 0
12.123	Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?	"Broken Windows Theory"	4 2 1 0
12.124	Are Uninterruptible Power Supply (UPS) or redundant power sources provided for safety and security of critical equipment, such as but not limited to: exit and platform lighting; parking lot lighting; ancillary space and shop lighting; intrusion detection (alarmed rooms and spaces, fare collection equipment, etc.); fire detection, alarm and suppression systems; public address (shop and public areas); call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?	Back-up power for critical safety and security equipment	4 3 2 1 0
12.125	At passenger stations at which a vulnerability assessment has identified a significant risk, and to the extent practicable, has the owner/operator removed trash receptacles and other non-essential receptacles or containers (with the exception of bomb resistant receptacles or clear plastic containers) from the platform areas of passenger terminals and stations?	Trash receptacles	4 0
12.126	Does the agency employ specific protective measures for all critical infrastructure (e.g. tunnels, bridges, stations, control centers, etc) identified through the risk assessment particularly at access points and ventilation infrastructure in place and maintained in optimal condition? Examples of protective measures include, but are not limited to, CCTV, intrusion detection systems, smart camera technology, fencing, lighting, access control, law enforcement patrols, canine patrols, physical protection for ventilation systems. If protective measures for this infrastructure are employed, summarize type and location in the justification.	Protective Measures for Critical Infrastructure	4 2 0
12.127 TSF 1	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available from other law enforcement agencies? If so, has the system implemented procedures for reporting of and response to positive reactions by the canine?	Explosive detection canine unit, Mutual Aid Agreements	4 2 0

13.101 TSF 1	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?	Document Review, Observation, Interview	Inspectors should refer to the MT BASE Guidance, Pg29.	Critical asset inspections (General)	4 2 0
13.102	Has the transit agency established procedures for inspecting/sweeping vehicles and stations to identify and manage suspicious items, based on HOT characteristics (hidden, obviously suspicious, not typical) or equivalent system?	Document Review, Observation, Interview, Verification	In justification, provide results of interview with Front Line employees.	Inspection procedures reflect "HOT" characteristics. "Yes" or "no."	4 0
13.103	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?	Document Review, Observation		Vehicle inspection checklist. "Yes" or "no."	4 0
13.104	Has the transit agency developed a form or quick reference guide for station attendants and others regarding station and facility inspections?	Document Review, Observation		Facility inspection checklist. "Yes" or "no."	4 0
13.105 TSF 2	Does the system document the results of inspections and implement any changes to policies and procedures or implement corrective actions, based on the findings?	Document Review, Observation, Interview		Inspection results	4 2 0
13.106 TSF 2	Does the agency conduct frequent inspections of access points, ventilation systems, and the interior of underground/underwater assets and systems for indications of suspicious activity?	Document Review, Observation, Interview		Inspections of non-normal areas. N/A if the system has no underground/underwater tunnels.	4 2 0
13.107	Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect?	Interview, Document Review	Agency should strive to implement and document their own unpredictable security measures using their own resources.	Randomness and unpredictability as it relates to inspections. "Yes" or "no."	4 0
13.108	Is there a process in place, with necessary training provided to personnel, to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.	Document Review, Observation, Interview	In justification, specify type and frequency of inspections.	Security Inspections: Vehicles	4 2 0
13.109	Is there a process in place, with necessary training provided to personnel, to ensure that all critical infrastructure are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.	Document Review, Observation, Interview	In justification, specify type and frequency of inspections.	Security Inspections: Critical Infrastructure	4 2 0

14.101 TSF 2	Does the agency conduct background investigations (i.e., criminal history and motor vehicle records) on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems?	Document Review	Inspectors should refer to the MT BASE Guidance, Pg30.	Background checks, HR Representative interview	4 2 0
14.102 TSF 2	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?	Document Review		Background checks, HR Representative interview	4 2 0
14.103	Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?	Document Review		Background checks, HR Representative interview	4 0
14.104	Is the background investigation process documented?	Document Review		Background check process, HR Representative interview	4 2 0
14.105	Is the criteria for background investigations based on employee type (senior management staff, law enforcement officers, managers/supervisors, operators, maintenance, safety/security sensitive, contractor, etc.) and/or responsibility and access documented?	Document Review		Background check process, HR Representative interview	4 2 0
					Con
15.101 TSF 2	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?	Document Review	Inspectors should refer to the MT BASE Guidance, Pg31.	Security-critical documentation, Engineering Representative interview	4 2 0
15.102	Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?	Document Review		Document control authority. "Yes" or "no"	4 0
15.103	Does the security review committee (or other designated group) review document control practices, assess compliance applicable procedures, and identify discrepancies and necessary corrective action?	Document Review		Document control policy monitoring	4 2 0

				Proc
16.101	Does the agency have a documented policy for identifying and controlling the distribution of and access to documents it considers to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520?	Document Review	Inspectors should refer to the MT BASE Guidance, Pg32.	Documented SSI Policy	4 2 0
16.102	Does the agency have a documented policy for proper handling, control, and storage of documents labeled as or otherwise determined to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520?	Document Review		Documented SSI Policy	4 2 0
16.103	Are employees who may be provided SSI materials per 49 CFR Part 15 or 1520) familiar with the documented policies for the proper handling of such materials?	Employee Interview		Employee familiarization (requires frontline interviews)	4 2 0
16.104	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)?	Employee Interview		SSI Training development ***and*** implementation (requires frontline interviews)	4 2 0
17.101	Has the agency established a schedule for conducting its internal security audit process?	Document Review	Inspectors should refer to the MT BASE Guidance, Pg32.	Established Schedule Internal Security Audit (self-assessment). An audit is focused on *practices* identified in the SSP and ensuring these policies are implemented and followed effectively.	4 2 0
17.102	Does the SSP contain a description of the process used by the agency to audit its implementation of the SSP over the course of the agency's published schedule?	Document Review	In justification, provide description of process.	Process Description: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively.	4 2 0
17.103	Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process?	Document Review		Checklists: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively.	4 2 0
17.104	Is the transit agency complying with its internal security audit schedule?	Interview / Document Review		Implementation: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively. "Yes" or "no."	4 0
17.105	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?	Document Review		Documentation: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively.	4 2 0
17.106	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?	Document Review		Peer Review: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively.	4 2 0

17.107	Does the transit agency's internal security audit process ensure that auditors are independent from those responsible for the activity being audited?	Internal Review		Independent Auditors: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively. "Yes" or "no."	4 0
17.108	Has the agency made its internal security audit schedule available to the SSO agency?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively. "Yes" or "no."	4 0
17.109	Has the agency made checklists and procedures used in its internal security audits available to the SSO agency?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively. "Yes" or "no."	4 0
17.110	Has the agency notified the SSO agency 30 days prior to the conduct of an internal security audit?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4 0
17.111	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?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4 0
17.112	Has the agency's chief executive certified to the SSO agency that the agency is in compliance with its SSP?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4 0
17.113	Was that certification included with the most recent annual report submitted to the SSO agency?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4 0
17.114	If the agency's chief executive was not able to certify to the SSO agency that the agency is in compliance with its SSP, was a corrective action plan developed and made available to the SSO?	Internal Review	49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4 0

ass Transit BASE Scoring Guidance - Appendix IX

al guidance , scores are to be assigned on a scale of 0-4 as follows:
nt should be in place but does not exist. (Equates to total non-adherence – 0%)
s not include all essential recommended components. (Equates to minimal adherence – 25-50%)
omponents but not fully implemented or practiced. (Equates to partial adherence or implementation – 50-75%)
t not monitored or periodically reviewed. (Equates to strong adherence, but not full implementation – 75-99%)
ly reviewed/verified. (Equates to full implementation – 100%) Also assigned to "yes/no" question having a "Yes" response.
ity element is not applicable and rational must be given to support the N/A rating.

Scoring Example
itten System Security Plans (SSPs) and Emergency Response Plans (ERPs)
System Security Plan (SSP)
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.
SSP is a complete document with polices and procedures that have been appropriately implemented by the agency. Only a few minor security elements are missing. Key concepts are detailed with minimal exceptions.
Generic policies and procedures are documented and implemented adequately. Key concepts are documented, but lacking any depth. In fact, the plan simply appears to be a commonly available "template."
SSP is a generalized document that is lacking any detailed, agency-specific security elements. Key concepts are missing or not adequately implemented by the agency.
There is no SSP in place.
Goals and objectives are identified, documented and actively monitored to ensure the SSP is fulfilling its purpose.
Goals and objectives are identified and documented, but not monitored. Items may be missing or ineffective.
Goals and objectives are minimal, lacking any specifics or depth. These items do not effectively assess and monitor the SSP's purpose and progress, respectively.
The SSP does not address goals or objectives of the security program.
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.
Policy statement a brief endorsement statement by chief executive and a signature.
Policy statement only includes a brief endorsement statement. No endorsement signature.
There is no policy statement of any sort in place.
SSP is a stand-alone document, separate from the System Safety Plan.
System Security Plan is part of another document. (Note: In the past, railroads/agencies would incorporate the Security Plan into the Safety Plan - using the APTA SSPP template, element 17: Security)
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.
Security plans address policies and procedures with varying degrees of implementation.
Security plans do not address items.
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.
Plans and procedures are in place and function appropriately. However, minor aspects are missing. SSP includes--or references documents that contain--the procedures.
Well organized procedures are in place and contained as part of another document with no reference in the SSP.
Procedures are lacking any depth or clarity, plans are scattered between multiple documents with no reference in SSP, or responsibilities are otherwise ineffectively assigned.
Procedures are not in place or documented.
Well-developed, ***specific*** procedures are in place and documented in the SSP ***or*** as part of another document and referenced in the SSP.
Procedures are in place with varying degrees of implementation or documentation.
Procedures are not in place or documented.
Well-developed, ***specific*** protocols are in place that address IED ***and*** WMD. These protocols are documented in the SSP ***or*** as part of another document, such as a stand-alone Emergency Response Plan, and referenced in the SSP.
Protocols are developed with varying degrees of implementation or documentation.
Protocols have not been developed.

Random, unpredictable measures are well-documented with specific measures assigned by employee-type. Includes both security and non-security personnel.
Random, unpredictable measures are documented. Measures are simply general guidance lacking specifics.
The agency relies on outside entities to provide random, unpredictable measures. Agency only participates in VIPR or other similar outreach. Participation in program is documented in the SSP.
Random, visible measures are not documented in the SSP.
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.
Security plays a role in all new projects and procurements and is part of the safety certification process. 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. This is required by the agency and documented in the agency's Safety plan--not the SSP.
Specific security concerns are considered for all new projects, but implementation is an informal process and not required (recommended as opposed to required). Process is documented.
Security is addressed on an informal basis with only general security guidance considered. Process is documented.
There is no documented evidence in place that suggest security is addressed with new projects or procurements.
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).
CPTED principles are addressed and implemented in a majority of facilities. This is documented in the SSP or other documents (which are referenced in the SSP). Vulnerabilities have been identified.
CPTED principles are addressed with minimal implementation. Principles are documented in the SSP or other documents (which are referenced in the SSP).
CPTED adoption is merely a general acknowledgement contained in the SSP or other document (that is referenced in the SSP).
CPTED is not adopted by the agency.
Annual review is a written requirement with verification measures in place (signed and dated)
Annual review is a "commonly known" requirement (not documented) or a written requirement with no verification measure in place.
SSP is reviewed on an "as-needed" basis, but at least every two years.
There are no review requirements in place, and the SSP is not regularly reviewed.
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.
Periodic reports are detailed and developed once in a two-year cycle ***OR*** periodic reports are developed once per year but are lacking in detail.
Informal reports are developed on an "as-needed" basis.
Reports are not documented, per se, but the agency does have an informal, verbal system in place to monitor the agency's progress in fulfilling its goals and objectives.
The agency does not monitor its progress in any way.
Annual review is verifiable by document review.
Annual review is only verifiable by interview.
SSP has not been reviewed.
Documented process for securing SSO review and approval of SSP is included in writing, or directly referenced, in the SSP.
Documented process does not exist.
Approval (including date of approved) is verifiable through document review.
SSP has been submitted to the SSO agency, but approval is pending.
SSP has not been approved.

Emergency Response Plan (ERP)
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.
ERP is a complete document with polices and procedures that have been appropriately implemented by the agency. Only a few minor elements are missing. Key concepts are detailed with minimal exceptions.
Generic policies and procedures are documented and implemented adequately. Key concepts are documented, but lacking any depth. In fact, the plan simply appears to be a commonly available "template."
ERP is a generalized document that is lacking any detailed, agency-specific security elements. Key concepts are missing or not adequately implemented by the agency.
There is no ERP in place.
Policy statement is well developed and includes all elements: endorsement statement, applicability, authority establishing the plan, and approval signature from the agencies chief executive.
Includes a brief endorsement statement by chief executive and a signature.
Policy statement only includes an endorsement signature.
Policy statement only includes a brief endorsement statement. No endorsement signature.
There is no policy statement of any sort in place.
Annual review is a written requirement with verification measures in place (signed and dated).
Annual review is a "commonly known" requirement (not documented) or a written requirement with no verification measure in place.
ERP is reviewed on an "as-needed" basis, but at least every two years.
There are no review requirements in place, and the ERP is not regularly reviewed.
Annual review is verifiable by document review.
Annual review is only verifiable by interview.
ERP has not been reviewed.
ERP includes documented provisions that ensure its coordination with the agency's safety and security plans.
ERP includes documented provisions that ensure its coordination with either the agency's security plans or the agency's safety plans--not both.
Provisions are in place and clearly implemented, but no documentation established.
Coordination is very informal with no specific provisions in place. Documentation includes only vague general statements ("Safety and security should be addressed during emergency situations").
There is no coordination between the ERP and SSP/SSPP.
Approval (including date of approval) is verifiable.
ERP has been approved, but approval is not verifiable.
ERP has not been approved.
Well-developed, ***specific*** procedures are in place and documented in the ERP ***or*** as part of another document and referenced in the ERP.
Procedures are in place with varying degrees of implementation or documentation.
Procedures are not in place or documented.
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.
Plans and procedures are in place and function appropriately. However, minor aspects are missing. ERP includes--or references documents that contains--the procedures.
Well organized procedures are in place and contained as part of another document with no reference in the ERP.
Procedures are lacking any depth or clarity, plans are scattered between multiple documents with no reference in ERP, or responsibilities are otherwise ineffectively assigned.
Procedures are not in place or documented.

Continuity of Operations plans exist and are included as part of the ERP (or in another document that is referenced in the ERP).
Continuity of Operations plans exist but are not included as part of the ERP or referenced in the ERP.
No Continuity of Operations plans exist.
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.
Business Recovery Plan is a well-developed document, missing only a few elements or details.
Business Recovery Plan is a generic plan that appears to be a commonly available "template" with only general procedures.
Business Recovery Plan is lacking details and appears incomplete.
There is no plan in place to achieve a timely and orderly recovery and resumption of full service.
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.
Business Continuity Plan is a well-developed document, missing only a few elements or details.
Business Continuity Plan is a generic plan that appears to be a commonly available "template" with only general procedures.
Business Continuity Plan is lacking details and appears incomplete.
There is no plan in place to ensure the continuity of operations.
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.
There is a back up operations control center, but it cannot fully replicate the primary operations center capabilities.
There is no back-up capabilities for the Operations Control Center.
Roles and Responsibilities for Security and Emergency Management
System Security Plan (SSP)
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.
The implementation of the security program has been assigned to a Senior Manager who is a "direct report" to the CEO. This responsibility is not documented in the SSP, but it is a commonly known assignment that is documented elsewhere.
The implementation of the security program has been assigned to a manager or leadership position that is not a "direct report" to the CEO. The responsibility is documented in the SSP.
The implementation of the security program has been ineffectively assigned to a position that cannot act independently. The responsibility is documented in the SSP.
The implementation of the security program is not assigned, or there is no documentation establishing the responsibility of implementation.
The agency has established comprehensive policies and procedures related to "chain of command" ***and*** "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.
The agency has established basic--yet fully developed--procedures related to "chain of command" ***and*** "lines of succession" for security responsibilities. Minor elements are missing or needing further development. Lines of succession may not be in-depth, only identifying one successor for security-critical roles. The policy is documented and shared with agency manager.
The agency has established and documented a "chain of command." Informal (or "generally understood") "lines of succession" are in place but not documented.
The agency has an informal (not documented) "chain of command" only.
The agency has no established "chain of command"
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.
Roles and responsibilities of security personnel are assigned by position and documented in the SSP or other documents; however, minor elements are missing or require minor additions.
General roles and responsibilities are assigned by position and documented in the SSP or other documents. While assigned by position type, the roles and responsibilities are vague. Position types identified may also be vague or missing key positions.
General security roles and responsibilities are documented in the SSP or other documents. These roles and responsibilities are not assigned by position.
Roles and responsibilities are not documented.
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.
Security-related responsibilities have been established for non-security personnel. Specific responsibilities are identified and assigned to all non-security personnel, regardless of job function ("blanket statement"). Responsibilities are documented in the SSP or other documents.
Specific security responsibilities for non-security personnel encompasses less than half of the applicable workforce, but the responsibilities in place are adequately developed. Responsibilities are documented.
Only general security-related responsibilities are documented.
No security-related roles have been established or documented for non-security personnel.
Senior staff and management conduct security meetings on a quarterly basis, at minimum, to review recommendations for changes to plans and processes. Verified by both interview and document review.
Senior staff and management conduct security meetings infrequently, but at least annually, to review recommendations for changes to plans and processes. Only verified through interview.
Senior staff and management meet on an infrequent basis, if ever, or meetings related to security are not conducted.
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.
A formal security committee or working group has been established. This group meets at least twice per year to review security incident reports, trends, and program audit findings. All applicable security items are addressed.
A formal security committee or working group has been established, but it only meets once per year or on an "as needed" basis. This score also applies if the group meets at a higher frequency but doesn't effectively address all applicable security items.
Security items are discussed and addressed by a Safety committee.

Security review committee does not exist or meets on an infrequent basis.

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.).
Entity has procedures in place to ensure that frontline personnel are made aware of anything relevant to the security of their transit system. Method of delivery is, for the most part, effective, with very little (but possible) chance of employees not receiving critical information. Agency has not developed a means of monitoring or tracking who receives informational briefings.
Briefings are only delivered through written-memos or other ineffective means of personal dispersal. For a score of 2, the delivery method might reach a high number of employees, but the message itself is not guaranteed (employees may not understand a message, employees may not actually read the message, and the agency may not be able to accurately gauge who has received the message).
Entity only utilizes bulletin board-style briefings.
No briefings.
Individual written guides or reference material based on job function have been provided to employees to assist employees with the implementation of security procedures. (Example: Driver's manual, SOP, etc.)
Individual written guides or reference material with generalized guidance have been provided to employees to assist employees with the implementation of security procedures.
Written guides or other written materials have been provided to every department and are available to employees if needed.
Written guides or other written materials exist but are not conveniently available to employees.
Written materials are not readily available to employees.
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.
The agency has a Primary and or Alternate Security Coordinator, but their roles are not clearly defined (may not be documented) and/or do not meet all criteria established by TSA (not available 24/7, etc.).
The agency has not identified any Security Coordinators.
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.
Agency has the ability to review incidents that have occurred up to one year earlier.
Agency has the ability to review incidents that have occurred up to six months earlier.
Agency has the ability to review incidents that have occurred up to three months earlier.
Agency does not maintain a record of security related incidents.
Emergency Response Plan (ERP)
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.
The implementation of the security program has been assigned to a Senior Manager who is a "direct report" to the CEO. This responsibility is not documented in the ERP, but it is a commonly known assignment that is documented elsewhere.
The implementation of the security program has been assigned to a manager or leadership position that is not a "direct report" to the CEO. The responsibility is documented in the ERP.
The implementation of the security program has been ineffectively assigned to a position that cannot act independently. The responsibility is documented in the ERP.
The implementation of the security program is not assigned, or there is no documentation establishing the responsibility of implementation.
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.
Emergency response roles and responsibilities have been developed and assigned to most departments. Not all departments have an assigned role in emergency response. Roles and responsibilities are well-developed and assigned effectively, but there is room for improvement. This is documented.
Documented roles and responsibilities have been only assigned to critical departments (security, etc.), may be generalized in nature, or a combination thereof.
Documented roles and responsibilities have been assigned as a blanket-statement. Roles may be vague or ineffectively developed.
Roles and responsibilities are not documented.
Roles and responsibilities of frontline personnel are assigned by position and documented in the ERP. Roles are comprehensive and detailed.
Roles and responsibilities of frontline personnel are assigned and documented in the ERP. Roles are relatively detailed and effectively assigned, but may be missing minor details.
Roles and responsibilities of frontline personnel are developed and documented in the ERP. Roles are general and lack specific details based on job function.
General security roles and responsibilities are documented in the SSP or other documents. These roles and responsibilities are not assigned by position.
Roles and responsibilities are not documented.
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.
The agency is proactive with emergency response. The ERP has been provided to departments that are critical to emergency response as well as some departments that would serve a secondary support role during emergency response.
The agency has only provided the ERP to departments that are critical to emergency response. Upon request, the ERP is readily available to other departments.
ERP distribution is very limited. Departments do not have easy access to the document.
The ERP is not distributed.
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.
Individual written guides or reference material with generalized guidance have been provided to all employees to assist employees with the implementation of emergency procedures.
Written guides or other written materials have been provided to every department and are available to employees if needed.
Written guides or other written materials exist but are not conveniently available to employees.
Written materials are not readily available to employees.
Senior staff and management conduct ERP coordination meetings on a ***monthly*** basis.
Senior staff and management conduct ERP coordination meetings on a ***quarterly*** basis.
Senior staff and management conduct ERP coordination meetings ***twice per year***.

Senior staff and management conduct ERP coordination meetings ***annually*** or on an "as needed" basis.
Senior staff and management meet on an infrequent basis, if ever, or meetings related to ERP coordination are not conducted.
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.).
Entity has procedures in place to ensure that frontline personnel are made aware of anything relevant to the emergency response. Method of delivery is, for the most part, effective, with very little (but possible) chance of employees not receiving critical information. Agency has not developed a means of monitoring or tracking who receives informational briefings.
Briefings are only delivered through written-memos or other ineffective means of personal dispersal. For a score of 2, the delivery method might reach a high number of employees, but the message itself is not guaranteed (employees may not understand a message, employees may not actually read the message, and the agency may not be able to accurately gauge who has received the message).
Entity only utilizes bulletin board-style briefings.
No briefings.
e supervisors, forepersons and managers are held accountable for security issues under their control
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). Verified by Interview, Document review and Frontline employee's
Frontline employees receive a ***monthly*** 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).
Frontline employees receive a ***quarterly*** 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).
Frontline employees are provided information regarding security and emergency response issues on an infrequent or "as needed" basis.
Frontline employees are not provided information regarding security and emergency response issues.
Supervisor/management ***security*** review and coordination meetings are held on a ***monthly*** basis.
Supervisor/management ***security*** review and coordination meetings are held on a ***bimonthly*** basis.
Supervisor/management ***security*** review and coordination meetings are held on a ***quarterly*** basis.
Supervisor/management ***security*** review and coordination meetings are held on an infrequent or "as-needed" basis.
Meetings are not held or do not focus on security.
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. Verified by both Interview and Document Review
The agency has an on-going, informal system of measuring its workforce's knowledge of security elements. The program may not be documented, but the agency can articulate specific measures it takes to ensure its personnel retain a working knowledge of security. Examples include informal (undocumented or unmeasured) internal testing or auditing.
Employees are tested after training, and Supervisors are tasked with ensuring protocols are followed and knowledge is retained.
Direct supervision is the only method of ensuring that security knowledge is retained.
The agency does not have a program of confirming that personnel have a working knowledge of security protocols.
There is a written policy that requires leadership to debrief frontline personnel regarding their involvement in or management of ***any*** security or emergency incidents. Verified by both Interview and Document Review
There isn't a written requirement, but leadership is expected to debrief frontline personnel regarding their involvement in or management of ***any*** security or emergency incidents. This expectation is widely known. Verified by both Interview and Document Review.
Leadership is expected to debrief frontline personnel only after ***major*** incidents regarding their involvement in or management of security or emergency incidents.
Debriefing are being held, but the policy is very insufficient and inconsistent.
There are no debriefing measures in place.
curity and Emergency Management Plan(s) with local and regional agencies
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. Verified by both Interview and Document Review
The agency has taken a proactive approach to emergency preparedness and has established mutual aid agreements with multiple types of outside entities.
The agency has taken a limited approach to emergency preparedness and has established mutual aid agreements with only all local law enforcement entities that operate with the geographical scope of their system.
The agency has taken the first steps of establishing mutual aid agreements. Agreements are actively being pursued.
Mutual aid agreements are non-existent and not being pursued.
The agency participates in a regional security and emergency preparedness/management working group or committee (***this is not the same as participation in drills or exercises).***
The agency does not participate in a security and emergency preparedness/management working group or committee.
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. Verified by both Interview and Document Review.
The agency has received--and is knowledgeable of--regional incident management protocols. These protocols are partially incorporated (or in the process of being incorporated) into the agency's ERP/SSP/SEPP. Verified by both Interview and Document Review.
The agency has received--and is knowledgeable of--regional incident management protocols. These protocols are not part of the agency's ERP.
The agency is aware of regional protocols and understands how they may obtain them.
The agency is completely unfamiliar with regional protocols.
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.
Agency resource inventory has not been provided to the regional EMA

Agency has established a point-of-contact at the Emergency Operations Center. Must be verified by Document Review.
Agency has no identified POC at the EOC.
Agency has officially designated a representative to be sent to the EOC, upon activation. This is documented in SSP/ERP/SEPP. Must be verified by Document Review.
The agency has designated a representative to be sent to the EOC, upon activation, although formal policies are not in place.
Agency has not designated a representative.
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. Must be verified by Document Review.
The agency has developed an ***informal*** 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. It is clear that the agency has planned for information sharing, but the capabilities are not documented.
Information sharing procedures and capabilities exist, but are vague and have received little attention or planning.
The agency has no information sharing capabilities or procedures and is not actively pursuing the development of any.
The agency's internal emergency response procedures follow the NRP and the NIMS. Must be verified by Document Review.
The agency's internal emergency response procedures do not follow the NRP and the NIMS.
The agency has shared its internal emergency response protocols with the regional EMA and appropriate first response agencies.
The agency has shared its internal emergency response protocols with ***only*** the regional EMA ***or only*** first response agencies.
The agency has not shared its emergency response protocols.
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.
The agency has an effective interoperable communications system (800mHz, UHF, VHF, interoperable CAD system), but minor elements are missing. Planning (training or documentation) is missing ***or*** the agency has not tested its system for compatibility.
The agency has an effective interoperable communications system (800mHz, UHF, VHF, interoperable CAD system). Neither planning (training or documentation) or compatibility testing is in place.
The agency's systems are not interoperable, but is in the process of actively implementing such a system (plans established, funds identified).
The agency's systems are not interoperable, nor is such a system being currently implemented.
The agency has developed effective alternatives to interoperable communication (beyond the reliance of standard communication, like telephone). These procedures are documented and shared with appropriate first responder agencies. Must be verified by Document Review.
The agency has developed partially effective alternatives to interoperable communication (beyond the reliance of standard communication, like telephone). The procedures are informal and may not be documented and/or shared with first responder agencies.
The agency has identified no alternatives for interoperable communication.
tablish and Maintain a Security and Emergency Training Program
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). Must be verified by Document Review and Frontline Employee's.
Initial training is provided with varying degrees of implementation.
Security is not addressed in initial training.
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). Must be verified by Document Review.
Training is provided with varying degrees of implementation.
Refresher training is not provided annually or does not focus on the appropriate subject.
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). Must be verified by Document Review.
Training is provided with varying degrees of implementation.
Refresher training is not provided annually or does not focus on the appropriate subject.
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). Must be verified by Document Review and Frontline Employee's.
Training is provided with varying degrees of implementation.
Refresher training is not provided annually or does not focus on the appropriate subject.
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). Must be verified by Document Review and Frontline Employee's.
Ongoing advanced security training based on job function is provided with varying degrees of implementation and frequency.
Ongoing security training based on job function is not provided.

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). Must be verified by Document Review and Frontline Employee's.
Initial training is provided with varying degrees of implementation.
Emergency response is not addressed in initial training.
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). Must be verified by Document Review.
Training is provided with varying degrees of implementation.
Refresher training is not provided annually or does not focus on the appropriate subject.
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). Must be verified by Document Review.
Training is provided with varying degrees of implementation.
Refresher training is not provided annually or does not focus on the appropriate subject.
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). Must be verified by Document Review and Frontline Employee's.
Training is provided with varying degrees of implementation.
Refresher training is not provided annually or does not focus on the appropriate subject.
All employees who may have a role in emergency response--frontline personnel ***and*** leadership--have received ICS training in accordance with the NIMS. The agency has a well-developed program with an official curriculum and training is provided annually in a formal environment (classroom or computer-based). Must be verified by Document Review and Frontline Employee's.
Training is provided with varying degrees of implementation.
ICS training is not provided.
Annual ICS and NIMS training based on job function is provided by the agency to all senior leadership. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
Senior leadership only receives basic ICS/NIMS training, or ICS/NIMS training is not provided.
Annual ICS and NIMS training based on job function is provided by the agency to all supervisors and managers. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
Supervisors and managers only receive basic ICS/NIMS training, or ICS/NIMS training is not provided.
Annual ICS and NIMS training based on job function is provided by the agency to all frontline personnel. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
ICS/NIMS training is not provided.
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). Training is provided annually. Must be verified by Document Review.
Training is provided with varying degrees of implementation.
The agency has not established training for its internal incident response procedures.
Annual training based on job function is provided by the agency to all senior leadership. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
Senior leadership only receives basic training, training appropriate for frontline personnel, or training is not provided.
Annual training based on job function is provided by the agency to all supervisors and managers. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
Supervisors and managers only receive basic training, training that is appropriate to frontline personnel, or training is not provided.
Annual training based on job function is provided by the agency to all frontline personnel. Must be verified by Document Review and Frontline Employee's.
Training appropriate to the position has been provided with varying degrees of implementation.
Training is not provided.
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). Must be verified by Document Review.
Training has been developed and provided with varying degrees of implementation.
The agency has not developed a relevant training program.

Annual training based on job function is provided by the agency to all senior leadership. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
Senior leadership only receives basic training, training is appropriate for frontline personnel, or training is not provided.
Annual training based on job function is provided by the agency to all supervisors and managers. Must be verified by Document Review.
Training appropriate to the position has been provided with varying degrees of implementation.
Supervisors and managers only receive basic training, training is appropriate to frontline personnel, or training is not provided.
Annual training based on job function is provided by the agency to all frontline personnel. Must be verified by Document Review and Frontline Employee's.
Training appropriate to the position has been provided with varying degrees of implementation.
Training is not provided.
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 provided in a formal environment (classroom or computer-based). Must be verified by Document Review.
Specialized counter-terrorism training is provided with varying degrees of implementation.
Specialized counter-terrorism training is provided with varying degrees of implementation.
All personnel in security-related positions receive annual specialized training supporting incident response. 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). Must be verified by Document Review.
Specialized incident response training is provided with varying degrees of implementation.
Specialized incident response training is provided with varying degrees of implementation.
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.
A program for monitoring and scheduling training exists with varying degrees of implementation.
Such a program does not exist.
The agency has a formal system to ***record and track*** personnel training for ***all security-related training***, including initial, annual, and periodic. Records for ***all*** employees contain the following: employee name/identifier, training/course identifier, and date of course completion. Must be verified by Document Review.
The agency employs a system with varying degrees of implementation.
Such a system does not exist, or ***security*** training is not specifically addressed.
The agency has a formal system to ***record and track*** personnel training for ***all emergency response-related training***, including initial, annual, and periodic. Records for ***all*** employees contain the following: employee name/identifier, training/course identifier, and date of course completion.
The agency employs a system with varying degrees of implementation.
Such a system does not exist, or ***emergency response*** training is not specifically addressed.
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. Must be verified by Document Review.
The agency has developed a program with varying degrees of implementation.
The agency has no established program of reviewing and updating security and emergency response training materials.
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 ***all*** appropriate employees.
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 for the agency to confidently reach ***most*** of those employees in timely manner..
Appropriate personnel are notified of operational changes. Individuals with a "need to know" are informally identified, but measures of communicating information is lacking consistency.
The agency notification measures are inconsistent with little to no planning involved whatsoever. Individuals with a "need to know" have not been identified.
Operational changes are rarely--if ever--communicated to employees, or no policy exists to support the recommendation.

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).
Security and emergency response training covers response and recovery operations in critical facilities and infrastructure with varying degrees of implementation.
Training does not cover response and recovery operations.
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.
The agency has provided training with varying degrees of implementation.
The agency has not provided training to external agencies to enable them to operate effectively in critical facilities and infrastructure.
The concept and employment of visible, unpredictable, and random security measures is included as part of the training curriculum for ***all*** personnel in security-related positions. This is documented in training materials. Must be verified by Document Review.
Training covers the concept of visible and random security measures with varying degrees of implementation.
Training does not cover the concept visible or random security measures.
The agency has developed and implemented a program to ***annually*** train or orient first responders and other supporting agencies (TSA VIPR teams) on their system vehicle familiarization. Training is well-developed, and the agency has actively offered it to outside entities. Must be verified by Document Review.
The program has been developed with varying degrees of implementation.
Such a program does not exist.
nd protocols to respond to the DHS National Terrorism Advisory System (NTAS).
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.
Incremental actions are identified with varying degrees of implementation or documentation.
Incremental actions are not documented.
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.
Actionable operational response protocols for specific threat scenarios from NTAS have been developed with varying degrees of implementation.
Actionable operational response protocols have not been developed or specific threat scenarios haven't been identified.
Job-specific NTAS training that focuses on incremental activities to be performed by employees has been provided annually by the agency. Training is a 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). Must be verified by Document Review.
Job-specific NTAS training is provided with varying degrees of implementation.
General NTAS training is provided to appropriate personnel.
The agency does not provide NTAS training.

and reinforce a Public Security and Emergency Awareness program:
Agency has implemented a well-developed public awareness program that addresses specific issues of both security ***and*** emergency response.
Agency has implemented a well-developed public awareness program that addresses specific issues of security. Emergency response material is generalized or missing.
Agency has implemented a well-developed public awareness program that address specific issues of emergency response and safety. Security material is generalized or missing.
Agency has a public awareness program, but the program is vague or otherwise ineffective.
The agency has no public awareness program in place.
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. Must be verified by Document Review and Onsite Observation.
Public awareness materials and outreach have been developed and deployed with varying degrees of implementation. Verified by Document Review only.
Public awareness materials and outreach have not been developed and/or deployed.
Public awareness material is consistent with the agency's overall announcement program. All information/instruction/guidance is the same. Must be verified by Document Review and Onsite Observation.
Public awareness material conflicts with the agency's overall announcement program.
The agency includes frequent mentions of general security ***and*** emergency preparedness items in its pre-recorded announcement messages at all appropriate areas, including at stations and onboard vehicles.
The agency includes frequent mentions of general security items (but no emergency preparedness items) in its pre-recorded announcement messages at all appropriate areas, including at stations and onboard vehicles.
The agency includes frequent mentions of general emergency preparedness items ***and*** infrequent mentions of general security items in its pre-recorded announcement messages at all appropriate areas, including at stations and onboard vehicles;
The agency includes ***infrequent*** mentions of general security and emergency preparedness items in its pre-recorded announcement messages at all appropriate areas, including at stations and onboard vehicles.
Security and emergency preparedness items are not included in the agency's pre-recorded announcement messages.
Passengers are urged to report unattended property, suspicious behavior, and other security concerns to an identified agency representative (uniformed crew member, law enforcement, etc.) or identified contact number. This is documented in awareness material and readily observable. Must be verified by Document Review and Onsite Observation.
Passengers are urged to report unattended property, suspicious behavior, and other security concerns with varying degrees of implementation.
Passengers are not urged to report unattended property, suspicious behavior, and other security concerns with varying degrees of implementation.
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. Must be verified by Document Review and Onsite Observation.
A mechanism is in place with varying degrees of implementation.
There is no mechanism in place.
The agency utilizes social media to issue public service announcements related to security or emergency response. This method is documented or readily observable.
The agency does not issue security-related PSAs or press releases to local media.
The agency issues security- and emergency response-related PSAs or press releases to local media. This method is documented or readily observable.
The agency does not issue emergency response-related PSAs or press releases to local media.
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. Must be verified by Document Review.
Training is provided with varying degrees of implementation.
Training is not provided.
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. Must be verified by Document Review.
The agency has established an active volunteer program with varying degrees of implementation.
The agency has not established an active volunteer program.

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. Must be verified by Document Review.
The agency has developed awareness material with varying degrees of implementation.
The agency has not developed awareness material to assist passengers on the means of safe evacuation.
The agency has a system in place to actively and effectively monitor and follow up on customer reports.
The agency has developed a system with varying degrees of effectiveness or implementation.
The agency has not developed a system for tracking and following up on customer reports.
Management Process to assess and manage threats, vulnerabilities and consequences
Risk assessment process is developed, documented, specifically addresses threats and vulnerabilities, and is approved by management. Must be verified by Document Review.
Risk assessment process is developed with varying degrees of implementation.
Risk assessment process has not been developed.
The agency has identified facilities and systems it considers critical assets. This is documented (or clearly implied in documentation/procedures). Must be verified by Document Review.
The agency has identified critical assets with varying degrees of documentation or development.
The agency has not identified critical assets.
A vulnerability assessment focused on the agency's ***critical assets*** has been conducted within the last 3 years. Must also be verified by Document Review.
A vulnerability assessment focused on the agency's ***critical assets*** has been conducted within the last 3 years. Only verified by Interview.
A security assessment focused on the agency's critical assets has not been conducted within the last 3 years.
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. Must be verified by Document Review.
A risk assessment has been conducted with varying degrees of implementation or training on completing such assessment. Assessment is documented and available for review. Must be verified by Document Review.
A risk assessment has not been conducted, or documentation does not exist.
The system has well-developed, well-documented policies and procedures in place to limit and monitor access to underground and underwater tunnels. Must be verified by Document Review.
Documented policies are in place with varying degrees of implementation. Verified only by Interview.
Policies and procedures have not been developed or documented.
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.
Security investments are prioritized based on information obtained during risk assessments; ***however***, this has been implemented or documented with varying degrees of development.
Security investments are not prioritized based on information obtained during risk assessments ***or*** risk assessments play no role in financial decisions.
The agency has provided TSA with ***all*** requested documents.
The agency has ***not*** provided TSA with ***all*** requested documents.
use an information sharing process for threat and intelligence information
The entity is actively involved with intelligence sharing and has developed a formalized (***documented***) method of sharing threat/intel information with multiple entities representing local, State ***and*** Federal law enforcement.
The entity has a formalized method of sharing information with varying degrees of implementation.
The entity does not have a formalized method of sharing information with law enforcement entities.
The agency reports threat/intel information ***directly*** to the JTTF or regional anti-terrorism task force. Must be verified by Document Review.
The agency does not report threat/intel information ***directly*** to the JTTF or regional anti-terrorism task force.
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.). Must be verified by Document Review.
The agency has detailed policies and protocols in place to report real-time threats/significant security concerns to appropriate law enforcement ***or*** TSOC. These protocols are documented and include a "time" element (immediately, within "X" hours, etc.).
General/vague policies and procedures are in place with varying degrees of implementation.
Policies and procedures are not in place.

The agency receives threat/intel information ***at least once per week.***
The agency receives threat/intel information on an ***every-other-week*** basis.
The agency receives threat/intel information on a ***monthly*** basis.
The agency receives threat/intel information on a ***quarterly*** basis ***or*** information is not ***directly*** from an appropriate source.
The agency does not receive threat/intel information.
The agency reports NTA security data to FTA.
The agency does not report NTA security data to FTA.
Conduct Tabletop and Functional Drills
The agency has developed a ***detailed*** 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 which is referenced in the SSPP.
The agency has developed a process with varying degrees of implementation or documentation.
The agency has not developed such a process.
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.
Roles, responsibilities and requirements regarding emergency planning are developed with varying degrees of implementation or documentation.
Roles, responsibilities and requirements regarding emergency planning are not developed or documented.
The agency conducts drills and exercises ***annually*** with the purpose of ***evaluating*** its emergency preparedness procedures.
The agency does not conduct drills and exercises ***annually,*** or the agency does not use drills/exercises to evaluate emergency preparedness procedures.
The agency has a ***documented requirement*** for drills/exercises to be conducted ***once per year*** at a minimum.
The agency does not have a documented requirement for drills/exercises to be conducted once per year at a minimum.
The process of drill/exercise evaluation is described and documented in the SSPP, SSP, or another document that is referenced by the SSPP/SSP.
The process of evaluation is not documented.
The program for providing employee training on emergency response protocols and procedures is ***documented.***
The training program is not ***documented.***
The agency participates as an ***active player*** in full-scale, regional exercises held at least ***annually***.
The agency does not participate as an ***active player*** in full-scale, regional exercises held at least ***annually.***
In the last year, the agency has been involved in drills/exercises that specifically focus on IEDs ***and*** WMD with appropriate external entities, to include first responders ***and*** other transit agencies that operate in the same environment.
Terrorism-specific drills have been conducted/participated in with varying degrees of action.
Terrorism-specific drills have not been conducted or participated in.
In the last year, the agency has reviewed and prepared after-action reports (or other evaluating report) for ***all*** drills and exercises. ***All*** evaluations are documented. Must be verified by Document Review.
The agency has evaluated drills with varying degrees of implementation or documentation.
The agency has not evaluated drills in the past year.

In the last year, the agency has updated plans, protocols, or processes to incorporate after-action report recommendations/findings. Must be verified by Document Review.
The agency has not made any changes based on the results of drills/exercises.
The agency has developed a formal, objective system of evaluating drill performance. The agency has identified evaluation ***criteria***, establishes drill/exercise ***goals***, and analyzes the results appropriately. This system is documented. Must be verified by Document Review.
The agency has established performance metrics with varying degrees of implementation.
The agency has not established metrics to assess performance during emergency exercises.
The agency conducts exercises of its security ***and*** emergency response plans to test operational capabilities of employees ***and*** first responders in underwater/underground infrastructure and other critical systems.
The agency conducts exercises with a varying degree of implementation.
The agency does not conduct exercises related to underwater/underground infrastructure.
The agency actively reaches out to external emergency agencies (local and regional) when planning and conducting exercises. The agency integrates ***all*** appropriate entities: fire, medical, ***and*** law enforcement.
Drills with external agencies have been conducted with varying degrees of inclusion or frequency.
Drills with external agencies have not been conducted.
Developing a Comprehensive Cyber Security Strategy
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. Must be verified by Document Review.
The agency has conducted an IT risk assessment with varying degrees of implementation or documentation.
The agency has not conducted an IT risk assessment.
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. Must be verified by Document Review.
Protocols have been established with varying degrees of implementation or documentation.
Such security protocols have not been established.
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).
An IT-security strategy has been developed with varying degrees of implementation or documentation.
An IT-security strategy has not been developed.

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.
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, but his/her responsibilities are ***not*** documented (but widely known).
The agency has formally designated an individual responsible for securing the internal network. This individual lacks a comprehensive knowledge of the agency's cybersecurity measures.
An individual has been informally designated, and his/her responsibilities are not widely known.
An individual has not been designated.
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).
IT-security training is provided with varying degrees of implementation.
IT-security training is not provided.
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. Must be verified by Document Review.
Cyber-incident response and reporting protocols have been established with varying degrees of implementation or documentation.
Cyber-incident response and reporting protocols have not been established.
The agency is aware of and makes use of available resources.
The agency is not aware of available resources ***or*** the agency does not use available resources.
Control Access to Security Critical Facilities
Restricted areas are identified and documented. Agency personnel are familiar with their location and restricted status. Must be verified by Document Review.
Restricted areas have been identified with varying degrees of implementation.
Restricted areas have not been identified.
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. Must be verified by Frontline Observation.
ID badges (or other effective measure) are issued with varying degrees of implementation.
ID badges or similar measures are not employed by the agency.
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.
The agency utilizes an access control system with varying degrees of implementation of capability.
The agency's access control procedures is not capable of monitoring, documenting, and updating access.
The agency has documented procedures in place to issue ID badges for visitors and contractors. These procedures are implemented perfectly.
The agency has procedures in place to issue ID badges for visitors and contractors with varying degrees of implementation or documentation. Must be verified by Frontline Observation.
The agency does not have procedures for issuing ID badges to visitors and contractors.
The agency has a documented policy that requires visitors to be escorted when accessing non-public areas. This policy is implemented perfectly.
The agency has policy In place with varying degrees of implementation or documentation.
The agency has no escort requirements for visitors.
Effective and capable CCTV systems are installed at all facilities. Must be verified by Frontline Observation.
Facilities are equipped with CCTV with varying degrees of installation or capability.
Facilities are equipped with CCTV with varying degrees of installation.
CCTV equipment protecting critical assets are completely integrated with other access control measures (door breach triggers automated CCTV functions, etc.).
CCTV is interfaced with access control systems with varying degrees of integration.
CCTV is a stand-alone system, not interfaced with access control.
Effective and capable CCTV systems are installed on a vast majority of vehicle fleet.
CCTV is installed with varying degrees of implementation or capability.
CCTV is not installed on vehicles ***or*** CCTV is non-functional.
CPTED is incorporated in the design of ***all*** projects. CPTED-related vulnerabilities are identified and corrected promptly using technological solutions or other solutions.
CPTED criteria is used with varying degrees of implementation.
CPTED criteria is not used.

The agency has installed physical barriers or intrusion detection systems to prevent unauthorized access at ***all*** appropriate stations, facilities, and critical infrastructure.
The agency uses barriers and intrusion detection systems with varying degrees of installation or capability.
The agency does not use physical barriers or intrusion detection systems at appropriate stations, facilities and/or critical infrastructure.
The agency has identified high risk/high consequence assets ***and*** has implemented additional security measures for ***all*** such assets. Additional measures are documented.
The agency has identified high risk/high consequence assets and developed additional security measures with varying degrees of implementation or documentation.
The agency has not identified high risk/high consequence assets ***and/or*** implemented additional security measures to protect such assets.
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.
The agency has a means of effectively monitoring a network of alarms.
The agency has a network of appropriate alarms that are not effectively monitored.
The agency utilizes an ineffective or insufficient network of alarms.
The agency has no alarm systems.
Call boxes are installed at ***all*** stations, terminals, and appropriate facilities. Call boxes are fully functional.
Call boxes are installed at varying degrees. Must be verified by Physical Observation.
Call boxes are not used.
The agency uses an automated access control system ***and*** performs a corrective analysis of ***all*** security breaches to prevent future occurrences of a similar nature. This corrective analysis is documented as part of an overarching policy or as part of an identified employee's responsibilities.
The agency uses an automated access control system ***and*** performs a formal corrective analysis of ***all*** security breaches to prevent future occurrences of a similar nature. Corrective analysis is being performed, but this responsibility is not documented.
The agency uses an automated access control system ***and*** performs a corrective analysis of some security breaches, including those deemed "important."
The agency uses an automated access control system, but has not developed procedures to perform corrective analysis of security breaches.
The agency does not use an automated access control system.
The agency has documented policies and specific, well-developed procedures that address the screening of mail or outside deliveries. Procedures are completely implemented.
The agency has specific, well-developed procedures that are not documented. Procedures are completely implemented.
The agency has general procedures in place with varying degrees of implementation.
The agency has policies or procedures for screening mail or outside deliveries.
The agency uses ***multiple*** methods of breach prevention (locks, anti-frag materials, bullet resistant materials, etc) at ***all*** critical locations.
The agency utilizes methods of breach prevention at critical location with varying degrees of implementation.
The agency does not use locks, bullet-resistant materials, or anti-fragmentation materials at critical locations.
NFPA 130 or equivalent is used in station design or modification criteria. Access Control systems do not interfere with safety or emergency operations.
Access control systems interfere with safety or emergency operations.
Directional signage and lighting is consistent at ***all*** stations and is installed in a manner that supports security, safety and emergency operations.
Directional signage and lighting is used with varying degrees of implementation or installation. Must be verified by Physical Observation.
Directional signage and lighting does not support security, safety, and emergency operations.
The agency uses gates and locks to prevent unauthorized access at ***all*** facilities. Policies and procedures are in place to effectively utilize locks and gates.
Gates and locks are used with varying degrees of implementation. Must be verified by Physical Observation.
Gates and locks are not used to restrict access to facilities.

The agency has a documented key control program that is managed by the security/internal police department.
The agency has a key control program with varying degrees of documentation or implementation.
The agency has no key control program.
Gates and locks are used at ***all*** facilities that are closed down. Policies and procedures are in place to effectively utilize locks and gates. Must be verified by Physical Observation.
Gates and locks are used with varying degrees of implementation. Must be verified by Physical Observation.
Gates and locks are not used to secure facilities after operating hours.
All (or the vast majority of) transit vehicles are equipped with radios, silent alarms, and/or passenger communication systems. Policies and procedures are in place to effectively utilize these measures.
Radios, silent alarms, and/or passenger communication systems are used with varying degrees of implementation.
Radios, silent alarms, and/or passenger communication systems are not used.
Graffiti-resistant/etch-resistant materials are used at ***all*** (or a vast majority of) facilities.
Materials are actively deployed at "problematic" areas prone to vandalism.
Materials are rarely used.
Materials are not used.
Uninterruptible Power Supplies are provided for ***all*** safety- and security-critical equipment.
A combination of UPS and other back-up power is provided for ***all*** safety- and security-critical equipment.
A combination of UPS and other back-up power is provided for a ***majority*** of safety- and security-critical equipment.
A combination of UPS and other back-up power is provided for main facilities.
The agency has no back-up power capabilities.
The agency has removed non-explosive resistant trash receptacles from platform areas of terminals and stations.
The agency has not removed non-explosive resistant trash receptacles from platform areas of terminals and stations.
The agency has formally identified critical infrastructure and deployed specific, effective protective measures, which are maintained and implemented appropriately, at ***all*** identified areas.
The agency has deployed protective measures with varying degrees of implementation or effectiveness.
Measures are not deployed to protect critical infrastructure or critical infrastructure has not been identified.
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.
The agency utilizes explosive detection canine teams with varying degrees of program development.
The agency does not use or have access to explosive detection canine teams.

Conduct Physical Security Inspections
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.
Security inspections are conducted with varying degrees of implementation or documentation. Must be verified by Document Review.
Security inspections are not conducted.
Documented security procedures reflect HOT characteristics. Must be verified by Frontline Employee's.
Documented security procedures do not reflect HOT characteristics.
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.
The agency does not use a checklist/form for vehicle security inspections ***or*** the agency's checklist/form does not address security.
The agency utilizes a checklist or other widely distributed document that specifically addresses ***security*** to assist personnel conducting station/facility inspections.
The agency does not use a checklist/form for facility security inspections ***or*** the agency's checklist/form does not address security.
Inspection results are documented ***and*** the agency implements corrective actions or other modifications based on these results. This is readily observable in changes made by the agency or is a documented policy.
Results are documented and changes are made with varying degrees of implementation or documentation.
Results are not documented ***or*** inspection results are not a factor in the decision-making process.
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. Must be verified by Document Review.
Security inspections are conducted with varying degrees of implementation or documentation.
Security inspections are not conducted.
Security activities are conducted at random times and at random intervals and these procedures are documented. Must be verified by Document Review.
Security activities are conducted at set times.
The agency has documented policies and procedures in place to ensure that ***all*** in-service rail cars are inspected at multiple times per day for suspicious or unattended items ***and*** personnel receive training to properly conduct these inspections.
Rail cars are inspected with varying degrees of implementation or documentation.
Rail cars are not inspected for suspicious or unattended items.
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 ***and*** personnel receive training to properly conduct these inspections.
Critical infrastructure is inspected with varying degrees of implementation or documentation.
Critical infrastructure is not inspected for suspicious or unattended items.

Conduct Background Investigations of Employees and Contractors
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.
The agency conducts an appropriate level of background check with varying degrees of implementation.
Agency-personnel are not subject to background investigation.
The agency **(a)** conducts an appropriate level of background check on relevant contract employees ***or*** **(b)** the agency builds appropriate background check criteria into the bid process ***and*** has established a method of verifying/auditing background checks.
The agency conducts (or requires) an appropriate level of background check with varying degrees of implementation.
Relevant contract employees are not subject to background investigation.
The agency's process for conducting background investigations has been reviewed by a legal professional.
The agency's process for conducting background investigations has ***not*** been reviewed by a legal professional.
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).
The background investigation process is documented with varying degrees of implementation.
The background investigation process is ***not*** documented.
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.
Background screening criteria (disqualifying conditions) is based on job-function, required level of access, and/or responsibility with varying degrees of implementation or documentation.
Background screening criteria is not documented.
trol Access to documents of security critical systems and facilities
The agency has well-developed document control procedures that protect security-critical documentation from unauthorized access. ***All*** documents are appropriately protected: plans, schematics, etc.
The agency has developed document control procedures with varying degrees of implementation.
The agency does not protect security-critical documentation.
A person or department has been formally tasked with administering the access control policy with respect to agency documents.
A person or department has ***not*** been formally tasked with administering the access control policy with respect to agency documents.
A security review committee actively reviews document control practices, assess compliance-applicable procedures, and identifies discrepancies and corrective action regularly.
A security review committee covers document control issues with varying degrees of action.
Document control issues are not addressed by the security review committee.

ess for handling and access to Sensitive Security Information (SSI)
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.
The agency's SSI policy covers identification and distribution with varying degrees of implementation or documentation.
The SSI policy is not documented ***or*** documentation contains no mention of SSI identification and distribution.
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.
The agency's SSI policy covers handling and storage with varying degrees of implementation or documentation.
The SSI policy is not documented or documentation contains no mention of SSI handling or storage.
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. Must be verified.
Based on a random sampling of frontline interviews, employees who may be provided SSI materials have a working knowledge of the agency's SSI policy with varying degrees of familiarity. Must be verified.
Based on a random sampling of frontline interviews, employees who may be provided SSI materials are not familiar with the agency's SSI policy ***or*** such a policy does not exist.
The agency has established official SSI training (with appropriate materials), ***and*** based on a sampling of frontline personnel interviews, ***all*** employees who may be provided access to SSI have been provided the training. Must be verified.
Based on a sampling of frontline interviews, SSI training has been provided with varying degrees of implementation or development. Must be verified.
SSI training has not been provided or has not been developed.
Audit Program
The agency has a documented schedule for conducting internal ***security*** audits in an ***ongoing manner over a three-year period.***
The agency has developed a schedule for conducting internal ***security*** audits with varying degrees of documentation.
The agency has no documented schedule for conducting internal ***security*** audits.
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.
The SSP contains a description of the internal security audit process with varying degrees of development or documentation.
The SSP does not contain a description of the internal security audit process.
The agency has well-developed procedures for conducting internal security audits ***and*** uses checklists/forms to properly and consistently conduct audits.
The agency has developed procedures ***and*** checklists with varying degrees of development or implementation.
The agency does not use checklists, but has documented procedures in place.
The agency has no documented procedures for
The agency is conducting internal security audits in a manner that reflects its established schedule. Must be verified by Document Review.
The agency is not complying with it established schedule ***or*** such a schedule does not exist.
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.
Internal security audits are documented with varying degrees of implementation.
Audits are not documented.
In the last 12 months, the Security Review Committee has reviewed audit reports, addressed findings, and updated plans and protocols as necessary.
In the last 12 months, the Security Review Committee has reviewed audit reports with varying degrees of action.
The Security Review Committee does not review audit reports ***or*** the committee has not reviewed audit reports within the last 12 months.

Auditors are independent from the individuals they are tasked with auditing to prevent any conflicts of interest.
Auditors are ***not*** independent from the individuals they are tasked with auditing.
The agency has made its internal security audit schedule available to the SSO agency.
The agency has ***not*** made its internal security audit schedule available to the SSO agency.
The agency has made checklists and procedures used in its internal security audits available to the SSO agency.
The agency has ***not*** made checklists and procedures used in its internal security audits available to the SSO agency.
The agency has notified the SSO agency 30 days prior to the conduct of an internal security audit.
The agency has ***not*** notified the SSO agency 30 days prior to the conduct of an internal security audit.
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.
A report documenting internal security audit process and the status of findings and corrective actions have ***not*** been made available to the SSO agency within the previous 12 months.
The agency's chief executive has certified to the SSO agency that the agency is in compliance with its SSP.
The agency's chief executive has ***not*** certified to the SSO agency that the agency is in compliance with its SSP.
The previously mentioned certification was included with the most recent annual report submitted to the SSO agency.
The previously mentioned certification was ***not*** included with the most recent annual report submitted to the SSO agency.
A corrective action plan was developed and made available to the SSO.
A corrective action plan was ***not*** developed and made available to the SSO.

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

Mass Transit Baseline Assessment for Security Enhancements (MT-BASE)

Transportation Security Administration

Date of Visit	TSA Field Office	Region #

FSD AOR Field Office (Optional):	
Assessment Started:	
Assessment Completed:	
Outbrief Conducted:	

TYPE OF VISIT	Agency
Corporate Review	

Is This A Revisit?	Date of Last Interview/Visit?	Street					
		City		State		Zip Code	

Not Governed By 49 CFR Part 659?		Agency Website:	
Agency Size:		Company Chosen By:	
Agency Annual Ridership Amount:		HTUA Name:	
Grant Funding - Section 5311 of Title 49:		Most Recent Grant Received in:	

Types of Service (Check all that apply)

Light Rail		Inclined Plane		Tourist / Scenic	
Heavy Rail		Funicular		Commuter	
Rapid Rail		Trolley		Intercity	
Monorail		Automated Guideway		Transit Bus	

Security Personnel Interviewed

Name	Title	Telephone	Cell	E-mail
	Security Coordinator			
	Alternate Security Coordinator			

Other Agency Points of Contact

Name	Title	Telephone	Cell	E-mail

TSI Inspector Information

Name	Title	Airport Code	Telephone	E-mail
	Lead TSI			
	Secondary TSI			

Supervisory Approval

Name	Title	Airport Code	Telephone	E-mail
	STSI			
	AFSD-I			

Headquarters Approval

Name	Title	Airport Code	Telephone	E-mail
		HQ		
		HQ		

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration
Mass Transit
Baseline Assessment & Security Enhancement Review Checklist

Company Name: 0
Lead Inspector: 0
Assessment Date: 12/30/1899

Section	Description	N/A	Findings Score	Justification: Source	Justification: Score Rationale
	MANAGEMENT AND ACCOUNTABILITY				
1.000	**Establish Written System Security Plans (SSPs) and Emergency Response Plans (ERPs)**				
1.100	**System Security Plan (SSP)**				
1.101	Does the transit agency have a System Security Plan (SSP)?				
1.102	Does the SSP identify the goals and objectives for the security program?				
1.103	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, including the agency's chief executive?				
1.104	Is the SSP separate from the agency's System Safety Program Plan (SSPP)?				
1.105 / T1	Do the Security and Emergency Response Plans address protection and response for critical underwater tunnels, underground stations/ tunnels and other critical systems, where applicable?				
1.106	Does the SSP contain or reference other documents establishing procedures for the management of security incidents by the operations control center (or dispatch center)?				
1.107	Does the SSP contain or reference other documents establishing plans, procedures, or protocols for responding to security events with external agencies (such as law enforcement, local EMA, fire departments, etc.)?				

1.108	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)?				
1.109 / T3	Are visible, random security measures integrated into security plans to introduce unpredictability into security activities for deterrent effect?				
1.110	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?				
1.111	Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?				
1.112	Does the SSP require an annual review?				
1.113	Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?				
1.114	Has an annual review of the SSP been performed and documented in the preceding 12 months?				
1.115	Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP?				
1.116	Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?				

1.200	Emergency Response Plan (ERP)				
1.201	Does the transit agency have an Emergency Response Plan (ERP)?				
1.202	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, including the agency's chief executive?				
1.203	Does the ERP require an annual review to determine if it needs to be updated?				
1.204	Has an annual review of the ERP been performed and documented in the preceding 12 months?				
1.205	Does the ERP include a process or review provision to ensure coordination with the transit agency's SSPP and SSP?				
1.206	Has the transit agency received documentation from the SSO confirming its review and approval of the ERP currently in effect?				
1.207	Does the ERP contain or reference other documents establishing plans, procedures, or protocols for responding to emergency events with external agencies (such as law enforcement, local EMA, fire departments, etc.)?				
1.208	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)?				
1.209	Does the ERP contain or reference other documents to provide for Continuity of Operations (COOP) while responding to emergency events?				

1.210	Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event?				
1.211	Does the agency have a written Business Continuity Plan and COOP to guide restoration of facilities and services following an emergency event?				
1.212	Does the agency have a back-up operations control center capability?				
2.000	**Define Roles and Responsibilities for Security and Emergency Management**				
2.100	**System Security Plan (SSP)**				
2.101	Does the SSP establish and assign responsibility for implementation of the security program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?				
2.102	Has the agency established lines of delegated authority/succession of security responsibilities and, if so, has that information been distributed to agency managers?				
2.103	Are roles and responsibilities for security and/or law enforcement personnel assigned by title and/or position established in the SSP or other documents?				
2.104	Are security-related roles and responsibilities for non-security and/or law enforcement personnel (i.e., operators, conductors, maintenance workers and station attendants) established in the SSP or other documents?				
2.105 / T2	Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes?				
2.106	Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings?				

2.107	Are informational briefings with appropriate personnel held whenever security protocols, threat levels, or protective measures are updated or as security conditions warrant?				
2.108	Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the SSP?				
2.109	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?				
2.110	Does the agency maintain a record of security related incidents that are reported within the agency?				

2.200	**Emergency Response Plan (ERP):**				
2.201	Does the ERP 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?				
2.202	Are emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?				
2.203 / T5	Are roles and responsibilities for front-line personnel (i.e. system law enforcement, system security officials, train or vehicle operators, conductors, station attendants, maintenance workers) described in the system's Emergency Response Plan (ERP)?				
2.204	Has the ERP been distributed to appropriate departments in the organization?				
2.205	Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the ERP?				
2.206	Are senior staff and middle management ERP coordination meetings held on a regular basis?				
2.207	Are informational briefings with appropriate personnel held whenever emergency response protocols are substantially changed or updated?				
3.000	**Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control**				
3.101	Do managers and supervisors routinely provide information to front-line personnel regarding security and emergency response issues?				

3.102	Are regular supervisor, manager, and/or foreperson security review and coordination briefings held? If so, detail frequency and subjects covered in the justification.				
3.103	Does the agency have a program for confirming that personnel have a working knowledge of security protocols? If so, summarize program in the justification.				
3.104	Are managers and/or supervisors required to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?				
4.000	**Coordinate Security and Emergency Management Plan(s) with local and regional agencies**				
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?				
4.102	Does the agency participate in a regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and response?				
4.103	Have regional incident management protocols been shared with the agency and incorporated into the agency's ERP/SSP/SEPP?				
4.104	Have agency resources been appropriately identified and provided to the regional EMA?				
4.105	Does the agency have a designated point-of-contact or liaison with the local/regional Emergency Operations Center (EOC)?				
4.106	Does the agency send a representative to the local/regional EOC, should it be activated?				

4.107	Does the agency have information sharing capabilities with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?				
4.108	Has the agency developed internal incident management protocols that comply with the National Response Plan and the National Incident Management System (NIMS)?				
4.109	Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?				
4.110 / T5	Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?				
4.111	If the agency's communications systems are NOT inter-operable with appropriate emergency response agencies, have alternate communication protocols been established? Describe the alternate communication protocols in the justification.				

	SECURITY AND EMERGENCY RESPONSE TRAINING				
5.000	**Establish and Maintain a Security and Emergency Training Program**				
5.101 / T4	Is initial training provided to all new agency employees regarding security orientation/awareness?				
5.102 / T4	Is annual refresher training provided regarding security orientation/awareness to Senior Management staff, managers and supervisors?				
5.103 / T4	Is annual refresher training provided regarding security orientation/awareness to managers and supervisors?				
5.104 / T4	Is annual refresher training provided regarding security orientation/awareness to front-line employees?				
5.105	Is ongoing advanced security training focused on job function provided at least annually?				
5.106 / T4	Is initial training provided to all new transit employees regarding emergency response?				
5.107 / T4	Is annual refresher training provided regarding emergency response to Senior Management staff, supervisors, and managers?				
5.108 / T4	Is annual refresher training provided regarding emergency response to Managers and Supervisors?				
5.109 / T4	Is annual refresher training provided regarding emergency response to front-line Employees?				

5.110 / T4	Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System at least annually?				
5.111	Has ICS and NIMS training appropriate to the position been provided to Senior Management staff, supervisors, and managers at least annually?				
5.112	Has ICS and NIMS training appropriate to the position been provided to managers and supervisors at least annually?				
5.113	Has ICS and NIMS training appropriate to the position been provided to front-line employees at least annually?				
5.114	Has the agency developed a program and provided annual training on its own incident response protocols?				
5.115 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to Senior Management staff, managers and supervisors at least annually?				
5.116 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to managers and supervisors?				
5.117 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to front-line employees at least annually?				
5.118 / T4	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?				

5.119	Has training focused on IEDs and WMDs appropriate to the position been provided to Senior Management staff, managers, and supervisors at least annually?				
5.120	Has training focused on IEDs and WMDs appropriate to the position been provided to manager and supervisors?				
5.121	Has training focused on IEDs and WMDs appropriate to the position been provided to front-line employees at least annually?				
5.122	Do law enforcement/security department personnel at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.				
5.123	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.				
5.124	Does the agency have an established program to monitor employee training and to schedule employees for training?				
5.125	Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?				
5.126	Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?				
5.127	Does the agency have a program to regularly review and update security awareness and emergency response training materials?				

5.128 / T4	Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?				
5.129 / T1	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.				
5.130 / T1	Has the agency provided training to regional first responders (law enforcement agencies, firefighters, and emergency medical response teams) to enable them to operate in critical facilities and infrastructure?				
5.131 / T3	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?				
5.132 / T4	Has the agency implemented a program to train or orient first responders (law enforcement, firefighters, emergency medical teams) and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?				
	NATIONAL TERRORISM ADVISORY SYSTEM (NTAS)				
6.000	**Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS)**				
6.101	Does the SSP contain or reference other documents identifying incremental actions (imminent or elevated) to be implemented for a NTAS threat?				
6.102 / T2	Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?				
6.103	Has the agency provided annual training and/or instruction focused on job function regarding the incremental activities to be performed by employees?				
	PUBLIC AWARENESS				
7.000	**Implement and reinforce a Public Security and Emergency Awareness program**				

7.101	Has the transit agency developed and implemented a public security and emergency awareness program?				
7.102 / T6	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)?				
7.103 / T6	Is the above consistent with agency's overall announcement program?				
7.104 / T6	Are general security awareness and emergency preparedness messages included in public announcement messages at stations and on board vehicles?				
7.105 / T6	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.				
7.106 / T6	Does the agency have an appropriate mechanism in place for passengers to communicate an (e.g., 1-800 number, smart phone applications, social media, etc.) that can be called or used to report security concerns? If so, is this information indicated in public awareness materials and messages?				
7.107	Does the agency issue public service announcements or press releases to social media (e.g. Twitter/ Facebook/etc., QRC codes, and/or apps for smart phones) regarding security and emergency protocols?				
7.108 / T6	Does the agency issue public service announcements or press releases to local media (e.g. newspaper, radio and/or television) regarding security or emergency protocols?				
7.109	Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response?				

7.110	Does the transit agency conduct an outreach program to enlist members of the public as security awareness volunteers, similar to Neighborhood Watch programs?				
7.111 / T1	Do public awareness materials and/or messages inform passengers on the means to evacuate safely from transit vehicles and underwater/underground facilities?				
7.112	Does the agency track and monitor customer complaints reported by passengers?				

	RISK MANAGEMENT				
8.000	Establish and use a risk management process				
8.101 / T2	Does the agency have a risk assessment process approved by its management, for managing threats and vulnerabilities? If so, summarize the process in the justification.				
8.102	Has the agency identified facilities and systems it considers to be its critical assets?				
8.103 / T2	Has the agency had an internal or external vulnerability assessment on its critical assets within the past 3 years? Specify the dates of the most recent assessments and the entity(ies) that conducted the assessment(s).				
8.104 / T1	Has the agency had an internal or external Risk Assessment, analyzing threat, vulnerability, & 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?				
8.105 / T2	Has the system implemented procedures to limit and monitor authorized access to underground and underwater tunnels? If so, summarize procedures in the justification.				
8.106	Are security investments prioritized using information developed in the risk assessment process?				
8.107 / T1	Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and related documents?				
	ESTABLISH A RISK ASSESSMENT AND INFORMATION SHARING PROCESS				
9.000	**Establish and use an information sharing process for threat and intelligence information.**				
9.101	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?				

9.102 / T2	Does the system report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?				
9.103 / T2	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)?				
9.104	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?				
9.105	Does the agency report their NTA security data to FTA as required by 49 CFR 659?				

	DRILLS AND EXERCISES				
10.000	**Conduct Tabletop and Functional Drills**				
10.101	Does the agency's System Safety Program Plan (SSPP) contain or reference a document describing the process used by the agency to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills?				
10.102	Does the agency's SSPP or SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?				
10.103 / T5	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.				
10.104	Does the agency's SSPP or a related document include a requirement for annual field exercises, tabletops and drills?				
10.105	Does the agency's SSPP 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)?				
10.106	Does the agency's SSPP or a related document describe or reference its program for providing employee training on emergency response protocols and procedures?				
10.107	Does the agency participate as an active player in full-scale, regional exercises held at least annually?				
10.108 / T5	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)?				
10.109 / T5	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?				

10.110 / T5	In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings and corrective actions? If so, summarize the actions taken in the justification.				
10.111	Has the agency established metrics to assess its performance during emergency exercises and to measure improvements?				
10.112 / T1	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 in underwater/underground infrastructure and other critical systems?				
10.113 / T5	Does the transit system integrate local and regional first responders (law enforcement, firefighters, emergency medical teams) in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place.				
11.000	**Developing a Comprehensive Cyber Security Strategy**				
11.101	Has the agency conducted a risk assessment to identify operational control and communication/business enterprise IT assets and potential vulnerabilities?				
11.102	Has the agency implemented protocols to ensure that all IT facilities (e.g., data centers, server rooms, etc.) and equipment are properly secured to guard against internal or external threats or attacks?				
11.103	Has a written strategy been developed and integrated into the overall security program to mitigate the cyber risk identified?				
11.104	Does the agency have a designated representative to secure the internal network through appropriate access controls for employees, a strong authentication (i.e., password) policy, encrypting sensitive data, and employing network security infrastructure (example: firewalls, intrusion detection systems, IT security audits, antivirus, etc.)?				
11.105	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?				

11.106	Has the agency established a cyber-incident response and reporting protocol?				
11.107	Is the agency aware of and using available resources (e.g., standards, PT-ISAC, US CERT, National Cyber Security Communication and Integration Center, etc.)?				

	FACILITY SECURITY AND ACCESS CONTROLS				
12.000	**Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors**				
12.101	Have assets and facilities requiring restricted access been identified?				
12.102	Are ID badges or other measures employed to restrict access to facilities not open to the public?				
12.103 / T2	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.)?				
12.104	Does the agency have procedures to issue ID badges for visitors and contractors?				
12.105	Does the agency require escorts for visitors accessing non-public areas?				
12.106	Is CCTV equipment installed in transit agency facilities?				
12.107	Is CCTV equipment protecting critical assets interfaced with an access control system?				
12.108	Is CCTV equipment installed on transit vehicles?				

12.109	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?				
12.110	Based on the risk assessment, does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?				
12.111 / T2	Has the system implemented protective measures to secure high risk/high consequence assets and systems identified in risk assessments? Examples of protective measures include but are not limited to CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems. If protective measures for this infrastructure are employed, summarize type and location in in the justification.				
12.112	Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?				
12.113	Are emergency call boxes provided for passengers?				
12.114	Do transit agency personnel administer an automated employee access control system and perform corrective analysis of security breaches?				
12.115	Does the agency have policies and procedures for screening of mail and/or outside deliveries?				
12.116	Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?				
12.117	Does the agency use National Fire Protection Association (NFPA) Standard 130 or equivalent to evaluate fire/life safety in station design or modification (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)?				

12.118	Is directional signage with adequate lighting provided in a consistent manner in all stations, both to provide orientation and to support emergency evacuation?				
12.119	Are gates and locks used on all facility doors to prevent unauthorized access?				
12.120	Are keys controlled through an established program managed by the security/police function?				
12.121	Are gates and locks also used to close down system facilities after operating hours?				
12.122	Do transit vehicles have radios, silent alarms, and/or passenger communication systems?				
12.123	Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?				
12.124	Are Uninterruptible Power Supply (UPS) or redundant power sources provided for safety and security of critical equipment, such as but not limited to: exit and platform lighting; parking lot lighting; ancillary space and shop lighting; intrusion detection (alarmed rooms and spaces, fare collection equipment, etc.); fire detection, alarm and suppression systems; public address (shop and public areas); call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?				
12.125	At passenger stations at which a vulnerability assessment has identified a significant risk, and to the extent practicable, has the owner/operator removed trash receptacles and other non-essential receptacles or containers (with the exception of bomb resistant receptacles or clear plastic containers) from the platform areas of passenger terminals and stations?				

12.126	Does the agency employ specific protective measures for all critical infrastructure (e.g., tunnels, bridges, stations, control centers, etc) identified through the risk assessment particularly at access points and ventilation infrastructure in place and maintained in optimal condition? Examples of protective measures include, but are not limited to, CCTV, intrusion detection systems, smart camera technology, fencing, lighting, access control, law enforcement patrols, canine patrols, physical protection for ventilation systems. If protective measures for this infrastructure are employed, summarize type and location in the justification.				
12.127 / T1	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available from other law enforcement agencies? If so, has the system implemented procedures for reporting of and response to positive reactions by the canine?				
13.000	**Conduct Physical Security Inspections**				
13.101 / T1	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?				
13.102	Has the transit agency established procedures for inspecting/sweeping vehicles and stations to identify and manage suspicious items, based on HOT characteristics (hidden, obviously suspicious, not typical) or equivalent system?				
13.103	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?				
13.104	Has the transit agency developed a form or quick reference guide for station attendants and others regarding station and facility inspections?				
13.105 / T2	Does the system document the results of inspections and implement any changes to policies and procedures or implement corrective actions, based on the findings?				
13.106 / T2	Does the agency conduct frequent inspections of access points, ventilation systems, and the interior of underground/underwater assets and systems for indications of suspicious activity?				

13.107	Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect?				
13.108	Is there a process in place, with necessary training provided to personnel, to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.				
13.109	Is there a process in place, with necessary training provided to personnel, to ensure that all critical infrastructure are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.				
	BACKGROUND INVESTIGATIONS				
14.000	**Conduct Background Investigations of Employees and Contra**				
14.101 / T2	Does the agency conduct background investigations (i.e., criminal history and motor vehicle records) on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems?				
14.102 / T2	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?				
14.103	Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?				
14.104	Is the background investigation process documented?				
14.105	Is the criteria for background investigations based on employee type (senior management staff, law enforcement officers, managers/supervisors, operators, maintenance, safety/security sensitive, contractor, etc.) and/or responsibility and access documented?				

	DOCUMENT CONTROL				
15.000	**Control Access to documents of security critical systems and facilities**				
15.101 / T2	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?				
15.102	Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?				
15.103	Does the security review committee (or other designated group) review document control practices, assess compliance applicable procedures, and identify discrepancies and necessary corrective action?				
16.000	**Process for handling and access to Sensitive Security Information (SSI)**				
16.101	Does the agency have a documented policy for identifying and controlling the distribution of and access to documents it considers to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520?				
16.102	Does the agency have a documented policy for proper handling, control, and storage of documents labeled as or otherwise determined to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520?				
16.103	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?				
16.104	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)?				
	SECURITY PROGRAM AUDITS				
17.000	**Audit Program**				
17.101	Has the agency established a schedule for conducting its internal security audit process?				

17.102	Does the SSP contain a description of the process used by the agency to audit its implementation of the SSP over the course of the agency's published schedule?				
17.103	Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process?				
17.104	Is the transit agency complying with its internal security audit schedule?				
17.105	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?				
17.106	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?				
17.107	Does the transit agency's internal security audit process ensure that auditors are independent from those responsible for the activity being audited?				
17.108	Has the agency made its internal security audit schedule available to the SSO agency?				
17.109	Has the agency made checklists and procedures used in its internal security audits available to the SSO agency?				
17.110	Has the agency notified the SSO agency 30 days prior to the conduct of an internal security audit?				
17.111	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?				
17.112	Has the agency's chief executive certified to the SSO agency that the agency is in compliance with its SSP?				
17.113	Was that certification included with the most recent annual report submitted to the SSO agency?				
17.114	If the agency's chief executive was not able to certify to the SSO agency that the agency is in compliance with its SSP, was a corrective action plan developed and made available to the SSO?				

Number of items requiring Options for Consideration	**0**

Date of Visit	TSA Field Office	Lead TSI Inspector
12/30/1899	0	0

Agency Name
0

Additional Information
General Description of the Entity: INSPECTOR SHALL PROVIDE A GENERAL NARRATIVE OVERVIEW OF THE ENTITY'S SCOPE OF OPERATIONS, FACILITIES, ETC.:
Other information obtained during BASE assessment:
Smart Practice Information:
Did you observe anything significant or "cutting edge" in the area of corporate/facility security?
1. List the infrastructure and assets identified as critical by the agency:
a.
b.
c.
d.
e.
f.
g.
2. Where do you, as an industry, feel vulnerable?
a.
b.
3. What concerns do you have?
a.
b.
4. In what Federal programs or security initiatives does your company participate?
a.
b.
c.

BASE Technical Scoring Sheet **This sheet is for data analysis only.**

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
1.000			Establish Written System Security Plans (SSPs) and Emergency Response Plans (ERPs)				0.0000000	0.0585640	0%
1.100			System Security Plan (SSP)				0.0000000	0.0284720	0%
1.101	B		Does the transit agency have a System Security Plan (SSP)?	0	0.000472	1	0	0.001888	0%
1.102			Does the SSP identify the goals and objectives for the security program?	0	0.000465	1	0	0.001860	0%
1.103	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, including the agency's chief executive?	0	0.000466	1	0	0.001864	0%
1.104	B		Is the SSP separate from the agency's System Safety Program Plan (SSPP)?	0	0.000385	1	0	0.001540	0%
1.105	B	T1	Do the Security and Emergency Response Plans address protection and response for critical underwater tunnels, underground stations/ tunnels and other critical systems, where applicable?	0	0.000459	1	0	0.001836	0%
1.106			Does the SSP contain or reference other documents establishing procedures for the management of security incidents by the operations control center (or dispatch center)?	0	0.000445	1	0	0.001780	0%
1.107	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.)?	0	0.000450	1	0	0.001800	0%
1.108			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)?	0	0.000463	1	0	0.001852	0%
1.109		T3	Are visible, random security measures integrated into security plans to introduce unpredictability into security activities for deterrent effect?	0	0.000454	1	0	0.001816	0%
1.110			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?	0	0.000465	1	0	0.001860	0%
1.111			Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?	0	0.000454	1	0	0.001816	0%
1.112			Does the SSP require an annual review?	0	0.000449	1	0	0.001796	0%
1.113			Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?	0	0.000438	1	0	0.001752	0%
1.114			Has an annual review of the SSP been performed and documented in the preceding 12 months?	0	0.000447	1	0	0.001788	0%
1.115			Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP?	0	0.000400	1	0	0.001600	0%
1.116			Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?	0	0.000406	1	0	0.001624	0%
1.200			Emergency Response Plan (ERP)				0.00000	0.03009	0%
1.201	B		Does the transit agency have an Emergency Response Plan (ERP)?	0	0.000652	1	0	0.002608	0%
1.202	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, including the agency's chief executive?	0	0.000643	1	0	0.002572	0%
1.203	B		Does the ERP require an annual review to determine if it needs to be updated?	0	0.000631	1	0	0.002524	0%
1.204			Has an annual review of the ERP been performed and documented in the preceding 12 months?	0	0.000631	1	0	0.002524	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		0%		0%		0%		0%		0%		0%
	Points	Possible	Points	Possible	Points	Possible	Points	Possible	Points	Possible	Points	Possible
Totals:	0	0.03954964	0	0.123912	0	0.00373898	0	0.02809735	0	0.0315	0	0.02622518
1.101												
1.102												
1.103												
1.104												
1.105	0	0.001836										
1.106												
1.107												
1.108												
1.109					0	0.001816						
1.110												
1.111												
1.112												
1.113												
1.114												
1.115												
1.116												
1.200												
1.201												
1.202												
1.203												
1.204												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		0%
	0.000000	0.026592
Totals:	0.000000	0.008928
1.101	0.000000	0.001888
1.102		
1.103	0.000000	0.001864
1.104	0.000000	0.001540
1.105	0.000000	0.001836
1.106		
1.107	0.000000	0.001800
1.108		
1.109		
1.110		
1.111		
1.112		
1.113		
1.114		
1.115		
1.116		
1.200	0.000000	0.017664
1.201	0.000000	0.002608
1.202	0.000000	0.002572
1.203	0.000000	0.002524
1.204		

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
1.205	B		Does the ERP include a process or review provision to ensure coordination with the rail transit agency's SSPP and SSP?	0	0.000612	1	0	0.002448	0%
1.206			Has the transit agency received documentation from the SSO confirming its review and approval of the ERP currently in effect?	0	0.000585	1	0	0.002340	0%
1.207	B		Does the ERP contain or reference other documents establishing plans, procedures, or protocols for responding to emergency events with external agencies (such as law enforcement, local EMA, fire departments, etc.)?	0	0.000629	1	0	0.002516	0%
1.208	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)?	0	0.000623	1	0	0.002492	0%
1.209			Does the ERP contain or reference other documents to provide for Continuity of Operations (COOP) while responding to emergency events?	0	0.000634	1	0	0.002536	0%
1.210			Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event?	0	0.000628	1	0	0.002512	0%
1.211			Does the agency have a written Business Continuity Plan and COOP to guide restoration of facilities and services following an emergency event?	0	0.000629	1	0	0.002516	0%
1.212	B		Does the agency have a back-up operations control center capability?	0	0.000626	1	0	0.002504	0%
2.000			**Define Roles and Responsibilities for Security and Emergency Management**				0	0.056136	0%
2.100			**System Security Plan (SSP)**				0	0.029456	0%
2.101			Does the SSP establish and assign responsibility for implementation of the security program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?	0	0.000761	1	0	0.003044	0%
2.102			Has the agency established lines of delegated authority/succession of security responsibilities and, if so, has that information been distributed to agency managers?	0	0.000730	1	0	0.002920	0%
2.103	B		Are roles and responsibilities for security and/or law enforcement personnel assigned by title and/or position established in the SSP or other documents?	0	0.000744	1	0	0.002976	0%
2.104	B		Are security-related roles and responsibilities for non-security and/or law enforcement personnel (i.e., operators, conductors, maintenance workers and station attendants) established in the SSP or other documents?	0	0.000731	1	0	0.002924	0%
2.105		T2	Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes?	0	0.000727	1	0	0.002908	0%
2.106			Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings?	0	0.000718	1	0	0.002872	0%
2.107	B		Are informational briefings with appropriate personnel held whenever security protocols, threat levels, or protective measures are updated or as security conditions warrant?	0	0.000757	1	0	0.003028	0%
2.108	B		Have appropriate reference guides or other written instructions or procedures been distributed to transit employees to implement the requirements of the SSP?	0	0.000694	1	0	0.002776	0%
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?	0	0.000758	1	0	0.003032	0%
2.11			Does the agency maintain a record of security related incidents that are reported within the agency?	0	0.000744	1	0	0.002976	0%
2.200			**2.b. Emergency Response Plan (ERP):**				0.00000	0.02668	0%
2.201			Does the ERP 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?	0	0.000980	1	0	0.003920	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
1.205												
1.206												
1.207												
1.208												
1.209												
1.210												
1.211												
1.212												
2												
2.100												
2.101												
2.102												
2.103												
2.104												
2.105			0	0.002908								
2.106												
2.107												
2.108												
2.109												
2.11												
2.200												
2.201												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
1.205	0.000000	0.002448
1.206		
1.207	0.000000	0.002516
1.208	0.000000	0.002492
1.209		
1.210		
	0.000000	0.002504
2	0	0.033776
2.100	0.000000	0.014736
2.101		
2.102		
2.103	0.000000	0.002976
2.104	0.000000	0.002924
2.105		
2.106		
2.107	0.000000	0.003028
2.108	0.000000	0.002776
2.109	0.000000	0.003032
2.200	0.000000	0.019040
2.201		

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
2.202	B		Are emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?	0	0.000950	1	0	0.003800	0%
2.203	B	T5	Are roles and responsibilities for front-line personnel (i.e. system law enforcement, system security officials, train or vehicle operators, conductors, station attendants, maintenance workers) described in the system's Emergency Response Plan (ERP)?	0	0.000950	1	0	0.003800	0%
2.204	B		Has the ERP been distributed to appropriate departments in the organization?	0	0.000960	1	0	0.003840	0%
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?	0	0.000950	1	0	0.003800	0%
2.206			Are senior staff and middle management ERP coordination meetings held on a regular basis?	0	0.000930	1	0	0.003720	0%
2.207	B		Are informational briefings with appropriate personnel held whenever emergency response protocols are substantially changed or updated?	0	0.000950	1	0	0.003800	0%
3.000			**Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control**				0.0000	0.0580	0%
3.101	B		Do managers and supervisors routinely provide information to front-line personnel regarding security and emergency response issues?	0	0.003700	1	0	0.014800	0%
3.102			Are regular supervisor, manager, and/or foreperson security review and coordination briefings held? If so, detail frequency and subjects covered in the justification.	0	0.003600	1	0	0.014400	0%
3.103	B		Does the agency have a program for confirming that personnel have a working knowledge of security protocols? If so, summarize program in the justification.	0	0.003600	1	0	0.014400	0%
3.104	B		Are managers and/or supervisors required to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?	0	0.003600	1	0	0.014400	0%
4.000			**Coordinate Security and Emergency Management Plan(s) with local and regional agencies**				0.0000	0.0584	0%
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?	0	0.001331	1	0	0.005324	0%
4.102	B		Does the agency participate in a regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and response?	0	0.001336	1	0	0.005344	0%
4.103	B		Have regional incident management protocols been shared with the agency and incorporated into the agency's ERP/SSP/SEPP?	0	0.001293	1	0	0.005172	0%
4.104			Have agency resources been appropriately identified and provided to the regional EMA?	0	0.001263	1	0	0.005052	0%
4.105	B		Does the agency have a designated point-of-contact or liaison with the local/regional Emergency Operations Center (EOC)?	0	0.001394	1	0	0.005576	0%
4.106			Does the agency send a representative to the local/regional EOC, should it be activated?	0	0.001347	1	0	0.005388	0%
4.107			Does the agency have information sharing capabilities with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?	0	0.001343	1	0	0.005372	0%
4.108	B		Has the agency developed internal incident management protocols that comply with the National Response Plan and the National Incident Management System (NIMS)?	0	0.001314	1	0	0.005256	0%
4.109			Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?	0	0.001286	1	0	0.005144	0%
4.110	B	T5	Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?	0	0.001325	1	0	0.005300	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
2.202												
2.203									0	0.0038		
2.204												
2.205												
2.206												
2.207												
3.000												
3.101												
3.102												
3.103												
3.104												
4.000												
4.101												
4.102												
4.103												
4.104												
4.105												
4.106												
4.107												
4.108												
4.109												
4.110									0	0.0053		

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
2.202	0.000000	0.003800
2.203	0.000000	0.003800
2.204	0.000000	0.003840
2.205	0.000000	0.003800
2.206		
2.207	0.000000	0.003800
3.000	0.000000	0.043600
3.101	0.000000	0.014800
3.102		
3.103	0.000000	0.014400
3.104	0.000000	0.014400
4.000	0.000000	0.032136
4.101		
4.102	0.000000	0.005344
4.103	0.000000	0.005172
4.104		
4.105	0.000000	0.005576
4.106		
4.107		
4.108	0.000000	0.005256
4.109		
4.110	0.000000	0.005300

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
4.111	B		If the agency's communications systems are NOT inter-operable with appropriate emergency response agencies, have alternate communication protocols been established? Describe the alternate communication protocols in the justification.	0	0.001372	1	0	0.005488	0%
			SECURITY AND EMERGENCY RESPONSE TRAINING						
5.000			**Establish and Maintain a Security and Emergency Training Program**				0.0000	0.0597	0%
5.101	B	T4	Is initial training provided to all new agency employees regarding security orientation/awareness?	0	0.000488	1	0	0.001952	0%
5.102		T4	Is annual refresher training provided regarding security orientation/awareness to Senior Management staff, managers and supervisors?	0	0.000473	1	0	0.001893	0%
5.103	B	T4	Is annual refresher training provided regarding security orientation/awareness to managers and supervisors?	0	0.000476	1	0	0.001902	0%
5.104	B	T4	Is annual refresher training provided regarding security orientation/awareness to front-line employees?	0	0.000472	1	0	0.001890	0%
5.105			Is ongoing advanced security training focused on job function provided at least annually?	0	0.000468	1	0	0.001872	0%
5.106	B	T4	Is initial training provided to all new transit employees regarding emergency response?	0	0.000484	1	0	0.001938	0%
5.107		T4	Is annual refresher training provided regarding emergency response to Senior Management staff, supervisors, and managers?	0	0.000472	1	0	0.001889	0%
5.108	B	T4	Is annual refresher training provided regarding emergency response to Managers and Supervisors?	0	0.000477	1	0	0.001909	0%
5.109	B	T4	Is annual refresher training provided regarding emergency response to front-line Employees?	0	0.000472	1	0	0.001889	0%
5.110	B	T4	Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System at least annually?	0	0.000462	1	0	0.001848	0%
5.111			Has ICS and NIMS training appropriate to the position been provided to Senior Management staff, supervisors, and managers at least annually?	0	0.000440	1	0	0.001761	0%
5.112	B		Has ICS and NIMS training appropriate to the position been provided to managers and supervisors at least annually?	0	0.000466	1	0	0.001862	0%
5.113			Has ICS and NIMS training appropriate to the position been provided to front-line employees at least annually?	0	0.000450	1	0	0.001799	0%
5.114	B		Has the agency developed a program and provided annual training on its own incident response protocols?	0	0.000474	1	0	0.001895	0%
5.115		T4	Has training on the agency's incident response protocols appropriate to the position been provided to Senior Management staff, managers and supervisors at least annually?	0	0.000465	1	0	0.001860	0%
5.116	B	T4	Has training on the agency's incident response protocols appropriate to the position been provided to managers and supervisors?	0	0.000471	1	0	0.001882	0%
5.117	B	T4	Has training on the agency's incident response protocols appropriate to the position been provided to front-line employees at least annually?	0	0.000468	1	0	0.001871	0%
5.118		T4	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?	0	0.000430	1	0	0.001722	0%
5.119			Has training focused on IEDs and WMDs appropriate to the position been provided to Senior Management staff, managers, and supervisors at least annually?	0	0.000460	1	0	0.001841	0%
5.120			Has training focused on IEDs and WMDs appropriate to the position been provided to manager and supervisors?	0	0.000476	1	0	0.001902	0%
5.121			Has training focused on IEDs and WMDs appropriate to the position been provided to front-line employees at least annually?	0	0.000470	1	0	0.001881	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
4.111												
5.000												
5.101							0	0.00195171				
5.102							0	0.0018925				
5.103							0	0.00190217				
5.104							0	0.00188983				
5.105												
5.106							0	0.00193796				
5.107							0	0.00188932				
5.108							0	0.0019088				
5.109							0	0.00188871				
5.110							0	0.00184816				
5.111												
5.112												
5.113												
5.114												
5.115							0	0.00185988				
5.116							0	0.00188221				
5.117							0	0.00187143				
5.118							0	0.00172182				
5.119												
5.120												
5.121												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
4.111	0.000000	0.005488
5.000	0.000000	0.029915
5.101	0.000000	0.001952
5.102		
5.103	0.000000	0.001902
5.104	0.000000	0.001890
5.105		
5.106	0.000000	0.001938
5.107		
5.108	0.000000	0.001909
5.109	0.000000	0.001889
5.110	0.000000	0.001848
5.111		
5.112	0.000000	0.001862
5.113		
5.114	0.000000	0.001895
5.115		
5.116	0.000000	0.001882
5.117	0.000000	0.001871
5.118		
5.119		
5.120		
5.121		

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
5.122			Do law enforcement/security department personnel at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.	0	0.000484	1	0	0.001936	0%
5.123			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.	0	0.000486	1	0	0.001942	0%
5.124	B		Does the agency have an established program to monitor employee training and to schedule employees for training?	0	0.000465	1	0	0.001858	0%
5.125			Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?	0	0.000461	1	0	0.001842	0%
5.126			Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?	0	0.000461	1	0	0.001845	0%
5.127			Does the agency have a program to regularly review and update security awareness and emergency response training materials?	0	0.000457	1	0	0.001829	0%
5.128	B	T4	Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?	0	0.000479	1	0	0.001916	0%
5.129	B	T1	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.	0	0.000459	1	0	0.001837	0%
5.130	B	T1	Has the agency provided training to regional first responders (law enforcement agencies, firefighters, and emergency medical response teams) to enable them to operate in critical facilities and infrastructure?	0	0.000432	1	0	0.001728	0%
5.131		T3	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?	0	0.000481	1	0	0.001923	0%
5.132	B	T4	Has the agency implemented a program to train or orient first responders (law enforcement, firefighters, emergency medical teams) and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?	0	0.000434	1	0	0.001737	0%
			HOMELAND SECURITY ADVISORY SYSTEM (HSAS)						
6.000			**Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system**				0.0000	0.0558	0%
6.101	B		Does the SSP contain or reference other documents identifying incremental actions (imminent or elevated) to be implemented for a NTAS threat?	0	0.004390	1	0	0.017560	0%
6.102	B	T2	Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?	0	0.004740	1	0	0.018960	0%
6.103			Has the agency provided annual training and/or instruction focused on job function regarding the incremental activities to be performed by employees?	0	0.004830	1	0	0.019320	0%
			PUBLIC AWARENESS						
7.000			**Implement and reinforce a Public Security and Emergency Awareness program**				0.0000	0.0528	0%
7.101	B		Has the transit agency developed and implemented a public security and emergency awareness program?	0	0.001195	1	0	0.004782	0%
7.102	B	T6	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)?	0	0.001186	1	0	0.004742	0%
7.103		T6	Is the above consistent with agency's overall announcement program?	0	0.001020	1	0	0.004079	0%
7.104	B	T6	Are general security awareness and emergency preparedness messages included in public announcement messages at stations and on board vehicles?	0	0.001065	1	0	0.004260	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
5.122												
5.123												
5.124												
5.125												
5.126												
5.127												
5.128							0	0.00191564				
5.129	0	0.001837										
5.130	0	0.001728										
5.131					0	0.00192298						
5.132							0	0.00173721				
6.000												
6.101												
6.102			0	0.01896								
6.103												
7.000												
7.101												
7.102											0	0.00474228
7.103											0	0.00407855
7.104											0	0.00426

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
5.122		
5.123		
5.124	0.000000	0.001858
5.125		
5.126		
5.127		
5.128	0.000000	0.001916
5.129	0.000000	0.001837
5.130	0.000000	0.001728
5.131		
5.132	0.000000	0.001737
6.000	0.000000	0.03652
6.101	0.000000	0.017560
6.102	0.000000	0.018960
6.103		
7.000	0.000000	0.027546
7.101	0.000000	0.004782
7.102	0.000000	0.004742
7.103		
7.104	0.000000	0.004260

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
7.105	B	T6	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.	0	0.001194	1	0	0.004774	0%
7.106	B	T6	Does the agency have an appropriate mechanism in place for passengers to communicate an (e.g., 1-800 number, smart phone applications, social media, etc.) that can be called or used to report security concerns? If so, is this information indicated in public awareness materials and messages?	0	0.001069	1	0	0.004276	0%
7.107			Does the agency issue public service announcements or press releases to social media (e.g. Twitter/ Facebook/etc., QRC codes, and/or apps for smart phones) regarding security and emergency protocols?	0	0.001039	1	0	0.004157	0%
7.108		T6	Does the agency issue public service announcements or press releases to local media (e.g. newspaper, radio and/or television) regarding security or emergency protocols?	0	0.001024	1	0	0.004094	0%
7.109			Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response?	0	0.001090	1	0	0.004362	0%
7.110			Does the transit agency conduct an outreach program to enlist members of the public as security awareness volunteers, similar to Neighborhood Watch programs?	0	0.001089	1	0	0.004356	0%
7.111	B	T1	Do public awareness materials and/or messages inform passengers on the means to evacuate safely from transit vehicles and underwater/underground facilities?	0	0.001178	1	0	0.004712	0%
7.112			Does the agency track and monitor customer complaints reported by passengers?	0	0.001042	1	0	0.004169	0%
			RISK MANAGEMENT						
8.000			Establish and use a risk management process				0.0000	0.0492	0%
8.101	B	T2	Does the agency have a risk assessment process approved by its management, for managing threats and vulnerabilities? If so, summarize the process in the justification.	0	0.001800	1	0	0.007200	0%
8.102	B		Has the agency identified facilities and systems it considers to be its critical assets?	0	0.001790	1	0	0.007160	0%
8.103	B	T2	Has the agency had an internal or external vulnerability assessment on its critical assets within the past 3 years? Specify the dates of the most recent assessments and the entity(ies) that conducted the assessment(s).	0	0.001750	1	0	0.007000	0%
8.104	B	T1	Has the agency had an internal or external Risk Assessment, analyzing threat, vulnerability, & 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?	0	0.001770	1	0	0.007080	0%
8.105	B	T2	Has the system implemented procedures to limit and monitor authorized access to underground and underwater tunnels? If so, summarize procedures in the justification.	0	0.001720	1	0	0.006880	0%
8.106			Are security investments prioritized using information developed in the risk assessment process?	0	0.001740	1	0	0.006960	0%
8.107	B	T1	Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and related documents?	0	0.001740	1	0	0.006960	0%
			ESTABLISH A RISK ASSESSMENT AND INFORMATION SHARING PROCESS						
9.000			**Establish and use an information sharing process for threat and intelligence information.**				0.0000	0.0387	0%
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?	0	0.002010	1	0	0.008040	0%
9.102	B	T2	Does the system report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?	0	0.001950	1	0	0.007800	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
7.105											0	0.00477414
7.106											0	0.00427588
7.107												
7.108											0	0.00409433
7.109												
7.110												
7.111	0	0.004712										
7.112												
8.000												
8.101			0	0.0072								
8.102												
8.103			0	0.007								
8.104	0	0.007080										
8.105			0	0.00688								
8.106												
8.107	0	0.006960										
9.000												
9.101												
9.102			0	0.0078								

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
7.105	0.000000	0.004774
7.106	0.000000	0.004276
7.107		
7.108		
7.109		
7.110		
7.111	0.000000	0.004712
7.112		
8.000	0.000000	0.042280
8.101	0.000000	0.007200
8.102	0.000000	0.007160
8.103	0.000000	0.007000
8.104	0.000000	0.007080
8.105	0.000000	0.006880
8.106		
8.107	0.000000	0.006960
9.000	0.000000	0.023680
9.101	0.000000	0.008040
9.102	0.000000	0.007800

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
9.103	B	T2	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)?	0	0.001960	1	0	0.007840	0%
9.104			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?	0	0.001860	1	0	0.007440	0%
9.105			Does the agency report their NTA security data to FTA as required by 49 CFR 659?	0	0.001900	1	0	0.007600	0%
			DRILLS AND EXERCISES						
10.000			**Conduct Tabletop and Functional Drills**				0.0000	0.0578	0%
10.101	B		Does the agency's System Safety Program Plan (SSPP) contain or reference a document describing the process used by the agency to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills?	0	0.001160	1	0	0.004640	0%
10.102	B		Does the agency's SSPP or SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?	0	0.001140	1	0	0.004560	0%
10.103	B	T5	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.	0	0.001170	1	0	0.004680	0%
10.104	B		Does the agency's SSPP or a related document include a requirement for annual field exercises, tabletops and drills?	0	0.001000	1	0	0.004000	0%
10.105	B		Does the agency's SSPP 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)?	0	0.001140	1	0	0.004560	0%
10.106			Does the agency's SSPP or a related document describe or reference its program for providing employee training on emergency response protocols and procedures?	0	0.001130	1	0	0.004520	0%
10.107	B		Does the agency participate as an active player in full-scale, regional exercises held at least annually?	0	0.001010	1	0	0.004040	0%
10.108		T5	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)?	0	0.000990	1	0	0.003960	0%
10.109		T5	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?	0	0.001110	1	0	0.004440	0%
10.110		T5	In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings and corrective actions? If so, summarize the actions taken in the justification.	0	0.001160	1	0	0.004640	0%
10.111			Has the agency established metrics to assess its performance during emergency exercises and to measure improvements?	0	0.001130	1	0	0.004520	0%
10.112	B	T1	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 in underwater/underground infrastructure and other critical systems?	0	0.001140	1	0	0.004560	0%
10.113	B	T5	Does the transit system integrate local and regional first responders (law enforcement, firefighters, emergency medical teams) in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place.	0	0.001170	1	0	0.004680	0%
11.000			**Developing a Comprehensive Cyber Security Strategy**				0.0000	0.0600	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
9.103			0	0.00784								
9.104												
9.105												
10.000												
10.101												
10.102												
10.103									0	0.00468		
10.104												
10.105												
10.106												
10.107												
10.108									0	0.00396		
10.109									0	0.00444		
10.110									0	0.00464		
10.111												
10.112	0	0.004560										
10.113									0	0.00468		
11.000												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
9.103	0.000000	0.007840
9.104		
9.105		
10.000	0.000000	0.035720
10.101	0.000000	0.004640
10.102	0.000000	0.004560
10.103	0.000000	0.004680
10.104	0.000000	0.004000
10.105	0.000000	0.004560
10.106		
10.107	0.000000	0.004040
10.108		
10.109		
10.110		
10.111		
10.112	0.000000	0.004560
10.113	0.000000	0.004680
11.000	0.000000	0.017040

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
11.101	B		Has the agency conducted a risk assessment to identify operational control and communication/business enterprise IT assets and potential vulnerabilities?	0	0.002137	1	0	0.008548	0%
11.102			Has the agency implemented protocols to ensure that all IT facilities (e.g., data centers, server rooms, etc.) and equipment are properly secured to guard against internal or external threats or attacks?	0	0.002186	1	0	0.008744	0%
11.103			Has a written strategy been developed and integrated into the overall security program to mitigate the cyber risk identified?	0	0.002108	1	0	0.008432	0%
11.104			Does the agency have a designated representative to secure the internal network through appropriate access controls for employees, a strong authentication (i.e., password) policy, encrypting sensitive data, and employing network security infrastructure (example: firewalls, intrusion detection systems, IT security audits, antivirus, etc.)?	0	0.002166	1	0	0.008664	0%
11.105			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?	0	0.002123	1	0	0.008492	0%
11.106	B		Has the agency established a cyber-incident response and reporting protocol?	0	0.002123	1	0	0.008492	0%
11.107			Is the agency aware of and using available resources (e.g., standards, PT-ISAC, US CERT, National Cyber Security Communication and Integration Center, etc.)?	0	0.002148	1	0	0.008592	0%
			FACILITY SECURITY AND ACCESS CONTROLS						
12.000			**Control Access to Security Critical Facilities with ID badges for all visitors, employees and contractors**				0.0000	0.0565	0%
12.101	B		Have assets and facilities requiring restricted access been identified?	0	0.000549	1	0	0.002196	0%
12.102	B		Are ID badges or other measures employed to restrict access to facilities not open to the public?	0	0.000541	1	0	0.002164	0%
12.103	B	T2	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.)?	0	0.000541	1	0	0.002164	0%
12.104	B		Does the agency have procedures to issue ID badges for visitors and contractors?	0	0.000543	1	0	0.002172	0%
12.105			Does the agency require escorts for visitors accessing non-public areas?	0	0.000541	1	0	0.002164	0%
12.106			Is CCTV equipment installed in transit agency facilities?	0	0.000541	1	0	0.002164	0%
12.107			Is CCTV equipment protecting critical assets interfaced with an access control system?	0	0.000539	1	0	0.002156	0%
12.108			Is CCTV equipment installed on transit vehicles?	0	0.000487	1	0	0.001948	0%
12.109			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?	0	0.000532	1	0	0.002128	0%
12.110			Based on the risk assessment, does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?	0	0.000532	1	0	0.002128	0%
12.111	B	T2	Has the system implemented protective measures to secure high risk/high consequence assets and systems identified in risk assessments? Examples of protective measures include but are not limited to CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems. If protective measures for this infrastructure are employed, summarize type and location in in the justification.	0	0.000540	1	0	0.002160	0%
12.112			Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?	0	0.000528	1	0	0.002112	0%
12.113			Are emergency call boxes provided for passengers?	0	0.000481	1	0	0.001924	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
11.101												
11.102												
11.103												
11.104												
11.105												
11.106												
11.107												
12.000												
12.101												
12.102												
12.103			0	0.002164								
12.104												
12.105												
12.106												
12.107												
12.108												
12.109												
12.110												
12.111			0	0.00216								
12.112												
12.113												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
11.101	0.000000	0.008548
11.102		
11.103		
11.104		
11.105		
11.106	0.000000	0.008492
11.107		
12.000	0.000000	0.017332
12.101	0.000000	0.002196
12.102	0.000000	0.002164
12.103	0.000000	0.002164
12.104	0.000000	0.002172
12.105		
12.106		
12.107		
12.108		
12.109		
12.110		
12.111	0.000000	0.002160
12.112		
12.113		

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
12.114			Do transit agency personnel administer an automated employee access control system and perform corrective analysis of security breaches?	0	0.000540	1	0	0.002160	0%
12.115			Does the agency have policies and procedures for screening of mail and/or outside deliveries?	0	0.000508	1	0	0.002032	0%
12.116			Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?	0	0.000525	1	0	0.002100	0%
12.117			Does the agency use National Fire Protection Association (NFPA) Standard 130 or equivalent to evaluate fire/life safety in station design or modification (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)?	0	0.000499	1	0	0.001996	0%
12.118			Is directional signage with adequate lighting provided in a consistent manner in all stations, both to provide orientation and to support emergency evacuation?	0	0.000532	1	0	0.002128	0%
12.119			Are gates and locks used on all facility doors to prevent unauthorized access?	0	0.000539	1	0	0.002156	0%
12.120			Are keys controlled through an established program managed by the security/police function?	0	0.000531	1	0	0.002124	0%
12.121	B		Are gates and locks also used to close down system facilities after operating hours?	0	0.000540	1	0	0.002160	0%
12.122			Do transit vehicles have radios, silent alarms, and/or passenger communication systems?	0	0.000526	1	0	0.002104	0%
12.123			Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?	0	0.000403	1	0	0.001612	0%
12.124	B		Are Uninterruptible Power Supply (UPS) or redundant power sources provided for safety and security of critical equipment, such as but not limited to: exit and platform lighting; parking lot lighting; ancillary space and shop lighting; intrusion detection (alarmed rooms and spaces, fare collection equipment, etc.); fire detection, alarm and suppression systems; public address (shop and public areas); call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?	0	0.000538	1	0	0.002152	0%
12.125			At passenger stations at which a vulnerability assessment has identified a significant risk, and to the extent practicable, has the owner/operator removed trash receptacles and other non-essential receptacles or containers (with the exception of bomb resistant receptacles or clear plastic containers) from the platform areas of passenger terminals and stations?	0	0.000467	1	0	0.001868	0%
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 in place and maintained in optimal condition? Examples of protective measures include, but are not limited to, CCTV, intrusion detection systems, smart camera technology, fencing, lighting, access control, law enforcement patrols, canine patrols, physical protection for ventilation systems. If protective measures for this infrastructure are employed, summarize type and location in the justification.	0	0.000541	1	0	0.002164	0%
12.127		T1	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available from other law enforcement agencies? If so, has the system implemented procedures for reporting of and response to positive reactions by the canine?	0	0.000529	1	0	0.002116	0%
13.000			**Conduct Physical Security Inspections**				0.0000	0.0626	0%
13.101	B	T1	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?	0	0.002180	1	0	0.008720	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
12.114												
12.115												
12.116												
12.117												
12.118												
12.119												
12.120												
12.121												
12.122												
12.123												
12.124												
12.125												
12.126												
12.127	0	0.002116										
13.000												
13.101	0	0.008720										

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
12.114		
12.115		
12.116		
12.117		
12.118		
12.119		
12.120		
12.121	0.000000	0.002160
12.122		
12.123		
12.124	0.000000	0.002152
12.125		
12.126	0.000000	0.002164
12.127		
13.000	0	0.02588
13.101	0.000000	0.008720

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
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?	0	0.002150	1	0	0.008600	0%
13.103			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?	0	0.002050	1	0	0.008200	0%
13.104			Has the transit agency developed a form or quick reference guide for station attendants and others regarding station and facility inspections?	0	0.001860	1	0	0.007440	0%
13.105		T2	Does the system document the results of inspections and implement any changes to policies and procedures or implement corrective actions, based on the findings?	0	0.002080	1	0	0.008320	0%
13.106	B	T2	Does the agency conduct frequent inspections of access points, ventilation systems, and the interior of underground/underwater assets and systems for indications of suspicious activity?	0	0.002140	1	0	0.008560	0%
13.107			Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect?	0	0.002140	1	0	0.008560	0%
13.108			Is there a process in place, with necessary training provided to personnel, to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.	0	0.000525	1	0	0.002100	0%
13.109			Is there a process in place, with necessary training provided to personnel, to ensure that all critical infrastructure are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.	0	0.000527	1	0	0.002108	0%
			BACKGROUND INVESTIGATIONS						
14.000			**Conduct Background Investigations of Employees and Contractors**				0.0000	0.0596	0%
14.101	B	T2	Does the agency conduct background investigations (i.e., criminal history and motor vehicle records) on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems?	0	0.003030	1	0	0.012120	0%
14.102	B	T2	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?	0	0.003000	1	0	0.012000	0%
14.103			Has counsel for the agency reviewed the process for conducting employee background investigations to confirm that procedures are consistent with applicable statutes and regulations?	0	0.002990	1	0	0.011960	0%
14.104	B		Is the background investigation process documented?	0	0.002940	1	0	0.011760	0%
14.105			Is the criteria for background investigations based on employee type (senior management staff, law enforcement officers, managers/supervisors, operators, maintenance, safety/security sensitive, contractor, etc.) and/or responsibility and access documented?	0	0.002930	1	0	0.011720	0%
			DOCUMENT CONTROL						
15.000			**Control Access to documents of security critical systems and facilities**				0.0000	0.0588	0%
15.101	B	T2	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?	0	0.005000	1	0	0.020000	0%
15.102	B		Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?	0	0.004900	1	0	0.019600	0%
15.103			Does the security review committee (or other designated group) review document control practices, assess compliance applicable procedures, and identify discrepancies and necessary corrective action?	0	0.004800	1	0	0.019200	0%
16.000			**Process for handling and access to Sensitive Security Information (SSI)**				0.0000	0.0590	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
13.102												
13.103												
13.104												
13.105			0	0.00832								
13.106			0	0.00856								
13.107												
13.108												
13.109												
14.000												
14.101			0	0.01212								
14.102			0	0.012								
14.103												
14.104												
14.105												
15.000												
15.101			0	0.02								
15.102												
15.103												
16.000												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
13.102	0.000000	0.008600
13.103		
13.104		
13.105		
13.106	0.000000	0.008560
13.107		
13.108		
13.109		
14.000	0.000000	0.035880
14.101	0.000000	0.012120
14.102	0.000000	0.012000
14.103		
14.104	0.000000	0.011760
14.105		
15.000	0.000000	0.039600
15.101	0.000000	0.020000
15.102	0.000000	0.019600
15.103		
16.000	0.000000	0.029668

Top 17 Scoring Detail

Category			Questions	Score	Weight	N/A	Points	Possible	Grade
			MANAGEMENT AND ACCOUNTABILITY						
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?	0	0.003764	1	0	0.015056	0%
16.102	B		Does the agency have a documented policy for proper handling, control, and storage of documents labeled as or otherwise determined to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15 or 1520?	0	0.003653	1	0	0.014612	0%
16.103			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?	0	0.003636	1	0	0.014544	0%
16.104			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)?	0	0.003706	1	0	0.014824	0%
			SECURITY PROGRAM AUDITS						
17.000			**Audit Program**				0.0000	0.0547	0%
17.101			Has the agency established a schedule for conducting its internal security audit process?	0	0.000895	1	0	0.003580	0%
17.102	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?	0	0.001210	1	0	0.004840	0%
17.103	B		Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process?	0	0.001209	1	0	0.004836	0%
17.104	B		Is the transit agency complying with its internal security audit schedule?	0	0.001188	1	0	0.004752	0%
17.105	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?	0	0.001204	1	0	0.004816	0%
17.106			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?	0	0.001157	1	0	0.004628	0%
17.107			Does the transit agency's internal security audit process ensure that auditors are independent from those responsible for the activity being audited?	0	0.001118	1	0	0.004472	0%
17.108			Has the agency made its internal security audit schedule available to the SSO agency?	0	0.000863	1	0	0.003452	0%
17.109			Has the agency made checklists and procedures used in its internal security audits available to the SSO agency?	0	0.000845	1	0	0.003380	0%
17.110			Has the agency notified the SSO agency 30 days prior to the conduct of an internal security audit?	0	0.000810	1	0	0.003240	0%
17.111			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?	0	0.000810	1	0	0.003240	0%
17.112			Has the agency's chief executive certified to the SSO agency that the agency is in compliance with its SSP?	0	0.000817	1	0	0.003268	0%
17.113			Was that certification included with the most recent annual report submitted to the SSO agency?	0	0.000789	1	0	0.003156	0%
17.114			If the agency's chief executive was not able to certify to the SSO agency that the agency is in compliance with its SSP, was a corrective action plan developed and made available to the SSO?	0	0.000756	1	0	0.003024	0%

Transit Security Fundamentals Scoring Detail

Line	Element 1		Element 2		Element 3		Element 4		Element 5		Element 6	
Grade:		**0%**		**0%**		**0%**		**0%**		**0%**		**0%**
16.101												
16.102												
16.103												
16.104												
17.000												
17.101												
17.102												
17.103												
17.104												
17.105												
17.106												
17.107												
17.108												
17.109												
17.110												
17.111												
17.112												
17.113												
17.114												

Baseline Security Scoring Detail

Line	Element 1	
Grade:		**0%**
16.101	0.000000	0.015056
16.102	0.000000	0.014612
16.103		
16.104		
17.000	0.000000	0.019244
17.101		
17.102	0.000000	0.004840
17.103	0.000000	0.004836
17.104	0.000000	0.004752
17.105	0.000000	0.004816
17.106		
17.107		
17.108		
17.109		
17.110		
17.111		
17.112		
17.113		
17.114		

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%

Grade
0%
0%
0%
0%
0%
0%
0%