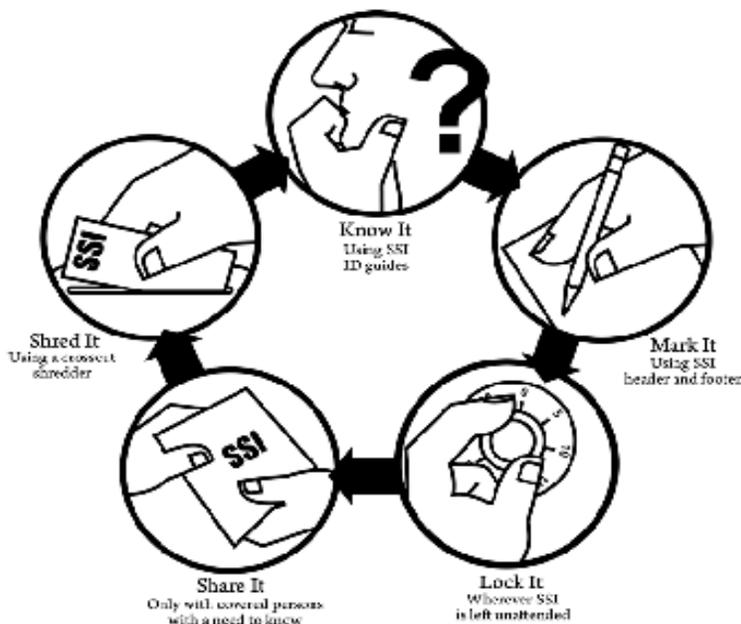


DEPARTMENT OF HOMELAND SECURITY

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

“
”

Line Element	SIDoT
1.101	Does the transit agency have a System Security Plan (SSP) which addresses personnel security, facility security, vehicle security and Threat/Vulnerability Management?
1.102	Does the SSP identify and actively monitor 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, such as the agency's chief executive?
1.104	Is the SSP separate from the agency's System Safety Program Plan (SSPP)?
1.105 TSF 1	Response Plans address protection and response for critical systems? (i.e., facilities, stations, terminals, office building, underwater tunnels, underground stations/ tunnels and
1.106	Does the SSP contain or reference other documents establishing procedures for the management of security incidents by the

	operations control center (or dispatch center) or other formal process?
1.107	other documents establishing plans, procedures, or protocols for responding to security events with external agencies (such as law enforcement, local EMA, fire
1.108	Has the agency partnered with local law enforcement/ first responders to develop Active Shooter procedures or protocols?
1.109	Does the SSP contain or reference other documents that establish procedures or protocols for responding to active shooter events?
1.110	other documents that establish protocols addressing specific threats from (i) Improvised Explosive Devices (IED) and (ii) Weapons of Mass Destruction (chemical, biological, radiological
1.111 / TSE3	Are visible, random security measures, based on employee type, integrated into security plans to introduce unpredictability into security activities for deterrent effect?
1.112	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?

1.113 Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?

1.114 Does the SSP require an annual review?

1.115 Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?

1.116 Has an annual review of the SSP been performed and documented in the preceding 12 months?

1.117 Does the SSP outline a process for securing SSO agency review and approval of updates to the

1.118 Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?

1.201 Does the transit agency have an Emergency Response Plan (ERP) which addresses specific policies and procedures related to emergency response.

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, such as 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	reference other documents establishing plans, procedures, or protocols for responding to emergency events with external agencies? (i.e. law enforcement,
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?

2.101 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 documented lines of delegated authority and lines of succession of security responsibilities?

2.103

Does the SSP or other documents establish roles and responsibilities for security and/or law enforcement personnel based on title and/or position?

2.104

Does the SSP or other documents establish security-related roles and responsibilities for non-security personnel based on title and/or position? (i.e., operators, conductors, maintenance workers and station attendants)

2.105
TSF 2

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 reference guides or other written instructions or procedures, appropriate to job function, been distributed to transit employees to implement the requirements of the SSP?

2.109

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

2.110

Does the agency maintain a record of security related incidents that are reported within the agency?

Does the ERP establish and assign responsibility for implementation of the emergency

2.201 response program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?

2.202 Are detailed, comprehensive emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?

2.203
TSF 5 Does the ERP establish emergency response roles and responsibilities for all front-line personnel based on title and/or position? (i.e. system law enforcement, system security officials, train or vehicle operators, conductors, station

attendants, maintenance workers)

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?

3.101

How frequently do managers and supervisors provide information to front-line personnel where security and emergency response issues are the primary focus?

3.102

How frequently are supervisor, manager, and/or foreperson security review and coordination briefings held?

3.103

Does the agency have a program that actively utilizes a formal process for confirming personnel have a measurable working knowledge of security protocols? (i.e. internal audits, challenge procedures, qualification testing)

3.104

Does the agency have a written policy requiring managers and/or supervisors to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?

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

regional Emergency Management Working Group or similar regional coordinating body for emergency preparedness and

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 from the local/regional Emergency Operations Center

4.106

(EOC)?
Does the agency send a representative to the

4.106 local/regional EOC, should it be activated?

4.107 Does the agency have a process for sharing information with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?

4.108 internal incident management protocols that comply with the National Response Plan and the National Incident Management

4.109 Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?

4.110 TSF 5 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.

5.101 TSF 4 Is initial training provided to all new agency employees regarding security orientation/awareness?

5.102 TSF 4	Is annual refresher training regarding security orientation/awareness provided to all employees regardless of position or job function in a formal manner?	
5.103 TSF 4	Is annual refresher training provided regarding security orientation/awareness to managers and supervisors?	
5.104 TSF 4	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	shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function?	
5.107	Is annual refresher training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function?	
5.108 TSF 4	Is initial training provided to all new transit employees regarding emergency response?	

5.109 / TSF 4	Is annual refresher training regarding emergency response provided to all employees regardless of position or job function in a formal manner?	
5.110 / T4		
5.111 / T4		
5.112 / TSF 4	Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System (NIMS)?	
5.113	Has ICS and NIMS training appropriate to the position been provided to Senior Management staff and supervisors? (Describe the frequency of training)	
5.114	Has ICS and NIMS training appropriate to the position been provided to frontline employees? (Describe the frequency of training)	
5.115	Has ICS and NIMS training appropriate to the position been provided to front-line employees at least annually?	
5.116	Has the agency developed a program and provided training on	

5.116	its own incident response protocols?	
5.117 / TSF 4	Is annual refresher training on the agency's incident response protocols appropriate to the position been provided to all employees regardless of position?	
5.118 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to managers and supervisors?	
5.119 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to front-line employees at least annually?	
5.120 / TSF 4	program for personnel regarding response to terrorism, including (i) Improvised Explosive Devices and ii) Weapons of Mass Destruction (chemical, biological, radiological, nuclear, IEDs and WMDs appropriate to the position been provided to all employees regardless of position or job function at least annually?	
5.121	Has training focused on IEDs and WMDs appropriate to the position been provided to manager and supervisors?	
5.122	Has training focused on IEDs and WMDs appropriate to the position been provided to front-line employees at least annually?	
5.123	Do law enforcement/security department personnel, security managers at the agency receive specialized training in counter-terrorism annually?	
5.124		

terrorism annually: Summarize program in the justification.
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.

5.125

Does the agency have an established program to monitor and schedule employee training?

5.126

Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?

5.127

Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?

5.128

Does the agency have a program to regularly review and update security awareness and emergency response training materials?

5.129

Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?

5.130 /
TSF 4

5.131 / TSF 1	awareness and emergency response training programs cover response and recovery operations in critical facilities and infrastructure? If so, summarize relevant provisions of program in	
5.132 / TSF 1	Has the agency provided training to regional first responders to enable them to operate in critical facilities and infrastructure? Has the agency provided local	
5.133	law enforcement/first responders opportunities to familiarize themselves with agency's system for response to Active Shooter	
5.134 / TSF 3	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures? Has the agency implemented a	first responder verification
5.135 / TSF 4	program to train or orient first responders and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?	
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 / TSF 2	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?

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

7.102 TSF 6 public outreach for security awareness and emergency preparedness (e.g., Transit Watch, "If You See Something, Say Something", message boards, brochures, channel cards, posters,

7.103 TSF 6 Is the above consistent with agency's overall announcement program?

7.104 TSF 6 Are general security awareness and emergency preparedness messages included in public announcement messages at stations and on board vehicles?

7.105 TSF 6 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
7.106 TSF 6	Does the agency have an appropriate mechanism in place for passengers to communicate a security concern? (e.g., 1-800 number, smart phone applications, social media, etc.)
7.107	releases to social media regarding security and emergency protocols? (e.g. Twitter/
7.108 TSF 6	Facebook, etc.) Does the agency conduct press releases to local media regarding security or emergency protocols? (e.g. newspaper, radio and/or
7.109	Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response? If so, describe training program and activities.
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 TSF 1	Do public awareness materials and/or messages inform passengers on the means to evacuate safely from transit vehicles and facilities?
7.112	Does the agency track and monitor customer complaints reported by passengers?
8.101 TSF 2	assessment process, approved by its management, for managing threats and vulnerabilities? If so,

summarize the process in the

8.102

Has the agency identified facilities and systems it considers to be its critical assets?

8.103
TSF 2

external vulnerability assessment on its critical assets within the past 3 years? Specify the dates of the most recent assessments and the entities that conducted

8.104
TSF 1

the 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

8.105
TSF 2

been properly trained to manage Has the system implemented procedures to limit and monitor 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
TSF 1

Upon request, has TSA been provided access to the agency vulnerability assessments, Security Plan and related

documents?

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

intelligence information directly

9.102 TSF 2	to FBI Joint Terrorism Task Force (JTTF) or other regional
9.103	Does the agency have policies requiring employees to report (internal or external) suspicious activity to their supervisor or management?
9.104 / TSF 2	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)?
9.105	threat and intelligence information directly from any Federal government agency, State Homeland Security Office, Regional or State Intelligence Fusion Center, PT-ISAC, or
9.106	other transit agencies? If so, Does the agency report their NTD security data to FTA as required by 49 CFR 659?
10.101	documented process to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and
10.102	Does the agency's or SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?
10.103 TSF 5	emergency preparedness by using annual field exercises, tabletop exercises, and/or drills? If so, please summarize the exercise

10.104	Does the agency's SPP or a related document include requirement for annual field exercises, tabletops and drills?
10.105	Does the agency documents the results of its emergency preparedness evaluations? (i.e., briefings, after action reports and information
10.106	reference its program for providing employee training on emergency response protocols
10.107	Does the agency participate as an active player in full-scale regional exercises, held at least annually?
10.108	In the last year, has the agency conducted drills or exercises specifically focus on active shooter scenarios with its employees?
10.109 / TSF 5	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
10.110 / 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
10.111 / TSF 5	and processes to incorporate after-action report recommendations/findings of corrective actions? If so,
10.112	Has the agency established a system for objectively measure and assess its performance during emergency exercises and to measure improvements?
10.113 /	emergency response plans to test capabilities of i.) employees and ii.) first responders to operate

10.113 / TSF 1	effectively throughout the agencies system? (i.e., facilities, stations, office buildings,
10.114 / TSF 5	Does the transit system integrate local and regional first responders in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place.



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	recurring cyber security training reinforces security roles, responsibilities, and duties of employees at all levels to protect

against and recognize cyber

11.106

Has the agency established a cyber-incident response and reporting protocol?

11.107

available resources (e.g., standards, PT-ISAC, US CERT National Cyber Security Communication and Integration

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

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.)?

12.104

Does the agency have documented procedures for issuing ID badges to visitors and contractors?

12.105

Does the agency has a documented policy that requires visitors to be escorted when accessing non-public areas.

12.106

Is CCTV equipment installed in transit agency facilities?

Is CCTV equipment protecting

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	Environmental Design (CPTED) and technology (e.g., CCTV, access control, intrusion detection, bollards, etc.) incorporated into design criteria
12.110	Does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified high risk/high consequence assets and critical systems? (i.e.,
12.111 TSF 2	CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE
12.112	Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?
12.113	Does the agency provide a method for passengers and visitors to report security and safety concerns from within the agency's system?
12.114	Does the transit agency 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	modifications? (including fire detection systems, firewalls and flame-resistant materials, back-up
12.118	Is directional signage with powered emergency lighting, adequate lighting provided in a consistent manner throughout their system, both to provide orientation and to support emergency evacuation?
12.119	Are gates and locks used on all facility doors to prevent unauthorized access during operating hours?
12.120	Are keys controlled through an established program that is documented?
12.121	Are gates and locks used to close down system facilities after operating hours?
12.122	Do transit vehicles have radios, silent alarms, and/or passenger communication systems?
	Does the transit agency use

12.123	Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?
12.124	Supply (UPS) or redundant power sources provided for safety and security of critical equipment, fire detection, alarm and suppression systems; public address; call-for-aid telephones; CCTV; emergency trip stations; vital train
12.125	Has the agency removed non explosive resistant trash receptacles from platform areas of terminals and stations?
12.126	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
12.127 TSF 1	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available through mutual aid agreements with other law enforcement agencies?
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? Describe
13.102	frequency of inspections and stations to identify and manage suspicious items, based on HOV has the transit agency developed
13.103	a form or quick reference guide for operations and personnel to conduct pre-trip, post-trip, and
13.104	within-trip inspections? Provide a form or quick reference guide for station attendants and others regarding station and facility

<p>13.105 TSF 2</p>	<p>regarding station and facility results of inspections and implement any changes to policies and procedures or implement corrective actions, based on the findings? Describe specific examples where</p>	
<p>13.106 TSF 2</p>	<p>Does the agency conduct frequent inspections of its critical systems access points, ventilation systems, and the interior of underground/underwater assets for indications of suspicious activity?</p>	
<p>13.107</p>	<p>Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect?</p>	
<p>13.108</p>	<p>Describe how Is there a process in place to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.</p>	
<p>13.109</p>	<p>necessary training provided to personnel, to ensure that all critical infrastructure are inspected at regular periodic intervals for suspicious or unattended items? Specify type</p>	
<p>14.101 TSF 2</p>	<p>background investigations on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems? (i.e.,</p>	
<p>14.102 TSF 2</p>	<p>criminal history and motor policy or law, does the agency conduct background investigations on contractors, including vendors, with access to critical facilities, sensitive security systems, and sensitive conducting employee background</p>	

14.103 investigations to confirm that procedures are consistent with

14.104 Does the agency have a documented process for conducting background investigations?

14.105 Is the criteria for background investigations based on employee type and responsibility, and is access documented?

15.101 TSF 2 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 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?

16.101 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

16.102 documented policy for proper handling, control, and storage of documents labeled as or

16.102	otherwise determined to be Sensitive Security Information (SSI) pursuant to 49 CFR Part 15
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)?

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	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 other designated group addressed

17.106	the findings and recommendations from the internal security audits, and Does the transit agency's internal
17.107	security audit process ensure that auditors are independent from those responsible for the activity
17.108	being audited? 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
17.111	audit? security audit process and the status of findings and corrective actions been made available to the SSO agency within the
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	was not able to certify to the SSO agency that the agency is in compliance with its SSP, was a corrective action plan developed

2" Security element is in place with all essential c

Comments	Items of Interest	
Establish W		
Inspectors should refer to the MT BASE Guidance, Pg12.	Policies and procedures related to <i>security</i> --including personnel security, vehicle security, facility security, and threat/vulnerability management.	4
		3
		2
		1
		0
	Documented method of effectively assessing and monitoring security program's purpose and progress.	4 2 1 0
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
	"Yes" or "No."	4 0
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
	Operation Control Center: managing incidents	4 3 2

		1
		0
In Justification, describe plans, procedures or protocols.	Documented plans for coordinating with external agencies.	4
		2
		0
	Active Shooter procedures or protocols were developed with local law enforcement and first responders	4
		2
		0
		4
		2
		0
	Protocols for IED <u>and</u> WMD	4
		2
		0
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
	Project/procurement planning, engineering, design, construction, and testing.	4
		3
		2

		1
		0
	Project design, engineering, and construction.	4
		3
		2
		1
		0
Reference date of last review in justification.	Annual review <u>requirement. A review is focused on written policy and ensuring policies are sufficient.</u>	4
		2
		1
		0
	An example of periodic reports reviewing SSP progress	4
		3
		2
		1
		0
	Documented evidence of a annual review. A review is focused on written <i>policy</i> and ensuring policies are sufficient.	4
		2
		0
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
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
		4
Inspectors should refer to the MT BASE Guidance, Pg13.	Emergency response procedures	3
		2

		1
		0
	Policy statement including: endorsement statement/signature, applicability, and authority/background of the plan.	4
		3
		2
		1
		0
	Documented requirement for annual review.	4
		2
		1
		0
Reference date of last review in justification.	Documented evidence of a annual review.	4
		2
		0
	Emergency response procedures coordinated with security and safety procedures. (Emergency procedures do not hinder safety or security.)	4
		3
		2
		1
		0
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
	Documented plans for coordinating with external agencies.	4
		2
		0
	Management of emergency events	4
		3
		2
		1
		0

Verify COOP addresses 5 main goals outlined in the MT BASE Guidance, Pg13.	Continuity of Operations plan.	4
		2
		0
	Procedures to recover from an event and resume normal operations.	4
		3
		2
		1
		0
	Procedures to continue essential operations during emergency.	4
		3
		2
		1
		0
indicate last time this was tested (if applicable) in Justification.	Secondary site of Operations Control.	4
		2
		0
Define		
Inspectors should refer to the MT BASE Guidance, Pg14.	Documented evidence assigning implementation of security program in the SSP.	4
		3
		2
		1
		0
		4

	Chain of Command and Lines of Succession for security responsibilities.	3
		2
		1
		0
	Security roles and responsibilities of Security Personnel.	4
		3
		2
		1
		0
	Security roles and responsibilities of non-security personnel.	4
		3
		2
		1
		0
Security should be the primary focus of these meetings and briefings	Management meetings for security recommendations. Operational.	4
		2
		0
Security should be the primary focus of these meetings and briefings	Security Review Committee	4
		3
		2

		1
		0
		4
	Security Briefings (written or verbal), means of acknowledgement. Operational.	3
		2
		1
		0
		4
	Reference guides for transit personnel	3
		2
		1
		0
This question applies to both Regulated and Non-Regulated entities.	Security Coordinator	4
		2
		0
		4
	Incident recording (may be document retention or summary archives)	3
		2
		1
		0
		4
Inspectors should refer	Documented evidence assigning	3

Inspectors should refer to the MT BASE Guidance, Pg14.	Documented evidence assigning implementation of security program in the ERP.	2
		1
		0
	Documented emergency response responsibilities.	4
		3
		2
		1
		0
	Frontline Personnel Responsibilities.	4
		3
		2
		1
		0
	ERP Distribution	4
		3
		2
		1
		0
	Reference guides for transit personnel	4
		3
		2
		1
		0
Emergency response should be the primary focus of these meetings and briefings	Management meetings for ERP coordination. Operational.	4
		3
		2
		1
		0

		0
		4
	Briefings related to emergency response. Operational.	3
		2
		1
		0
Ensure that operations and maintenance		
		4
Inspectors should refer to the MT BASE Guidance, Pg16.	Frontline Personnel Briefings	3
		2
		1
		0
		4
	Supervisor Briefings	3
		2
		1
		0
		4
Possible follow-up questions needed. Summarize program in justification.	Internal verification of knowledge	3
		2
		1

		0
		4
	Debriefing Requirement	3
		2
		1
		0

Coordinate Se

		4
Inspectors should refer to the MT BASE Guidance, Pg16.	MOUs involving law enforcement, other transit agencies, and first responders	3
		2
		1
		0

	Regional Emergency Management Group. "Yes" or "No."	4
		0

		4
	Regional Incident Management Protocols	3
		2
		1
		0

	Agency Resources. "Yes" or "No."	4
		0

	POC identified from EOC. "Yes" or "No."	4
		0

		4
	Agency Representative sent to EOC.	2

	"Yes" or "No."	0
	Information Sharing Capabilities	4
		2
		1
		0
	Internal Incident Management Protocols. "Yes" or "No."	4
		0
	Internal Emergency Response Protocols. "Yes" or "No."	4
		2
		0
	Interoperability	4
		3
		2
		1
		0
	Interoperability Substitute	4
		2
		0
Es		
Inspectors should refer to the MT BASE Guidance, Pg18.	Training records, training material	4
		2

		0
		4
	Training records, training material	2
		0
		4
	Training records, training material	2
		0
		4
	Training records, training material	2
		0
		4
	Training records, training material	2
		0
		4
	Training records, training material	2
		0
General emergency response / awareness training	Training records, training material	2
		0

		2
		0
	Training records, training material	4
		2
		0
	Training records, training material	4
		2
		0
	Training records, training material	4
		2
		0
	Training records, training material	4
		2
		0
	Training records, training material	4
		2
		0
	in justification, provide description of specialized training or provider.	4
	Training records, training material	2

		0
in justification, provide description of specialized training or provider.	Training records, training material	4 2 0
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
This question asks specifically about security-related courses.	Training Recording (Security) (ex. 30-day file)	4 2 0
This question asks specifically about emergency response related courses.	Training Recording (Emergency Response) (ex. 30-day file)	4 2 0
	Security Review and Updating	4 2 0
	Operational Changes	4 3 2 1 0

	Response and recovery operations in critical facilities and infrastructure.	4 2 0
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
ent enforcem		4 2 0
	Training program featuring concepts of random and highly visible countermeasures.	4 2 0
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 and		
Inspectors should refer to the MT BASE Guidance, Pg19.	Incremental actions based on NTAS threat	4 2 0
	Response protocols for specific threat scenarios based on NTAS	4 2 0

	Job-specific NTAS training	4	2	1	0	
Implement						
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
	Active outreach, utilizes program materials	4	2	0		
	Appropriate outreach material. "Yes" or "no."	4	0			
	Public announcements (Pre-recorded voice announcements)	4	3	2	1	0
	Materials specifically mention reporting unattended property, suspicious behavior and security concerns.	4	2			

		0
	Effective reporting mechanism	4
		2
		0
In justification, provide description of social media utilized.	Social Media Announcements for Security and Emergency. "Yes" or "No."	4
		0
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
	Training for non-employee volunteers for emergency response	4
		2
		0
	Active volunteer program (not the same as "See Something, Say Something")	4
		2
		0
If agency has no underwater/underground facilities question applies to transit vehicles.	Passenger evacuation guidance material	4
		2
		0
	Customer complaint tracking system	4
		2
		0
Establish and use a Risk I		
Inspectors should refer to the MT BASE Guidance, Pg20.	Process of Risk Assessment	4
		2

		0
In Justification, describe the critical assets identified by the agency.	Identification of Critical Assets	4
		2
		0
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
Scoring Justification should list at a minimum: date of assessment, identify critical assets, who conducted the assessment, etc.	Recent Risk Assessment (specifically <u>threat</u> , <u>vulnerability</u> , and <u>consequence</u> analyzed), appropriate personnel trained.	4
		2
		0
	Access to underground and underwater tunnels. N/A if the system does not have underground/underwater tunnels.	4
		2
		0
In justification, examples of improvements based off of risk assessment results should be provided.	Security Investments, examples of security investment prioritization	4
		2
		0
	Inspector was able to review <i>all</i> requested documents, including assessments and Security Plans. "Yes" or "no."	4
		0
Establish and		
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
	Reporting <i>directly</i> to ITTE or regional	4

	Reporting directly to JTF or regional anti-terrorism body. "Yes" or "no."	0
		4
		2
		0
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
	Documented evidence of intel receiving (Daily Report, etc.).	4
		3
		2
		1
		0
49 CFR PART 659 SSO Only Question	NTA Security Data (regulation)	4
		0
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
	Emergency planning responsibilities and drills/exercises general requirements	4
		2
		0
Agency driven	Agency conducting functional drills and exercises. "Yes" or "no."	4
		0

	Annual Requirement. "Yes" or "no."	4 0
	Results of drills/ exercises/ evaluations, documentation of results. "Yes" or "no."	4 0
	Documented training. "Yes" or "no."	4 0
Region driven	Active-player participation. "Yes" or "no."	4 0
		4 2 0
In Justification, describe the drill/exercise and include date.	Drills: Specific Focus. Participants: other transit agencies, first responders.	4 2 0
	Evaluation of results	4 2 0
In Justification, summarize the actions taken in the justification.	Evaluation of results, plan modifications. "Yes" or "no."	4 0
	Method of analysis	4 2 0
In addition to underwater/underground infrastructure, this	Drills in underwater/underground	4

question applies to other critical systems as identified by the entity.	infrastructure and other critical systems.	2
		0
In justification, summarize each joint event and state when it took place.	Drills with external agencies	4
		2
		0
Inspectors should refer to the MT BASE Guidance, Pg24.	Risk assessment focused on <u>IT SECURITY</u>	4
		2
		0
	Security measures for critical IT facilities/equipment	4
		2
		0
	Written IT security measures	4
		2
		0
	IT Security Coordinator	4
		3
		2
		1
		0
	Recurrent cybersecurity training	4
		2

		0
	Cyber-incident response and reporting protocols	4
		2
		0
In Justification, describe resources used by agency.	Available resources. "Yes" or "no."	4
		0

Section Header

Inspectors should refer to the MT BASE Guidance, Pg26.	Restricted Areas	4
		2
		0
	ID Badges	4
		2
		0
	Access Control Monitoring/Updating	4
		2
		0
	ID Badges for contractors and visitors	4
		2
		0
	Escorts Policy	4
		2
		0
	CCTV: Facilities	4
		2
		0
		4

	CCTV: Access Control	2
		0
	CCTV: Vehicles	4
		2
		0
	CPTED; Design/Engineering Representative interview	4
		2
		0
Physical barriers	4	
	2	
	0	
Additional measures for high-risk assets	4	
	2	
	0	
Alarm monitoring	4	
	3	
	2	
	1	
	0	
Call boxes	4	
	2	
	0	
Automated Access Control (employee-controlled badge/keycard entry)	4	
	3	
	2	
	1	

		0
		4
	Mail screening	2
		1
		0
		4
	Breach preparedness at critical location	2
		0
	Access Control does not interfere with Safety or Emergency Operations. "Yes" or "no."	4
		0
		4
	Lighting	2
		0
		4
	Methods of restricting access	2
		0
		4
	Key control program	2
		0
		4
	Methods of securing facilities	2
		0
		4
	Means of communication	2
		0
		4

	"Broken Windows Theory"	2
		1
		0
	Back-up power for critical safety and security equipment	4
		3
		2
		1
		0
	Trash receptacles	4
		0
	Protective Measures for Critical Infrastructure	4
		2
		0
	Explosive detection canine unit, Mutual Aid Agreements	4
		2
		0
Inspectors should refer to the MT BASE Guidance, Pg29.	Critical asset inspections (General)	4
		2
		0
In justification, provide results of interview with Front Line employees.	Inspection procedures reflect "HOT" characteristics. "Yes" or "no."	4
		0
	Vehicle inspection checklist. "Yes" or "no."	4
		0
	Facility inspection checklist. "Yes" or "no."	4
		0

		4
	Inspection results	2
		0
	Inspections of non-normal areas. N/A if the system has no underground/underwater tunnels.	4
		2
		0
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
In justification, specify type and frequency of inspections.	Security Inspections: Vehicles	4
		2
		0
In justification, specify type and frequency of inspections.	Security Inspections: Critical Infrastructure	4
		2
		0
Inspectors should refer to the MT BASE Guidance, Pg30.	Background checks, HR Representative interview	4
		2
		0
	Background checks, HR Representative interview	4
		2
		0
	Background checks, HR	4

	Background checks, HR Representative interview	0
	Background check process, HR Representative interview	4
		2
		0
	Background check process, HR Representative interview	4
		2
		0
Con		
Inspectors should refer to the MT BASE Guidance, Pg31.	Security-critical documentation, Engineering Representative interview	4
		2
		0
	Document control authority. "Yes" or "no"	4
		0
	Document control policy monitoring	4
		2
		0
Proc		
Inspectors should refer to the MT BASE Guidance, Pg32.	Documented SSI Policy	4
		2
		0
	Documented SSI Policy	4

		2
		0
	Employee familiarization (requires frontline interviews)	4
		2
		0
	SSI Training development and implementation (requires frontline interviews)	4
		2
		0
Inspectors should refer to the MT BASE Guidance, Pg32.	Established Schedule Internal Security Audit (self-assessment). An audit is focused on <i>practices</i> identified in the SSP and ensuring these policies are implemented and followed effectively.	4
		2
		0
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
	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
	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
	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
	Peer Review: Internal Security Audit (self-assessment). An audit is focused	4

	(self-assessment). An audit is focused on practices identified in the SSP and ensuring these policies are implemented and followed effectively.	2
	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."	0
	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
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."	0
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
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	0
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	0
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	0
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	4
49 CFR PART 659 SSO Only Question	SSO: Internal Security Audit (self-assessment). "Yes" or "no."	0

Mass Transit BASE Scoring Guidance - Appendix IX

Components but not fully implemented or practiced. (Equates to partial adherence)

Score

Written 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 security. SSP is missing no key elements and has been completely implemented by the agency.

SSP is a complete document with policies and procedures that have been appropriately detailed with minimal exceptions.

Generic policies and procedures are documented and implemented adequately. Key elements are commonly available "template."

SSP is a generalized document that is lacking any detailed, agency-specific security elements. There is no SSP in place.

Goals and objectives are identified, documented and actively monitored to ensure they are met.

Goals and objectives are identified and documented, but not monitored. Items may not be met.

Goals and objectives are minimal, lacking any specifics or depth. These items do not address the security program.

The SSP does not address goals or objectives of the security program.

Policy statement is a well developed written statement (memo, mission statement, 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 used to have a separate document for SSP. This is no longer the case. See element 17: Security)

Security plans address specific policies and procedures related to security and emergency response for 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) are documented elsewhere, such as in a stand-alone Emergency Response Plan, the SSP, or other documents.

Plans and procedures are in place and function appropriately. However, minor aspects are missing.

Well organized procedures are in place and contained as part of another document.

Procedures are lacking any depth or clarity, plans are scattered between multiple documents.

Procedures are not in place or documented.

Well-developed, **specific** procedures are in place and documented in the SSP **or** as part of other documents.

Procedures are in place with varying degrees of implementation or documentation.

Procedures are not in place or documented.

Active Shooter procedures and protocols were developed with local law enforcement and first responders response to an Active Shooter threat.

Active shooter procedures were developed without local law enforcement and first responders.

Law enforcement/ first responders have not been engaged in the development of active shooter procedures.

Well-developed, **specific** procedures or protocols are in place that address Active Shooter threats, such as a stand-alone Emergency Response Plan, and referenced in the SSP.

Procedures or protocols exist and are documented however the procedures are general in nature.

Procedures or protocols have not been developed.

Well-developed, **specific** protocols are in place that address IED **and** WMD. These protocols are documented in the 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 to personnel.

Random, unpredictable measures are documented. Measures are simply general guidelines.

The agency relies on outside entities to provide random, unpredictable measures. A plan is not 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 culture. A process is in place for planning and implementing a project with security playing a role in the implementation.

Security plays a role in all new projects and procurements and is part of the safety culture with security playing a role in various phases, including: planning, engineering, construction, and testing. The agency's Safety plan--not the SSP.

Specific security concerns are considered for all new projects, but implementation is not documented.

Security is addressed on an informal basis with only general security guidance considered.

There is no documented evidence in place that suggest security is addressed with need.

CPTED principles are addressed in all facilities and fully implemented. These principles

CPTED principles are addressed and implemented in a majority of facilities. This is documented
been identified.

CPTED principles are addressed with minimal implementation. Principles are documented

CPTED adoption is merely a general acknowledgement contained in the SSP or other

CPTED is not adopted by the agency.

Annual review is a written requirement with verification measures in place (signed and

Annual review is a "commonly known" requirement (not documented) or a written requirement

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

Periodic reports are detailed and developed once in a two-year cycle **OR** periodic reports

Informal reports are developed on an "as-needed" basis.

Reports are not documented, per se, but the agency does have an informal, verbal summary

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 written

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
by the agency.

ERP is a complete document with polices and procedures that have been appropriately
detailed with minimal exceptions.

Generic policies and procedures are documented and implemented adequately. Key documents
commonly available "template."

ERP is a generalized document that is lacking any detailed, agency-specific security e

There is no ERP in place.

Policy statement is well developed and includes all elements: endorsement statement
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 sig

There is no policy statement of any sort in place.

Annual review is a written requirement with verification measures in place (signed a

Annual review is a "commonly known" requirement (not documented) or a written r

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 s

ERP includes documented provisions that ensure its coordination with either the ag

Provisions are in place and clearly implemented, but no documentation established.

Coordination is very informal with no specific provisions in place. Documentation inc
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 p

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 th
documented in the ERP. If documented elsewhere, the ERP references that docume

Plans and procedures are in place and function appropriately. However, minor aspe

Well organized procedures are in place and contained as part of another document

Procedures are lacking any depth or clarity, plans are scattered between multiple d

Procedures are not in place or documented.

Continuity of Operations plans exist and are included as part of the ERP (or in another document).

Continuity of Operations plans exist but are not included as part of the ERP or referenced in another document.

No Continuity of Operations plans exist.

Business Recovery Plan is a comprehensive plan. Essential business functions (HR, IT, etc.) are identified and detailed. The plan outlines steps to be taken to return the agency to a normal state of operations and how the agency transitions from emergency operations to business recovery.

Business Recovery Plan is a well-developed document, missing only a few elements.

Business Recovery Plan is a generic plan that appears to be a commonly available "template" plan.

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 operations.

Business Continuity Plan is a comprehensive plan. Essential operations functions (business processes, etc.) are identified and detailed. Procedures are detailed and effective in mitigating any disruption to operations. Contingency plans are identified and documented. Resulting SOP changes are documented.

Business Continuity Plan is a well-developed document, missing only a few elements.

Business Continuity Plan is a generic plan that appears to be a commonly available "template" plan.

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 is not the primary Operation Control Center.

There is a back up operations control center, but it cannot fully replicate the primary operations control center.

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 or higher.

The implementation of the security program has been assigned to a Senior Manager or higher, but not a commonly known assignment that is documented elsewhere.

The implementation of the security program has been assigned to a manager or leader, but not an SSP.

The implementation of the security program has been ineffectively assigned to a position.

The implementation of the security program is not assigned, or there is no documentation.

The agency has established comprehensive policies and procedures related to "chain of succession" that are documented, and lines of succession include multiple individuals based on the importance of the position. This policy is shared with agency managers.

The agency has established basic--yet fully developed--procedures related to "chain of command" or needing further development. Lines of succession may not be in-depth, only identifying the manager.

The agency has established and documented a "chain of command." Informal (or "grapevine")

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 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 with additions.

General roles and responsibilities are assigned by position and documented in the SSP. Specific Position types identified may also be vague or missing key positions.

General security roles and responsibilities are documented in the SSP or other documents.

Roles and responsibilities are not documented.

Specific security-related responsibilities have been established for non-security personnel. Security-related responsibilities are comprehensive and clearly identify the role non-security personnel play in the documents.

Security-related responsibilities have been established for non-security personnel. Specific responsibilities by 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 total responsibilities. 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. Interview and document review.

Senior staff and management conduct security meetings infrequently, but at least annually. Interview.

Senior staff and management meet on an infrequent basis, if ever, or meetings related to security.

A formal security committee or working group has been established. This group meets quarterly to review 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 quarterly. All applicable security items are addressed.

A formal security committee or working group has been established, but it only meets quarterly. 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 message delivery systems for security messages based on message importance: face-to-face briefings, agency has also developed a means of tracking/monitoring who has (or has not) received messages (e.g., etc.).

Entity has procedures in place to ensure that frontline personnel are made aware of security messages in an effective, with very little (but possible) chance of employees not receiving critical information through informational briefings.

Briefings are only delivered through written-memos or other ineffective means of communication, but the message itself is not guaranteed (employees may not understand a message or not know 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 (Example: Driver's manual, SOP, etc.)

Individual written guides or reference material with generalized guidance have been provided to employees.

Written guides or other written materials have been provided to every department and employee.

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 a minimum of once a month.

The agency has a Primary and or Alternate Security Coordinator, but their roles are not clearly defined (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 last year.

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.

The implementation of the security program has been assigned to a Senior Manager or other commonly known assignment that is documented elsewhere.

The implementation of the security program has been assigned to a manager or leader of the ERP.

The implementation of the security program has been ineffectively assigned to a position.

The implementation of the security program is not assigned, or there is no documentation.

The agency takes an all-inclusive, system-wide approach to emergency preparedness across all departments. Roles are comprehensive, detailed, and documented.

Emergency response roles and responsibilities have been developed and assigned to all departments. Roles and responsibilities are well-developed and assigned effectively, but there is room for improvement.

Documented roles and responsibilities have been only assigned to critical departments.

Documented roles and responsibilities have been assigned as a blanket-statement for all departments.

Roles and responsibilities are not documented.

Roles and responsibilities of frontline personnel are assigned by position and documented.

Roles and responsibilities of frontline personnel are assigned and documented in the ERP.

Roles and responsibilities of frontline personnel are developed and documented in the ERP.

General security roles and responsibilities are documented in the SSP or other documentation.

Roles and responsibilities are not documented.

The agency takes a total approach to emergency response, including all departments.

The agency is proactive with emergency response. The ERP has been provided to departments that are critical to emergency response and a secondary support role during emergency response.

The agency has only provided the ERP to departments that are critical to emergency response.

ERP distribution is very limited. Departments do not have easy access to the documentation.

The ERP is not distributed.

Individual written guides or reference material based on job function have been provided to all employees.

Individual written guides or reference material with generalized guidance have been provided to all employees in the form of procedures.

Written guides or other written materials have been provided to every department.

Written guides or other written materials exist but are not conveniently available to all 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 relat

Policies and procedures are in place to ensure that frontline personnel are made aw
delivery systems for security messages based on message importance: face-to-face v
also developed a means of tracking/monitoring who has (or has not) received high-i

Entity has procedures in place to ensure that frontline personnel are made aware of
with very little (but possible) chance of employees not receiving critical information.
briefings.

Briefings are only delivered through written-memos or other ineffective means of pe
but the message itself is not guaranteed (employees may not understand a message
gauge who has received the message).

Entity only utilizes bulletin board-style briefings.

No briefings.

Supervisors, forepersons and managers are held accountable for security issues

Frontline employees receive a **weekly** briefing from their immediate supervisor rega
primary focus of briefings (or equal to that of safety). Verified by Interview, Document

Frontline employees receive a **monthly** briefing from their immediate supervisor reg
primary focus of briefings (or equal to that of safety).

Frontline employees receive a **quarterly** briefing from their immediate supervisor re
primary focus of briefings (or equal to that of safety).

Frontline employees are provided information regarding security and emergency res

Frontline employees are not provided information regarding security and emergenc

Supervisor/management **security** review and coordination meetings are held on a **m**

Supervisor/management **security** review and coordination meetings are held on a **b**

Supervisor/management **security** review and coordination meetings are held on a **q**

Supervisor/management **security** review and coordination meetings are held on an

Meetings are not held or do not focus on security.

The agency actively engages its workforce to ensure a high rate of security knowledge
audits, challenge procedures, or qualification testing. The program--or procedures/r

The agency has an on-going, informal system of measuring its workforce's knowledge
specific measures it takes to ensure its personnel retain a working knowledge of sec

Employees are tested after training, and Supervisors are tasked with ensuring proto

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 the agency's policies and procedures.

There is a written policy that requires leadership to debrief frontline personnel regarding both Interview and Document Review.

There isn't a written requirement, but leadership is expected to debrief frontline personnel. This expectation is widely known. Verified by both Interview and Document Review.

Leadership is expected to debrief frontline personnel only after **major** incidents regarding Debriefing are being held, but the policy is very insufficient and inconsistent.

There are no debriefing measures in place.

Security and Emergency Management Plan(s) with local and regional agencies

The agency has taken a comprehensive approach to emergency preparedness and has coordinated with during an emergency situation. This includes: law enforcement entities. Interview and Document Review.

The agency has taken a proactive approach to emergency preparedness and has established

The agency has taken a limited approach to emergency preparedness and has established a geographical scope of their system.

The agency has taken the first steps of establishing mutual aid agreements. Agreements are non-existent and not being pursued.

The agency participates in a regional security and emergency preparedness/management plan.

The agency does not participate in a security and emergency preparedness/management plan.

The agency has received--and is knowledgeable of--regional incident management plans. Verified by both Interview and Document Review.

The agency has received--and is knowledgeable of--regional incident management plans and the agency's ERP/SSP/SEPP. Verified by both Interview and Document Review.

The agency has received--and is knowledgeable of--regional incident management plans.

The agency is aware of regional protocols and understands how they may obtain the information.

The agency is completely unfamiliar with regional protocols.

The agency has provided the regional EMA with a detailed list of resources (vehicles, equipment, personnel, etc.).

Agency resource inventory has not been provided to the regional EMA.

Agency has established a point-of-contact at the Emergency Operations Center. Mutual aid agreements are non-existent and not being pursued.

Agency has no identified POC at the EOC.

Agency has officially designated a representative to be sent to the EOC, upon activation.

The agency has designated a representative to be sent to the EOC, upon activation, but the representative has not been identified.

Agency has not designated a representative.

The agency has developed a **formal** method of effectively sharing information with the EOC, and the method of sharing is known by both entities. Capabilities are documented. Must be verified.

The agency has developed an **informal** method of effectively sharing with the EOC, and the method of sharing is known by both entities. It is clear that the agency has planned for information sharing.

Information sharing procedures and capabilities exist, but are vague and have received no verification.

The agency has no information sharing capabilities or procedures and is not actively seeking to develop them.

The agency's internal emergency response procedures follow the NRP and the NIMS ICS.

The agency's internal emergency response procedures do not follow the NRP and the NIMS ICS.

The agency has shared its internal emergency response protocols with the regional EOC.

The agency has shared its internal emergency response protocols with **only** the regional EOC.

The agency has not shared its emergency response protocols.

The agency is very proactive in regards to interoperable communication and ensures compatibility across jurisdictional lines. The agency uses compatible radio systems (800mHz, UHF, VHF, etc.) for communication, and has tested its system for compatibility with appropriate external agencies.

The agency has an effective interoperable communications system (800mHz, UHF, VHF, etc.) with documentation) is missing **or** the agency has not tested its system for compatibility.

The agency has an effective interoperable communications system (800mHz, UHF, VHF, etc.) with testing is in place.

The agency's systems are not interoperable, but is in the process of actively implementing interoperable systems.

The agency's systems are not interoperable, nor is such a system being currently implemented.

The agency has developed effective alternatives to interoperable communication (both formal and informal) documented and shared with appropriate first responder agencies. Must be verified.

The agency has developed partially effective alternatives to interoperable communication (both formal and informal) and may not be documented and/or shared with first responder agencies.

The agency has identified no alternatives for interoperable communication.

Establish and Maintain a Security and Emergency Training Program

All new employees, regardless of job function, receive initial training, which is focused on an official curriculum and training is provided in a formal environment (classroom or on-the-job).

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 matter, and training is provided in a formal environment (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 matter.

Annual refresher training is well-developed with an official curriculum, focused on the appropriate subject matter, and training is provided in a formal environment (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 matter.

Annual refresher training is well-developed with an official curriculum, focused on the appropriate subject matter, and training is provided 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.

Refresher training is not provided annually or does not focus on the appropriate subject matter.

Advanced security training is provided in an ongoing manner, with classes/courses based on job function, and 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.

Ongoing security training based on job function is not provided.

All employees, regardless of job function, receive initial training, which is focused on the appropriate subject matter, and training is provided in a formal environment (classroom or computer-based). Must be verified by Document Review. Initial training is provided with varying degrees of implementation.

Training specific to Active Shooter is not provided.

All employees, regardless of job function, receive annual Active Shooter training. Training is provided in a formal environment (classroom or computer-based). Must be verified by Document Review.

Training is provided with varying degrees of implementation.

Refresher training is not provided annually.

All new employees, regardless of job function, receive initial training, which is focused on the appropriate subject matter, and training is provided in a formal environment (classroom or computer-based). Must be verified by Document Review.

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 matter, and is provided annually to all employees. This training should 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 matter.

Annual refresher training is well-developed with an official curriculum, focused on the appropriate subject matter, and is provided annually to all employees. This training should 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 matter.

Annual refresher training is well-developed with an official curriculum, focused on the appropriate subject matter, and is provided annually to all employees. This training should 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 matter.

All employees who may have a role in emergency response--frontline personnel and supervisors receive annual refresher training in a well-developed program with an official curriculum and training is provided annually in a formal environment (classroom or computer-based). This training should 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 employees.

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 employees.

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 employees.

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 with official training materials, and is provided in a formal environment (classroom or computer-based).

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 leaders.

Training appropriate to the position has been provided with varying degrees of implementation.

Senior leadership only receives basic training, training appropriate for frontline personnel.

Annual training based on job function is provided by the agency to all supervisors and managers.

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 the position.

Annual training based on job function is provided by the agency to all frontline personnel.

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 off-site program (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 leaders.

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.

Annual training based on job function is provided by the agency to all supervisors and managers.

Training appropriate to the position has been provided with varying degrees of implementation.

Supervisors and managers only receive basic training, training is appropriate to the position.

Annual training based on job function is provided by the agency to all frontline personnel.

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 terrorism instruction led by subject matter experts. Training is part of an established curriculum. 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 support and instruction led by subject matter experts. Training is part of an established curriculum. 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 of easily determining employee training status, and having the ability to effectively schedule training.

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 containing 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 **security** training is not specifically addressed.

The agency has a formal system to **record and track** personnel training for **all emergency response** training containing 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 procedures (generally or as a "role/responsibility"), and the program ensures material changes are documented.

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 procedures.

Appropriate personnel are notified of operational changes--including those related to security and emergency response--and measures are in place to effectively reach **all** appropriate employees.

Appropriate personnel are notified of operational changes--including those related to security and emergency response--and measures are in place for the agency to confidently reach **most** of the appropriate employees.

Appropriate personnel are notified of operational changes. Individuals with a "need to know" are notified with consistency.

The agency notification measures are inconsistent with little to no planning involved. Operational changes are rarely--if ever--communicated to employees, or no policy exists.

The agency's security and emergency response training covers response and recovery and is part of an official curriculum, utilizes effective training materials, and is provided in

Security and emergency response training covers response and recovery operations

Training does not cover response and recovery operations.

The agency has provided training to regional first responders to enable them to operate and 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. The agency has developed and implemented a program to orient local law enforcement agency actively offers this familiarization separate from drills or exercises. Must be verified. The agency has provided training with varying degrees of implementation.

Such a program does not exist.

The concept and employment of visible, unpredictable, and random security measures is 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

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 familiarization. Training is well-developed, and the agency has actively offered it to outside

The program has been developed with varying degrees of implementation.

Such a program does not exist.

and protocols to respond to the DHS National Terrorism Advisory System (NTAS).

The agency has identified incremental actions that correlate with NTAS threat level 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 protocols documented.

Actionable operational response protocols for specific threat scenarios from NTAS have been

Actionable operational response protocols have not been developed or specific threat scenarios

Job-specific NTAS training that focuses on incremental activities to be performed by official curriculum, focuses on appropriate individual roles in response to NTAS threat. 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

Agency has implemented a well-developed public awareness program that addresses

Agency has implemented a well-developed public awareness program that addresses

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 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 effectiveness.

Public awareness materials and outreach have not been developed and/or deployed with varying degrees of effectiveness.

Public awareness material is consistent with the agency's overall announcement program 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 at stations and onboard vehicles.

The agency includes frequent mentions of general security items (but no emergency preparedness items) including at stations and onboard vehicles.

The agency includes frequent mentions of general emergency preparedness items at all appropriate areas, including at stations and onboard vehicles;

The agency includes ***infrequent*** mentions of general security and emergency preparedness items at stations and onboard vehicles.

Security and emergency preparedness items are not included in the agency's pre-recorded announcements.

Passengers are urged to report unattended property, suspicious behavior, and other safety concerns (e.g., law enforcement, etc.) or identified contact number. This is documented in awareness materials.

Passengers are urged to report unattended property, suspicious behavior, and other safety concerns.

Passengers are not urged to report unattended property, suspicious behavior, and other

The agency utilizes an effective mechanism in place that can be used by passengers
mechanism is actively monitored by the agency and widely distributed to passenger
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 se

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

The agency does not issue emergency response-related PSAs or press releases to loc

The agency conducts training of non-employee volunteers to aid with system evacu
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 awarene
Must be verified by Document Review.

The agency has established an active volunteer program with varying degrees of imp

The agency has not established an active volunteer program.

The agency has developed awareness material to assist passengers on the means to
readily available or readily visible to passengers. Must be verified by Document Revi

The agency has developed awareness material with varying degrees of implementat

The agency has not developed awareness material to assist passengers on the mean

The agency has a system in place to actively and effectively monitor and follow up o

The agency has developed a system with varying degrees of effectiveness or implem

The agency has not developed a system for tracking and following up on customer r

Management Process to assess and manage threats, vulnerabilities and consequ

Risk assessment process is developed, documented, specifically addresses threats a

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 in the Risk Assessment Report.

The agency has identified critical assets with varying degrees of documentation or documentation.

The agency has not identified critical assets.

A vulnerability assessment focused on the agency's ***critical assets*** has been conducted.

A vulnerability assessment focused on the agency's ***critical assets*** has been conducted.

A security assessment focused on the agency's critical assets has not been conducted.

A risk assessment focused on the agency's ***critical assets*** has been conducted within the agency's risk management process. The personnel tasked with conducting the assessment have been provided training. Documented. The personnel tasked with conducting the assessment have been provided training. Document Review.

A risk assessment has been conducted with varying degrees of implementation or documentation. 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 protect critical assets. Document Review.

Documented policies are in place with varying degrees of implementation. Verified by Document Review.

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 the agency's recent security investments that corrected items identified in risk assessments.

Security investments are prioritized based on information obtained during risk assessments and risk assessment development.

Security investments are not prioritized based on information obtained during risk assessments.

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 process for sharing information with local, State ***and*** Federal law enforcement.

The entity has a formalized method of sharing information with varying degrees of formality.

The entity does not have a formalized method of sharing information with law enforcement.

The agency reports threat/intel information ***directly*** to the JTTF or regional anti-terrorism center.

The agency does not report threat/intel information **directly** to the JTTF or regional

The agency has detailed policies and protocols in place to report suspicious activity

Agency has an informal, commonly know process for reporting suspicious activity.

Policy or procedures do not exist

The agency has detailed policies and protocols in place to report real-time threats/s documented and include a "time" element (immediately, within "X" hours, etc.).

The agency has detailed policies and protocols in place to report real-time threats/s documented and include a "time" element (immediately, within "X" hours, etc.).

General/vague policies and procedures are in place with varying degrees of impleme

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 r

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 emergency planning and participation in exercises and drills. This is documented in t

The agency has developed a process with varying degrees of implementation or doc

The agency has not developed such a process.

The agency has documented roles and responsibilities that detail how it performs its agency has established written requirements for emergency drills and exercises (tim and requirements are documented in the agency's SSPP or SSP--or another documen

Roles, responsibilities and requirements regarding emergency planning are develop

Roles, responsibilities and requirements regarding emergency planning are not deve

The agency conducts drills and exercises **annually** with the purpose of **evaluating** its

The agency does not conduct drills and exercises **annually**, or the agency does not u

The agency has a **documented requirement** for drills/exercises to be conducted **once**

The agency does not have a documented requirement for drills/exercises to be conducted

The process of drill/exercise evaluation is described and documented in the SSPP, SSPP

The process of evaluation is not documented.

The program for providing employee training on emergency response protocols and

The training program is not **documented**.

The agency participates as an **active player** in full-scale, regional exercises held at least

The agency does not participate as an **active player** in full-scale, regional exercises held

In the last year, the agency has conducted its own drills and/or exercises specific to

Drills and/or exercises specific to Active Shooter are conducted by the agency however

Drills or exercises were not conducted annually

In the last year, the agency has been involved in drills/exercises that specifically focus on
transit agencies that operate in the same environment.

Terrorism-specific drills have been conducted/participated in with varying degrees of

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
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

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
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
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) medical, **and** law enforcement.

Drills with external agencies have been conducted with varying degrees of inclusion.

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 and addresses threats, vulnerabilities, and consequences. Must be verified by Document

The agency has conducted an IT risk assessment with varying degrees of implementation.

The agency has not conducted an IT risk assessment.

The agency has identified all critical IT facilities/infrastructure and established procedures well-developed--specifically referencing IT-facilities/equipment and IT-security--and

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 (included as part of the SSP or other appropriate document).

An IT-security strategy has been developed with varying degrees of implementation.

An IT-security strategy has not been developed.

The agency has formally designated an individual responsible for securing the internal cybersecurity measures, and his/her responsibilities are documented.

The agency has formally designated an individual responsible for securing the internal cybersecurity measures, but his/her responsibilities are **not** documented (but widely

The agency has formally designated an individual responsible for securing the internal measures.

An individual has been informally designated, and his/her responsibilities are not widely

An individual has not been designated.

The agency provides ongoing, recurrent cyber training that **identifies cyber threats** part of an official curriculum, utilizes well-developed materials, and is provided in a t

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 of a cyber-incident **and** (b) to whom cyber-incidents shall be reported. Must be ver

Cyber-incident response and reporting protocols have been established with varying

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

Control Access to Security Critical Facilities

Restricted areas are identified and documented. Agency personnel are familiar with

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 re verified by Frontline Observation.

ID badges (or other effective measure) are issued with varying degrees of implemen

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 fo

The agency utilizes an access control system with varying degrees of implementation

The agency's access control procedures is not capable of monitoring, documenting,

The agency has documented procedures in place to issue ID badges for visitors and c

The agency has procedures in place to issue ID badges for visitors and contractors w Observation.

The agency does not have procedures for issuing ID badges to visitors and contracto

The agency has a documented policy that requires visitors to be escorted when acce

The agency has policy In place with varying degrees of implementation or document

The agency has no escort requirements for visitors.

Effective and capable CCTV systems are installed at all facilities. Must be verified by

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 acce

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

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

The agency uses barriers and intrusion detection systems with varying degrees of in

The agency does not use physical barriers or intrusion detection systems at appropri

The agency has identified high risk/high consequence assets and has implemented a

The agency has identified high risk/high consequence assets and developed addition

The agency has not identified high risk/high consequence assets and/or implemente

The agency has a means of effectively monitoring a network of alarms, including intr
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 boxe

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 ana
analysis is documented as part of an overarching policy or as part of an identified en

The agency uses an automated access control system and performs a formal correct
analysis is being performed, but this responsibility is not documented.

The agency uses an automated access control system and performs a corrective ana

The agency uses an automated access control system, but has not developed proced

The agency does not use an automated access control system.

The agency has documented policies and specific, well-developed procedures that a

The agency has specific, well-developed procedures that are not documented. Proce

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, l

The agency utilizes methods of breach prevention at critical location with varying de

The agency does not use locks, bullet-resistant materials, or anti-fragmentation mat

NFPA 130 or equivalent is used in station design or modification criteria. Access Con

Access control systems interfere with safety or emergency operations.

Directional signage and lighting is consistent at **all** stations and is installed in a man

Directional signage and lighting is used with varying degrees of implementation or in

Directional signage and lighting does not support security, safety, and emergency op

The agency uses gates and locks to prevent unauthorized access at **all** facilities. Polic

Gates and locks are used with varying degrees of implementation. Must be verified l

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/

The agency has a key control program with varying degrees of documentation or im

The agency has no key control program.

Gates and locks are used at **all** facilities that are closed down. Policies and procedur

Gates and locks are used with varying degrees of implementation. Must be verified l

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, a
utilize these measures.

Radios, silent alarms, and/or passenger communication systems are used with varyi

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) facilit

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.

The agency has not removed non-explosive resistant trash receptacles from platform areas.

The agency has formally identified critical infrastructure and deployed specific, effective protective measures in critical infrastructure areas.

The agency has deployed protective measures with varying degrees of implementation.

Measures are not deployed to protect critical infrastructure or critical infrastructure areas.

The agency utilizes explosive detection canine teams (with appropriate mutual aid agreements) regarding their use.

The agency utilizes explosive detection canine teams with varying degrees of program implementation.

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 that are appropriately documented and implemented perfectly.

Security inspections are conducted with varying degrees of implementation or documentation.

Security inspections are not conducted.

Documented security procedures reflect HOT characteristics. Must be verified by FRO.

Documented security procedures do not reflect HOT characteristics.

The agency utilizes a checklist or other widely distributed document that specifically addresses vehicle security inspections.

The agency does not use a checklist/form for vehicle security inspections ***or*** the agency does not use a checklist/form for facility security inspections.

The agency utilizes a checklist or other widely distributed document that specifically addresses facility security inspections.

The agency does not use a checklist/form for facility security inspections ***or*** the agency does not use a checklist/form for vehicle security inspections.

Inspection results are documented **and** the agency implements corrective actions on agency or is a documented policy.

Results are documented and changes are made with varying degrees of implementation.

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, etc.) multiple times per week. These procedures are documented appropriately and implemented.

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 activities are documented.

Security activities are conducted at set times.

The agency has documented policies and procedures in place to ensure that **all** in-service 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 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 and contractors information/facilities/systems.

The agency conducts an appropriate level of background check with varying degrees of implementation or documentation.

Agency-personnel are not subject to background investigation.

The agency **(a)** conducts an appropriate level of background check on relevant contractors **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 or documentation.

Relevant contract employees are not subject to background investigation.

The agency's process for conducting background investigations has been reviewed by an independent party.

The agency's process for conducting background investigations has **not** been reviewed.

The process for conducting background checks is documented. This includes the following information (the name of the person who is responsible for conducting the investigation, and other factors of consideration that are relevant to the investigation being 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, requirements, and the type of background check. This is documented.

Background screening criteria (disqualifying conditions) is based on job-function, requirements, and the type of background check. This is documented.

Background screening criteria is not documented.

Control Access to documents of security critical systems and facilities

The agency has well-developed document control procedures that protect security-critical information, such as 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 program.

A person or department has **not** been formally tasked with administering the access control program.

A security review committee actively reviews document control practices, assesses compliance, and reports findings to management.

A security review committee covers document control issues with varying degrees of implementation.

Document control issues are not addressed by the security review committee.

Policy for handling and access to Sensitive Security Information (SSI)

The agency has a fully-developed policy for identifying and controlling the distribution of SSI, including: (1) what materials are considered SSI; (2) how SSI is marked; (3) who has access to SSI; and (4) how SSI is destroyed/disposed of.

The agency's SSI policy covers identification and distribution with varying degrees of implementation.

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 SSI, including: (1) proper handling of SSI (how distribution is tracked, how SSI should be treated once received, and how SSI is destroyed/disposed of).

The agency's SSI policy covers handling and storage with varying degrees of implementation.

The SSI policy is not documented or documentation contains no mention of SSI handling.

Based on a random sampling of frontline personnel interviews, **all** employees who may be provided with SSI training, (a) what constitutes SSI, (b) how it is controlled, (c) how it is handled, and (d) how it is stored.

Based on a random sampling of frontline interviews, employees who may be provided with SSI training have varying degrees of familiarity. Must be verified.

Based on a random sampling of frontline interviews, employees who may be provided with SSI training have varying degrees of familiarity.

The agency has established official SSI training (with appropriate materials), **and** based on a random sampling of frontline interviews, 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 familiarity.

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 accordance with the established schedule.

The agency has developed a schedule for conducting internal **security** audits with varying degrees of implementation.

The agency has no documented schedule for conducting internal **security** audits.

The agency has a detailed, well-documented process for conducting internal **security** audits; (1) how these items are audited (methods of verification); and (2) how these items are audited (methods of verification); and (3) how these items are audited (methods of verification).

The SSP contains a description of the internal security audit process with varying degrees of implementation.

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** checklists with varying degrees of implementation.

The agency has developed procedures **and** checklists with varying degrees of implementation.

The agency does not use checklists, but has documented procedures in place.

The agency has no documented procedures for conducting internal security audits.

The agency is conducting internal security audits in a manner that reflects its established schedule.

The agency is not complying with its 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) findings; (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, and the results are documented.

In the last 12 months, the Security Review Committee has reviewed audit reports with

The Security Review Committee does not review audit reports or the committee has

Auditors are independent from the individuals they are tasked with auditing to prevent

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

The agency has not made checklists and procedures used in its internal security audits available

The agency has notified the SSO agency 30 days prior to the conduct of an internal security

The agency has not notified the SSO agency 30 days prior to the conduct of an internal security

A report documenting internal security audit process and the status of findings and

A report documenting internal security audit process and the status of findings and
months.

The agency's chief executive has certified to the SSO agency that the agency is in compliance

The agency's chief executive has not certified to the SSO agency that the agency is in compliance

The previously mentioned certification was included with the most recent annual report

The previously mentioned certification was not included with the most recent annual report

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.

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY Transportation Security Administration

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

MTPR FY2021 V.2
(January 2021)



Transportation Security Administration

Date of Visit	TSA Field Office	Region #
1/4/2021		
FSD AOR Field Office (Optional):		
Assessment Started:		
Assessment Completed:		
Outbrief Conducted:		

TYPE OF VISIT		Agency			
Corporate Review					
Is This A Revisit?	Virtual?	Date of Last Interview/Visit?	Street	City	State
					Zip Code
Not Governed By 49 CFR Part 659?		Agency Website:			
Agency Size:		Company Chosen By:			
Average DAILY Ridership (Number Only):		HTUA Name:			
Grant Funding - Section 5311 of Title 49:			Most Recent Grant Received in:		

Types of Service (Check all that apply)					EXIS Conducted
Light Rail		Inclined Plane		Tourist / Scenic	
Heavy Rail		Funicular		Commuter	
Rapid Rail		Trolley		Intercity	RMAST Conducted
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		

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY Transportation Security Administration					
Mass Transit					
Mass Transit Baseline Assessment for Security Enhancements (MT-BASE)				MTPR FY2021 V.2 (January 2021)	
Company Name:		Lead Inspector:		0	
0		Assessment Date:		1/4/2021	
Section	Description	N/A	Findings Score	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) which addresses personnel security, facility security, vehicle security and Threat/Vulnerability Management?				
1.102	Does the SSP identify and actively monitor 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, such as 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 systems? (i.e., facilities, stations, terminals, offices building, underwater tunnels, underground stations/ tunnels and other critical systems)				
1.106	Does the SSP contain or reference other documents establishing procedures for the management of security incidents by the operations control center (or dispatch center) or other formal process?				
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	Has the agency partnered with local law enforcement/ first responders to develop active shooter procedures or protocols?				
1.109	Does the SSP contain or reference other documents that establish procedures or protocols for responding to active shooter events?				
1.110	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)?				
1.111 / T3	Are visible, random security measures, based on employee type, integrated into security plans to introduce unpredictability into security activities for deterrent effect?				
1.112	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?				
1.113	Does the SSP include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) principles as part of the agency's engineering practices?				
1.114	Does the SSP require an annual review?				
1.115	Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?				
1.116	Has an annual review of the SSP been performed and documented in the preceding 12 months?				
1.117	Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP?				
1.118	Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?				

SENSITIVE SECURITY INFORMATION

1.200 Emergency Response Plan (ERP)					
1.201	Does the transit agency have an Emergency Response Plan (ERP) which addresses specific policies and procedures related to emergency response.				
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, such as 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? (i.e. 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 documented lines of delegated authority and lines of succession of security responsibilities?				
2.103	Does the SSP or other documents establish roles and responsibilities for security and/or law enforcement personnel based on title and/or position?				
2.104	Does the SSP or other documents establish security-related roles and responsibilities for non-security personnel based on title and/or position? (i.e., operators, conductors, maintenance workers and station attendants)				
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 reference guides or other written instructions or procedures, appropriate to job function, 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?				

SENSITIVE SECURITY INFORMATION

2.200 Emergency Response Plan (ERP):					
2.201	Does the ERP establish and assign responsibility for implementation of the emergency response program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?				
2.202	Are detailed, comprehensive emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?				
2.203 / T5	Does the ERP establish emergency response roles and responsibilities for all front-line personnel based on title and/or position? (i.e. system law enforcement, system security officials, train or vehicle operators, conductors, station attendants, maintenance workers)				
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	How frequently do managers and supervisors provide information to front-line personnel where security and emergency response issues are the primary focus?				
3.102	How frequently are supervisor, manager, and/or foreperson security review and coordination briefings held?				
3.103	Does the agency have a program that actively utilizes a formal process for confirming personnel have a measurable working knowledge of security protocols? (i.e. internal audits, challenge procedures, qualification testing)				
3.104	Does the agency have a written policy requiring managers and/or supervisors to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?				
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 from 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 a process for sharing information 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.	X			

SENSITIVE SECURITY INFORMATION

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 regarding security orientation/awareness provided to all employees regardless of position or job function in a formal manner?			
5.103 / T4	Is annual refresher training provided regarding security orientation/awareness to managers and supervisors?	X		
5.104 / T4	Is annual refresher training provided regarding security orientation/awareness to front-line employees?	X		
5.105	Is ongoing advanced security training focused on job function provided at least annually?			
5.106	Is initial training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function, in a formal manner?			
5.107	Is annual refresher training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function?			
5.108 / T4	Is initial training provided to all new transit employees regarding emergency response?			
5.109 / T4	Is annual refresher training regarding emergency response provided to all employees regardless of position or job function in a formal manner?			
5.110 / T4		X		
5.111 / T4		X		
5.112 / T4	Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System (NIMS)?			
5.113	Has ICS and NIMS training appropriate to the position been provided to Senior Management staff and supervisors? (Describe the frequency of training)			
5.114	Has ICS and NIMS training appropriate to the position been provided to frontline employees? (Describe the frequency of training)			
5.115	Has ICS and NIMS training appropriate to the position been provided to front-line employees at least annually?	X		
5.116	Has the agency developed a program and provided training on its own incident response protocols?			
5.117 / T4	Is annual refresher training on the agency's incident response protocols appropriate to the position been provided to all employees regardless of position or job function?			
5.118 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to managers and supervisors?	X		
5.119 / T4	Has training on the agency's incident response protocols appropriate to the position been provided to front-line employees at least annually?	X		
5.120 / 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?			
5.121	Has training focused on IEDs and WMDs appropriate to the position been provided to all employees regardless of position or job function at least annually?			
5.122	Has training focused on IEDs and WMDs appropriate to the position been provided to manager and supervisors?	X		
5.123	Has training focused on IEDs and WMDs appropriate to the position been provided to front-line employees at least annually?	X		
5.124	Do law enforcement/security department personnel, security managers at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.			
5.125	Do law enforcement/security department personnel at the agency receive specialized training supporting their incident management and emergency response roles at least annually? Summarize program in the justification.			
5.126	Does the agency have an established program to monitor and schedule employee training?			
5.127	Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?			
5.128	Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?			
5.129	Does the agency have a program to regularly review and update security awareness and emergency response training materials?			

SENSITIVE SECURITY INFORMATION

5.130 / T4	Are all appropriate personnel notified via briefings, email, voicemail, or signage of changes in threat condition, protective measures or the employee watch programs?				
5.131 / 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.				
5.132 / T1	Has the agency provided training to regional first responders to enable them to operate in critical facilities and infrastructure?				
5.133	Has the agency provided local law enforcement/first responders opportunities to familiarize themselves with agency's system for response to emergencies? (e.g. Active Shooter, etc.)				
5.134 / T3	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?				
5.135 / T4	Has the agency implemented a program to train or orient first responders and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?				
HOMELAND SECURITY ADVISORY SYSTEM (HSAS)					
6.000 Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system					
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 a security concern? (e.g., 1-800 number, smart phone applications, social media, etc.)				
7.107	Does the agency issue public service announcements or press releases to social media regarding security and emergency protocols? (e.g. Twitter/ Facebook/etc., QRC codes, and/or apps for smart phones)				
7.108 / T6	Does the agency issue public service announcements or press releases to local media regarding security or emergency protocols? (e.g. newspaper, radio and/or television)				
7.109	Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response? If so, describe training program and activities.				
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 facilities?				
7.112	Does the agency track and monitor customer complaints reported by passengers?				

SENSITIVE SECURITY INFORMATION

RISK MANAGEMENT					
8.000	Establish and use a risk management process				
8.101 / T2	Does the agency have its own risk assessment process, approved by its management, for managing threats and vulnerabilities? If so, summarize the process in the justification.				
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 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 agency report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?				
9.103	Does the agency have policies requiring employees to report (internal or external) suspicious activity to their supervisor or management?				
9.104 / 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)?				
9.105	Does the agency routinely receive threat and intelligence information directly from any Federal government agency, State Homeland Security Office, Regional or State Intelligence Fusion Center, PT-ISAC, or other transit agencies? If so, describe frequency.				
9.106	Does the agency report their NTD security data to FTA as required by 49 CFR 659?				

SENSITIVE SECURITY INFORMATION

DRILLS AND EXERCISES				
10.000 Conduct Tabletop and Functional Drills				
10.101	Does the agency have a documented process to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills?			
10.102	Does the agency's 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 SPP or a related document include a requirement for annual field exercises, tabletops and drills?			
10.105	Does the agency's SPP or SSP describe or reference how the agency documents the results of its emergency preparedness evaluations? (i.e., briefings, after action reports and implementation of findings)			
10.106	Does the agency's SPP 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	In the last year, has the agency conducted drills or exercises specifically focus on active shooter scenarios with its employees?			
10.109 / 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)?			
10.110 / 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			
10.111 / T5	In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings or corrective actions? If so, summarize the actions taken in the justification.			
10.112	Has the agency established a system for objectively measure and assess its performance during emergency exercises and to measure improvements?			
10.113 / 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 throughout the agencies system? (i.e., facilities, stations, office buildings, terminals, underwater/ underground infrastructure and other critical systems)			
10.114 / T5	Does the transit system integrate local and regional first responders in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place.			
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.)?			

SENSITIVE SECURITY INFORMATION

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 documented procedures for issuing ID badges to visitors and contractors?				
12.105	Does the agency have a documented policy that requires visitors to be escorted when 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	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 critical systems? (i.e., CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems)				
12.112	Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?				
12.113	Does the agency provide a method for passengers and visitors to report security and safety concerns from within the agency's system?				
12.114	Does the transit agency 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 modifications? (including fire detection systems, firewalls and flame-resistant materials, back-up powered emergency lighting, defaults in turnstile and other systems supporting emergency exists, and pre-recorded public announcements)				
12.118	Is directional signage with adequate lighting provided in a consistent manner throughout their system, both to provide orientation and to support emergency evacuation?				
12.119	Are gates and locks used on all facility doors to prevent unauthorized access during operating hours?				
12.120	Are keys controlled through an established program that is documented?				
12.121	Are gates and locks 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, fire detection, alarm and suppression systems; public address; call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?				
12.125	Has the agency removed non-explosive resistant trash receptacles from platform areas of 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?				
12.127 / T1	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available through mutual aid agreements with other law enforcement agencies?				
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? Describe frequency of inspection.				
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? Describe specific examples where improvements to policy or procedures have occurred.				

SENSITIVE SECURITY INFORMATION

13.106 / T2	Does the agency conduct frequent inspections of its critical systems access points, ventilation systems, and the interior of underground/underwater assets for indications of suspicious activity?				
13.107	Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect? Describe how.				
13.108	Is there a process in place to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.				
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 Contractors					
14.101 / T2	Does the agency conduct background investigations on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems? (i.e., criminal history and motor vehicle records)				
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	Does the agency have a documented process for conducting background investigations?				
14.105	Is the criteria for background investigations based on employee type and responsibility, and is access documented?				

SENSITIVE SECURITY INFORMATION

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
--	----------

SENSITIVE SECURITY INFORMATION

Date of Visit	TSA Field Office	Lead TSI Inspector
1/4/2021	0	0
Agency Name		
0		
Additional Information		
General Description of the Entity: 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.		

	SAI 1	SAI 2	SAI 3	SAI 4
Enter Previous BASE Implementation >>>				
Select SAI's to be Targeted>>>				

For a BASE Assessment targeting of the levels of implementation from Assessment in the yellow cells above in the box directly below the SAI to current targeted BASE Assessment

If this is NOT a Targeted SAI BASE BASE levels of implementation in the number to the right. Leave it at

SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12

For specific SAI's, please enter in all cells from the agency's previous BASE Assessment. Then place the number (1-5) to be targeted to identify the priority.

In the box below, enter the targeted BASE Assessment.

1

For the BASE Assessment, fill in the previous BASE Assessment in the yellow cells above. Disregard the number "1".

SAI 13	SAI 14	SAI 15	SAI 16	SAI 17	Overall

enter the current
assessment (1-5)

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY		
Transportation Security Administration		
Mass Transit Baseline Assessment for Security Enhancements (MT-BASE)		MTPR FY2021 V.2 (January 2021)
Agency Name:	0	Lead Inspector: 0
		Assessment Date: 1/4/2021

SPT #	STRATEGIC PERFORMANCE TARGETS	Implementation
1	Comprehensive Drill and Exercise program for reinforcing implementation of security centered around agency specific security plans, policies, and procedures. (TSA recommends EXIS)	0%
2	Security Awareness Training program for employee implementation of agency specific security plans, policies, and procedures. (TSA recommends FOP/RMAST)	0%
3	Comprehensive Audit and Inspection program for adherence with implementation of agency specific security plans, policies, and procedures. (TSA recommends SETA)	0%

SAI #	SECURITY ACTION ITEM (SAI) DESCRIPTION	Implementation	Baseline
1	Establish written Security Programs and Emergency Management Plans	0%	0%
2	Define roles and responsibilities for security and emergency management	0%	0%
3	Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control	0%	0%
4	Coordinate Security and Emergency Management Plan(s) with local and regional agencies	0%	0%
5	Establish and maintain a Security and Emergency Training Program	0%	0%
6	Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system	0%	0%
7	Implement and reinforce a Public Security and Emergency Awareness program	0%	0%
8	Establish and use a risk management process	0%	0%
9	Establish and use an information sharing process for threat and intelligence information	0%	0%
10	Conduct Tabletop and Functional Drills	0%	0%
11	Developing a Comprehensive Cyber Security Strategy	0%	0%
12	Control access to security critical facilities with ID badges for all visitors, employees and contractors	0%	0%
13	Conduct physical security inspections	0%	0%
14	Conduct background investigations of employees and contractors	0%	0%
15	Control access to documents of security-critical systems and facilities	0%	0%
16	Ensure existence of a process for handling and access to Sensitive Security Information (SSI)	0%	0%
17	Conduct Security Program audits	0%	0%

Overall Implementation:	0.00%	0.00%
--------------------------------	--------------	--------------

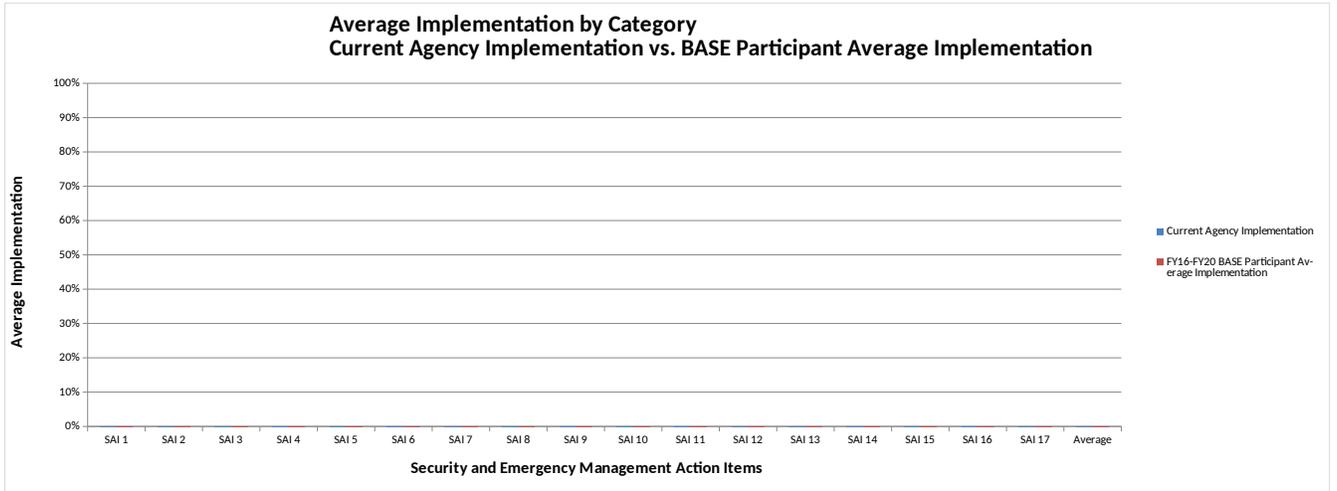
Color Key:

	Requirements have been met.
	Requirements are partially met and/or are in the process of being completed.
	Does not meet requirements as described in reference materials.

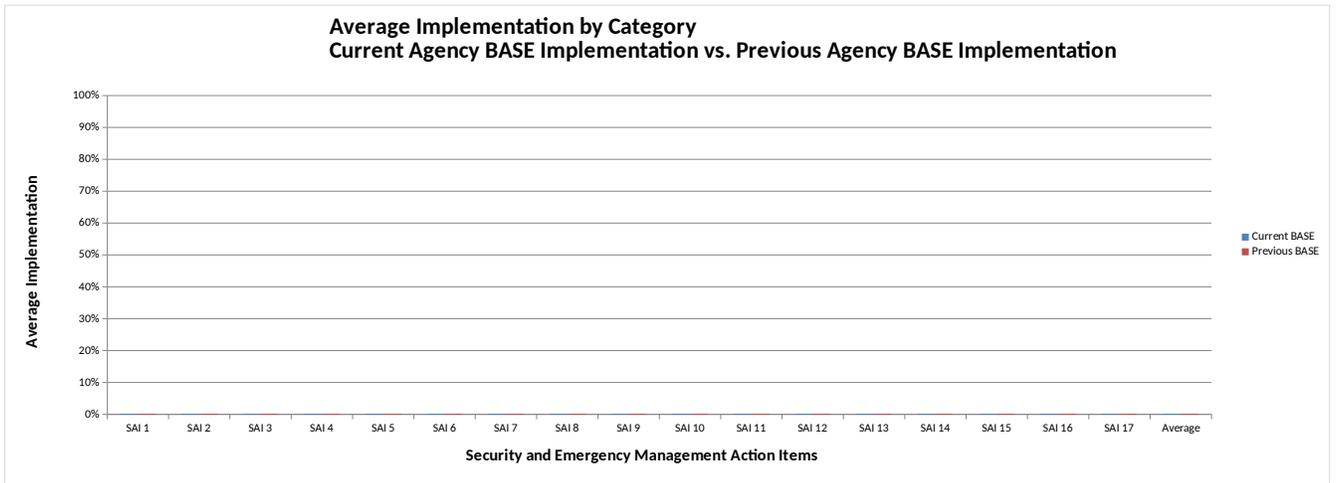
This Agency Did Not Meet the Requirements of the Gold Standard Award.

SENSITIVE SECURITY INFORMATION

Current Stakeholder vs. BASE Participant Average																		
	SAI 1	SAI 2	SAI 3	SAI 4	SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12	SAI 13	SAI 14	SAI 15	SAI 16	SAI 17	Average
Current Agency Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
BASE Participant Average Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Difference	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%



Current BASE vs. Previous BASE Comparison																		
	SAI 1	SAI 2	SAI 3	SAI 4	SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12	SAI 13	SAI 14	SAI 15	SAI 16	SAI 17	Average
Current Agency Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Previous Agency BASE Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Difference	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%



SENSITIVE SECURITY INFORMATION

BASE Technical Scoring Sheet

This sheet is for data analysis only.

Totals	0.000000	792.000000	0.00%
---------------	-----------------	-------------------	--------------

Totals	0.000000	356.000000	0.00%
---------------	-----------------	-------------------	--------------

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)				0.000000	120.000000	0.00%
1.100		System Security Plan (SSP)				0.000000	72.000000	0%
1.101	B	Does the transit agency have a System Security Plan (SSP) which addresses personnel security, facility security, vehicle security and Threat/Vulnerability Management?	0	1.000000	1	0	4.000000	0%
1.102		Does the SSP identify and actively monitor the goals and objectives for the security program?	0	1.000000	1	0	4.000000	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, such as the agency's chief executive?	0	1.000000	1	0	4.000000	0%
1.104	B	Is the SSP separate from the agency's System Safety Program Plan (SSPP)?	0	1.000000	1	0	4.000000	0%
1.105	B T1	Do the Security and Emergency Response Plans address protection and response for critical systems? (i.e., facilities, stations, terminals, offices building, underwater tunnels, underground stations/ tunnels and other critical systems)	0	1.000000	1	0	4.000000	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) or other formal process?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
1.108		Has the agency partnered with local law enforcement/ first responders to develop active shooter procedures or protocols?	0	1.000000	1	0	4.000000	0%
1.109		Does the SSP contain or reference other documents that establish procedures or protocols for responding to active shooter events?	0	1.000000	1	0	4.000000	0%
1.110		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	1.000000	1	0	4.000000	0%
1.111	T3	Are visible, random security measures, based on employee type, integrated into security plans to introduce unpredictability into security activities for deterrent effect?	0	1.000000	1	0	4.000000	0%
1.112		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	1.000000	1	0	4.000000	0%
1.113		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	1.000000	1	0	4.000000	0%
1.114		Does the SSP require an annual review?	0	1.000000	1	0	4.000000	0%
1.115		Does the transit agency produce periodic reports reviewing its progress in meeting its SSP goals and objectives?	0	1.000000	1	0	4.000000	0%
1.116		Has an annual review of the SSP been performed and documented in the preceding 12 months?	0	1.000000	1	0	4.000000	0%
1.117		Does the SSP outline a process for securing SSO agency review and approval of updates to the SSP?	0	1.000000	1	0	4.000000	0%
1.118		Has the transit agency submitted and received documentation from the SSO confirming its review and approval of the SSP currently in effect?	0	1.000000	1	0	4.000000	0%
1.200		Emergency Response Plan (ERP)				0.000000	48.000000	0%
1.201	B	Does the transit agency have an Emergency Response Plan (ERP) which addresses specific policies and procedures related to emergency response.	0	1.000000	1	0	4.000000	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, such as the agency's chief executive?	0	1.000000	1	0	4.000000	0%
1.203	B	Does the ERP require an annual review to determine if it needs to be updated?	0	1.000000	1	0	4.000000	0%
1.204		Has an annual review of the ERP been performed and documented in the preceding 12 months?	0	1.000000	1	0	4.000000	0%
1.205	B	Does the ERP include a process or review provision to ensure coordination with the transit agency's SSPP and SSP?	0	1.000000	1	0	4.000000	0%
1.206		Has the transit agency received documentation from the SSO confirming its review and approval of the ERP currently in effect?	0	1.000000	1	0	4.000000	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? (i.e. law enforcement, local EMA, fire departments, etc.)	0	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail			
Line	Element 1	Grade	
Grade:		0.00%	
	0.000000	48.000000	0.00%
Totals:	0.000000	20.000000	0%
1.101	0.000000	4.000000	0%
1.102			
1.103	0.000000	4.000000	0%
1.104	0.000000	4.000000	0%
1.105	0.000000	4.000000	0%
1.106			
1.107	0.000000	4.000000	0%
1.108			
1.109			
1.110			
1.111			
1.112			
1.113			
1.114			
1.115			
1.116			
1.117			
1.118			
1.200	0.000000	28.000000	0%
1.201	0.000000	4.000000	0%
1.202	0.000000	4.000000	0%
1.203	0.000000	4.000000	0%
1.204			
1.205	0.000000	4.000000	0%
1.206			
1.207	0.000000	4.000000	0%

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
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	1.000000	1	0	4.000000	0%
1.209		Does the ERP contain or reference other documents to provide for Continuity of Operations (COOP) while responding to emergency events?	0	1.000000	1	0	4.000000	0%
1.210		Does the agency have a written Business Recovery Plan to guide restoration of facilities and services following an emergency event?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
1.212	B	Does the agency have a back-up operations control center capability?	0	1.000000	1	0	4.000000	0%
2.000		Define Roles and Responsibilities for Security and Emergency Management				0	68	0%
2.100		System Security Plan (SSP)				0	40.000000	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	1.000000	1	0	4.000000	0%
2.102		Has the agency established documented lines of delegated authority and lines of succession of security responsibilities?	0	1.000000	1	0	4.000000	0%
2.103	B	Does the SSP or other documents establish roles and responsibilities for security and/or law enforcement personnel based on title and/or position?	0	1.000000	1	0	4.000000	0%
2.104	B	Does the SSP or other documents establish security-related roles and responsibilities for non-security personnel based on title and/or position? (i.e., operators, conductors, maintenance workers and station attendants)	0	1.000000	1	0	4.000000	0%
2.105	T2	Do senior staff and middle management conduct security meetings to review recommendations for changes to plans and processes?	0	1.000000	1	0	4.000000	0%
2.106		Does a Security Review Committee (or other designated group) regularly review security incident reports, trends, and program audit findings?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
2.108	B	Have reference guides or other written instructions or procedures, appropriate to job function, been distributed to transit employees to implement the requirements of the SSP?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
2.11		Does the agency maintain a record of security related incidents that are reported within the agency?	0	1.000000	1	0	4.000000	0%
2.200		2.b. Emergency Response Plan (ERP):				0.00000	28.00000	0%
2.201		Does the ERP establish and assign responsibility for implementation of the emergency response program to a Senior Manager who is a "direct report" to the agency's Chief Executive Officer?	0	1.000000	1	0	4.000000	0%
2.202	B	Are detailed, comprehensive emergency response roles and responsibilities for all departments identified in the ERP or other supporting documents?	0	1.000000	1	0	4.000000	0%
2.203	B T5	Does the ERP establish emergency response roles and responsibilities for all front-line personnel based on title and/or position? (i.e. system law enforcement, system security officials, train or vehicle operators, conductors, station attendants, maintenance workers)	0	1.000000	1	0	4.000000	0%
2.204	B	Has the ERP been distributed to appropriate departments in the organization?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
2.206		Are senior staff and middle management ERP coordination meetings held on a regular basis?	0	1.000000	1	0	4.000000	0%
2.207	B	Are informational briefings with appropriate personnel held whenever emergency response protocols are substantially changed or updated?	0	1.000000	1	0	4.000000	0%
3.000		Ensure that operations and maintenance supervisors, forepersons and managers are held accountable for security issues under their control				0.0000	16.0000	0%
3.101	B	How frequently do managers and supervisors provide information to front-line personnel where security and emergency response issues are the primary focus?	0	1.000000	1	0	4.000000	0%
3.102		How frequently are supervisor, manager, and/or foreperson security review and coordination briefings held?	0	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail			
Line	Element 1		Grade
Grade:		0.00%	
1.208	0.000000	4.000000	0%
1.209			
1.210			
	0.000000	4.000000	0%
2	0	40	0%
2.100	0.000000	20.000000	0%
2.101			
2.102			
2.103	0.000000	4.000000	0%
2.104	0.000000	4.000000	0%
2.105			
2.106			
2.107	0.000000	4.000000	0%
2.108	0.000000	4.000000	0%
2.109	0.000000	4.000000	0%
2.200	0.000000	20.000000	0%
2.201			
2.202	0.000000	4.000000	0%
2.203	0.000000	4.000000	0%
2.204	0.000000	4.000000	0%
2.205	0.000000	4.000000	0%
2.206			
2.207	0.000000	4.000000	0%
3.000	0.000000	12.000000	0%
3.101	0.000000	4.000000	0%
3.102			

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
3.103	B	Does the agency have a program that actively utilizes a formal process for confirming personnel have a measurable working knowledge of security protocols? (i.e. internal audits, challenge procedures, qualification testing)	0	1.000000	1	0	4.000000	0%
3.104	B	Does the agency have a written policy requiring managers and/or supervisors to debrief front-line employees regarding their involvement in or management of any security or emergency incidents?	0	1.000000	1	0	4.000000	0%
4.000		Coordinate Security and Emergency Management Plan(s) with local and regional agencies				0.0000	40.0000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
4.103	B	Have regional incident management protocols been shared with the agency and incorporated into the agency's ERP/SSP/SEPP?	0	1.000000	1	0	4.000000	0%
4.104		Have agency resources been appropriately identified and provided to the regional EMA?	0	1.000000	1	0	4.000000	0%
4.105	B	Does the agency have a designated point-of-contact or liaison from the local/regional Emergency Operations Center (EOC)?	0	1.000000	1	0	4.000000	0%
4.106		Does the agency send a representative to the local/regional EOC, should it be activated?	0	1.000000	1	0	4.000000	0%
4.107		Does the agency have a process for sharing information with the regional/local EOC (i.e., contacts, procedures, resource inventories, etc.)?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
4.109		Have the agency's emergency response protocols been shared with the EMA and appropriate first responder agencies?	0	1.000000	1	0	4.000000	0%
4.110	B T5	Has the transit system tested its communications systems for interoperability with appropriate emergency response agencies?	0	1.000000	1	0	4.000000	0%
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	1.000000	0	0	0.000000	#DIV/0!
SECURITY AND EMERGENCY RESPONSE TRAINING								
5.000		Establish and Maintain a Security and Emergency Training Program				0.0000	104.0000	0%
5.101	B T4	Is initial training provided to all new agency employees regarding security orientation/awareness?	0	1.000000	1	0	4.000000	0%
5.102	T4	Is annual refresher training regarding security orientation/awareness provided to all employees regardless of position or job function in a formal manner?	0	1.000000	1	0	4.000000	0%
5.103	B T4	Is annual refresher training provided regarding security orientation/awareness to managers and supervisors?	0	1.000000	0	0	0.000000	#DIV/0!
5.104	B T4	Is annual refresher training provided regarding security orientation/awareness to front-line employees?	0	1.000000	0	0	0.000000	#DIV/0!
5.105		Is ongoing advanced security training focused on job function provided at least annually?	0	1.000000	1	0	4.000000	0%
5.106		Is initial training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function, in a formal manner?	0	1.000000	1	0	4.000000	0%
5.107		Is annual refresher training specific to active shooter (run/fight/hide, Lockdown procedures or similar) provided to all employees regardless of position or job function?	0	1.000000	1	0	4.000000	0%
5.108	B T4	Is initial training provided to all new transit employees regarding emergency response?	0	1.000000	1	0	4.000000	0%
5.109	T4	Is annual refresher training regarding emergency response provided to all employees regardless of position or job function in a formal manner?	0	1.000000	1	0	4.000000	0%
5.110	B T4	Is annual refresher training provided regarding emergency response to Managers and Supervisors?	0	1.000000	0	0	0.000000	#DIV/0!
5.111	B T4	Is annual refresher training provided regarding emergency response to front-line Employees?	0	1.000000	0	0	0.000000	#DIV/0!
5.112	B T4	Have agency employees received general training on Incident Command System (ICS) procedures in accordance with National Incident Management System (NIMS)?	0	1.000000	1	0	4.000000	0%
5.113		Has ICS and NIMS training appropriate to the position been provided to Senior Management staff and supervisors? (Describe the frequency of training)	0	1.000000	1	0	4.000000	0%
5.114	B	Has ICS and NIMS training appropriate to the position been provided to frontline employees? (Describe the frequency of training)	0	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail

Line	Element 1	Grade
Grade:		0.00%
3.103	0.000000	4.000000
3.104	0.000000	4.000000
4.000	0.000000	20.000000
4.101		
4.102	0.000000	4.000000
4.103	0.000000	4.000000
4.104		
4.105	0.000000	4.000000
4.106		
4.107		
4.108	0.000000	4.000000
4.109		
4.110	0.000000	4.000000
4.111	0.000000	0.000000
5.000	0.000000	40.000000
5.101	0.000000	4.000000
5.102		
5.103	0.000000	0.000000
5.104	0.000000	0.000000
5.105		
5.106		
5.107		
5.108	0.000000	4.000000
5.109		
5.110	0.000000	0.000000
5.111	0.000000	0.000000
5.112	0.000000	4.000000
5.113		
5.114	0.000000	4.000000

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
5.115		Has ICS and NIMS training appropriate to the position been provided to front-line employees at least annually?	0	1.000000	0	0	0.000000	#DIV/0!
5.116	B	Has the agency developed a program and provided training on its own incident response protocols?	0	1.000000	1	0	4.000000	0%
5.117	T4	Is annual refresher training on the agency's incident response protocols appropriate to the position been provided to all employees regardless of position or job function?	0	1.000000	1	0	4.000000	0%
5.118	B T4	Has training on the agency's incident response protocols appropriate to the position been provided to managers and supervisors?	0	1.000000	0	0	0.000000	#DIV/0!
5.119	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	1.000000	0	0	0.000000	#DIV/0!
5.12	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	1.000000	1	0	4.000000	0%
5.121		Has training focused on IEDs and WMDs appropriate to the position been provided to all employees regardless of position or job function at least annually?	0	1.000000	1	0	4.000000	0%
5.122		Has training focused on IEDs and WMDs appropriate to the position been provided to manager and supervisors?	0	1.000000	0	0	0.000000	#DIV/0!
5.123		Has training focused on IEDs and WMDs appropriate to the position been provided to front-line employees at least annually?	0	1.000000	0	0	0.000000	#DIV/0!
5.124		Do law enforcement/security department personnel, security managers at the agency receive specialized training in counter-terrorism annually? Summarize program in the justification.	0	1.000000	1	0	4.000000	0%
5.125		Do law enforcement/security department personnel at the agency receive specialized training supporting their incident management and emergency response roles at least annually? Summarize program in the justification.	0	1.000000	1	0	4.000000	0%
5.126	B	Does the agency have an established program to monitor and schedule employee training?	0	1.000000	1	0	4.000000	0%
5.127		Does the agency have a system that records and tracks personnel training for all security-related courses (including initial, annual, periodic and other)?	0	1.000000	1	0	4.000000	0%
5.128		Does the transit agency have a system that records and tracks personnel training for emergency response courses (including initial, periodic and other)?	0	1.000000	1	0	4.000000	0%
5.129		Does the agency have a program to regularly review and update security awareness and emergency response training materials?	0	1.000000	1	0	4.000000	0%
5.130	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	1.000000	1	0	4.000000	0%
5.131	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	1.000000	1	0	4.000000	0%
5.132	B T1	Has the agency provided training to regional first responders to enable them to operate in critical facilities and infrastructure?	0	1.000000	1	0	4.000000	0%
5.133		Has the agency provided local law enforcement/first responders opportunities to familiarize themselves with agency's system for response to emergencies? (e.g. Active Shooter, etc.)	0	1.000000	1	0	4.000000	0%
5.134	T3	Does training of transit system law enforcement and/or security personnel integrate the concept and employment of visible, random security measures?	0	1.000000	1	0	4.000000	0%
5.135	B T4	Has the agency implemented a program to train or orient first responders and other potential supporting assets (e.g., TSA regional personnel for VIPR exercises) on their system vehicle familiarization?	0	1.000000	1	0	4.000000	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	12.0000	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	1.000000	1	0	4.000000	0%
6.102	B T2	Does the agency have actionable operational response protocols for the specific threat scenarios from NTAS?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
PUBLIC AWARENESS								
7.000		Implement and reinforce a Public Security and Emergency Awareness program				0.0000	48.0000	0%

Baseline Security Scoring Detail		
Line	Element 1	Grade
Grade:		0.00%
5.115		
5.116	0.000000	4.000000 0%
5.117		
5.118	0.000000	0.000000 #DIV/0!
5.119	0.000000	0.000000 #DIV/0!
5.12		
5.121		
5.122		
5.123		
5.124		
5.125		
5.126	0.000000	4.000000 0%
5.127		
5.128		
5.129		
5.130	0.000000	4.000000 0%
5.131	0.000000	4.000000 0%
5.132	0.000000	4.000000 0%
5.133		
5.134		
5.135	0.000000	4.000000 0%
6.000	0.000000	8.00000 0%
6.101	0.000000	4.000000 0%
6.102	0.000000	4.000000 0%
6.103		
7.000	0.000000	24.000000 0%

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
7.101	B	Has the transit agency developed and implemented a public security and emergency awareness program?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
7.103	T6	Is the above consistent with agency's overall announcement program?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
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	1.000000	1	0	4.000000	0%
7.106	B T6	Does the agency have an appropriate mechanism in place for passengers to communicate a security concern? (e.g., 1-800 number, smart phone applications, social media, etc.)	0	1.000000	1	0	4.000000	0%
7.107		Does the agency issue public service announcements or press releases to social media regarding security and emergency protocols? (e.g. Twitter/ Facebook/etc., QRC codes, and/or apps for smart phones)	0	1.000000	1	0	4.000000	0%
7.108	T6	Does the agency issue public service announcements or press releases to local media regarding security or emergency protocols? (e.g. newspaper, radio and/or television)	0	1.000000	1	0	4.000000	0%
7.109		Does the transit agency conduct a volunteer training program for non-employees to aid with system evacuations and emergency response? If so, describe training program and activities.	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
7.111	B T1	Do public awareness materials and/or messages inform passengers on the means to evacuate safely from transit vehicles and facilities?	0	1.000000	1	0	4.000000	0%
7.112		Does the agency track and monitor customer complaints reported by passengers?	0	1.000000	1	0	4.000000	0%
RISK MANAGEMENT								
8.000		Establish and use a risk management process				0.0000	28.0000	0%
8.101	B T2	Does the agency have its own risk assessment process, approved by its management, for managing threats and vulnerabilities? If so, summarize the process in the justification.	0	1.000000	1	0	4.000000	0%
8.102	B	Has the agency identified facilities and systems it considers to be its critical assets?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
8.105	B T2	Has the system implemented procedures to limit and monitor access to underground and underwater tunnels? If so, summarize procedures in the justification.	0	1.000000	1	0	4.000000	0%
8.106		Are security investments prioritized using information developed in the risk assessment process?	0	1.000000	1	0	4.000000	0%
8.107	B T1	Upon request, has TSA been provided access to the agency's vulnerability assessments, Security Plan and related documents?	0	1.000000	1	0	4.000000	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	24.0000	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	1.000000	1	0	4.000000	0%
9.102	B T2	Does the agency report threat and intelligence information directly to FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force?	0	1.000000	1	0	4.000000	0%
9.103		Does the agency have policies requiring employees to report (internal or external) suspicious activity to their supervisor or management?	0	1.000000	1	0	4.000000	0%
9.104	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	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail		
Line	Element 1	Grade
Grade:		0.00%
7.101	0.000000	4.000000
7.102	0.000000	4.000000
7.103		
7.104	0.000000	4.000000
7.105	0.000000	4.000000
7.106	0.000000	4.000000
7.107		
7.108		
7.109		
7.110		
7.111	0.000000	4.000000
7.112		
8.000		0.000000
8.101	0.000000	4.000000
8.102	0.000000	4.000000
8.103	0.000000	4.000000
8.104	0.000000	4.000000
8.105	0.000000	4.000000
8.106		
8.107	0.000000	4.000000
9.000		0.000000
9.101	0.000000	4.000000
9.102	0.000000	4.000000
9.103		
9.104	0.000000	4.000000

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
9.105		Does the agency routinely receive threat and intelligence information directly from any Federal government agency, State Homeland Security Office, Regional or State Intelligence Fusion Center, PT-ISAC, or other transit agencies? If so, describe frequency.	0	1.000000	1	0	4.000000	0%
9.106		Does the agency report their NTD security data to FTA as required by 49 CFR 659?	0	1.000000	1	0	4.000000	0%
DRILLS AND EXERCISES								
10.000		Conduct Tabletop and Functional Drills		0.0000			56.0000	0%
10.101	B	Does the agency have a documented process to develop an approved, coordinated schedule for all emergency management program activities, including local/regional emergency planning and participation in exercises and drills?	0	1.000000	1	0	4.000000	0%
10.102	B	Does the agency's or SSP describe or reference how the agency performs its emergency planning responsibilities and requirements regarding emergency drills and exercises?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
10.104	B	Does the agency's SPP or a related document include a requirement for annual field exercises, tabletops and drills?	0	1.000000	1	0	4.000000	0%
10.105	B	Does the agency's SPP or SSP describe or reference how the agency documents the results of its emergency preparedness evaluations? (i.e., briefings, after action reports and implementation of findings)	0	1.000000	1	0	4.000000	0%
10.106		Does the agency's SPP or a related document describe or reference its program for providing employee training on emergency response protocols and procedures?	0	1.000000	1	0	4.000000	0%
10.107	B	Does the agency participate as an active player in full-scale, regional exercises, held at least annually?	0	1.000000	1	0	4.000000	0%
10.108		In the last year, has the agency conducted drills or exercises specifically focus on active shooter scenarios with its employees?	0	1.000000	1	0	4.000000	0%
10.109	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	1.000000	1	0	4.000000	0%
10.110	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	1.000000	1	0	4.000000	0%
10.111	T5	In the last 12 months, has the agency updated plans, protocols and processes to incorporate after-action report recommendations/findings or corrective actions? If so, summarize the actions taken in the justification.	0	1.000000	1	0	4.000000	0%
10.112		Has the agency established a system for objectively measure and assess its performance during emergency exercises and to measure improvements?	0	1.000000	1	0	4.000000	0%
10.113	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 throughout the agencies system? (i.e., facilities, stations, office buildings, terminals, underwater/ underground infrastructure and other critical systems)	0	1.000000	1	0	4.000000	0%
10.114	B T5	Does the transit system integrate local and regional first responders in drills, tabletop exercises, and/or field exercises? If so, summarize each joint event and state when it took place.	0	1.000000	1	0	4.000000	0%
11.000		Developing a Comprehensive Cyber Security Strategy		0.0000			28.0000	0%
11.101	B	Has the agency conducted a risk assessment to identify operational control and communication/business enterprise IT assets and potential vulnerabilities?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
11.103		Has a written strategy been developed and integrated into the overall security program to mitigate the cyber risk identified?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
11.106	B	Has the agency established a cyber-incident response and reporting protocol?	0	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail			
Line	Element 1		Grade
Grade:		0.00%	
9.105			
9.106			
10.000	0.000000	32.000000	0%
10.101	0.000000	4.000000	0%
10.102	0.000000	4.000000	0%
10.103	0.000000	4.000000	0%
10.104	0.000000	4.000000	0%
10.105	0.000000	4.000000	0%
10.106			
10.107	0.000000	4.000000	0%
10.108			
10.109			
10.110			
10.111			
10.112			
10.113	0.000000	4.000000	0%
10.114	0.000000	4.000000	0%
11.000	0.000000	8.000000	0%
11.101	0.000000	4.000000	0%
11.102			
11.103			
11.104			
11.105			
11.106	0.000000	4.000000	0%

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
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	1.000000	1	0	4.000000	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	108.0000	0%
12.101	B	Have assets and facilities requiring restricted access been identified?	0	1.000000	1	0	4.000000	0%
12.102	B	Are ID badges or other measures employed to restrict access to facilities not open to the public?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
12.104	B	Does the agency have documented procedures for issuing ID badges to visitors and contractors?	0	1.000000	1	0	4.000000	0%
12.105		Does the agency have a documented policy that requires visitors to be escorted when accessing non-public areas.	0	1.000000	1	0	4.000000	0%
12.106		Is CCTV equipment installed in transit agency facilities?	0	1.000000	1	0	4.000000	0%
12.107		Is CCTV equipment protecting critical assets interfaced with an access control system?	0	1.000000	1	0	4.000000	0%
12.108		Is CCTV equipment installed on transit vehicles?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
12.110		Does the agency use fencing, barriers, and/or intrusion detection to protect against unauthorized entry into stations, facilities, and other identified critical assets?	0	1.000000	1	0	4.000000	0%
12.111	B T2	Has the system implemented protective measures to secure high risk/high consequence assets and critical systems? (i.e., CCTV, intrusion detection systems, smart camera technology, fencing, enhanced lighting, access control, LE patrols, K-9s, protection of ventilation systems)	0	1.000000	1	0	4.000000	0%
12.112		Does the transit agency monitor a network of security, fire, duress, intrusion, utility and internal 911 alarm systems?	0	1.000000	1	0	4.000000	0%
12.113		Does the agency provide a method for passengers and visitors to report security and safety concerns from within the agency's system?	0	1.000000	1	0	4.000000	0%
12.114		Does the transit agency administer an automated employee access control system and perform corrective analysis of security breaches?	0	1.000000	1	0	4.000000	0%
12.115		Does the agency have policies and procedures for screening of mail and/or outside deliveries?	0	1.000000	1	0	4.000000	0%
12.116		Have locks, bullet resistant materials and anti-fragmentation materials been installed/used at critical locations?	0	1.000000	1	0	4.000000	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 modifications? (including fire detection systems, firewalls and flame-resistant materials, back-up powered emergency lighting, defaults in turnstile and other systems supporting emergency exists, and pre-recorded public announcements)	0	1.000000	1	0	4.000000	0%
12.118		Is directional signage with adequate lighting provided in a consistent manner throughout their system, both to provide orientation and to support emergency evacuation?	0	1.000000	1	0	4.000000	0%
12.119		Are gates and locks used on all facility doors to prevent unauthorized access during operating hours?	0	1.000000	1	0	4.000000	0%
12.120		Are keys controlled through an established program that is documented?	0	1.000000	1	0	4.000000	0%
12.121	B	Are gates and locks used to close down system facilities after operating hours?	0	1.000000	1	0	4.000000	0%
12.122		Do transit vehicles have radios, silent alarms, and/or passenger communication systems?	0	1.000000	1	0	4.000000	0%
12.123		Does the transit agency use graffiti-resistant/etch-resistant materials for walls, ceilings, and windows?	0	1.000000	1	0	4.000000	0%
12.124	B	Are Uninterruptible Power Supply (UPS) or redundant power sources provided for safety and security of critical equipment, fire detection, alarm and suppression systems; public address; call-for-aid telephones; CCTV; emergency trip stations; vital train control functions; etc.?	0	1.000000	1	0	4.000000	0%
12.125		Has the agency removed non-explosive resistant trash receptacles from platform areas of terminals and stations?	0	1.000000	1	0	4.000000	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?	0	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail		
Line	Element 1	Grade
Grade:		0.00%
11.107		
12.000	0.000000	32.000000 0%
12.101	0.000000	4.000000 0%
12.102	0.000000	4.000000 0%
12.103	0.000000	4.000000 0%
12.104	0.000000	4.000000 0%
12.105		
12.106		
12.107		
12.108		
12.109		
12.110		
12.111	0.000000	4.000000 0%
12.112		
12.113		
12.114		
12.115		
12.116		
12.117		
12.118		
12.119		
12.120		
12.121	0.000000	4.000000 0%
12.122		
12.123		
12.124	0.000000	4.000000 0%
12.125		
12.126	0.000000	4.000000 0%

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
12.127	T1	Does the agency have or utilize explosive detection canine teams, either maintained by the system or made available through mutual aid agreements with other law enforcement agencies?	0	1.000000	1	0	4.000000	0%
13.000		Conduct Physical Security Inspections				0.0000	36.0000	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? Describe frequency of inspection.	0	1.000000	1	0	4.000000	0%
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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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? Describe specific examples where improvements to policy or procedures have occurred.	0	1.000000	1	0	4.000000	0%
13.106	B T2	Does the agency conduct frequent inspections of its critical systems access points, ventilation systems, and the interior of underground/underwater assets for indications of suspicious activity?	0	1.000000	1	0	4.000000	0%
13.107		Does the system integrate randomness and unpredictability into its security activities to enhance deterrent effect? Describe how.	0	1.000000	1	0	4.000000	0%
13.108		Is there a process in place to ensure that in service vehicles are inspected at regular periodic intervals for suspicious or unattended items? Specify type and frequency of inspections.	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
BACKGROUND INVESTIGATIONS								
14.000		Conduct Background Investigations of Employees and Contractors				0.0000	20.0000	0%
14.101	B T2	Does the agency conduct background investigations on all new front-line operations and maintenance employees, and employees with access to sensitive security information, facilities and systems? (i.e., criminal history and motor vehicle records)	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
14.104	B	Does the agency have a documented process for conducting background investigations?	0	1.000000	1	0	4.000000	0%
14.105		Is the criteria for background investigations based on employee type and responsibility, and is access documented?	0	1.000000	1	0	4.000000	0%
DOCUMENT CONTROL								
15.000		Control Access to documents of security critical systems and facilities				0.0000	12.0000	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	1.000000	1	0	4.000000	0%
15.102	B	Has the agency designated a department/person responsible for administering the access control policy with respect to agency documents?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
16.000		Process for handling and access to Sensitive Security Information (SSI)				0.0000	16.0000	0%
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	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail		
Line	Element 1	Grade
Grade:	0.00%	
12.127		
13.000	0	12
13.101	0.000000	4.000000
13.102	0.000000	4.000000
13.103		
13.104		
13.105		
13.106	0.000000	4.000000
13.107		
13.108		
13.109		
14.000	0.000000	12.000000
14.101	0.000000	4.000000
14.102	0.000000	4.000000
14.103		
14.104	0.000000	4.000000
14.105		
15.000	0.000000	8.000000
15.101	0.000000	4.000000
15.102	0.000000	4.000000
15.103		
16.000	0.000000	8.000000
16.101	0.000000	4.000000

SENSITIVE SECURITY INFORMATION

Top 17 Scoring Detail

Category		Questions	Score	Weight	N/A	Points	Possible	Grade
MANAGEMENT AND ACCOUNTABILITY								
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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
SECURITY PROGRAM AUDITS								
17.000		Audit Program				0.0000	56.0000	0%
17.101		Has the agency established a schedule for conducting its internal security audit process?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
17.103	B	Has the transit agency established checklists and procedures to govern the conduct of its internal security audit process?	0	1.000000	1	0	4.000000	0%
17.104	B	Is the transit agency complying with its internal security audit schedule?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
17.108		Has the agency made its internal security audit schedule available to the SSO agency?	0	1.000000	1	0	4.000000	0%
17.109		Has the agency made checklists and procedures used in its internal security audits available to the SSO agency?	0	1.000000	1	0	4.000000	0%
17.110		Has the agency notified the SSO agency 30 days prior to the conduct of an internal security audit?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%
17.112		Has the agency's chief executive certified to the SSO agency that the agency is in compliance with its SSP?	0	1.000000	1	0	4.000000	0%
17.113		Was that certification included with the most recent annual report submitted to the SSO agency?	0	1.000000	1	0	4.000000	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	1.000000	1	0	4.000000	0%

Baseline Security Scoring Detail

Line	Element 1		Grade
Grade:		0.00%	
16.102	0.000000	4.000000	0%
16.103			
16.104			
17.000	0.000000	16.000000	0%
17.101			
17.102	0.000000	4.000000	0%
17.103	0.000000	4.000000	0%
17.104	0.000000	4.000000	0%
17.105	0.000000	4.000000	0%
17.106			
17.107			
17.108			
17.109			
17.110			
17.111			
17.112			
17.113			
17.114			

DO NOT MODIFY OR ENTER ANY DATA

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Mass Transit Agency Comprehensive SAI Checklist

Agency Name:

0

SAI #	SECURITY ACTION ITEM (SAI) DESCRIPTION
1	Establish written Security Programs and Emergency Management Plans
2	Define roles and responsibilities for security and emergency management
3	Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control
4	Coordinate Security and Emergency Management Plan(s) with local and regional agencies
5	Establish and maintain a Security and Emergency Training Program
6	Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system
7	Implement and reinforce a Public Security and Emergency Awareness program
8	Establish and use a risk management process
9	Establish and use an information sharing process for threat and intelligence information
10	Conduct Tabletop and Functional Drills
11	Developing a Comprehensive Cyber Security Strategy
12	Control access to security critical facilities with ID badges for all visitors, employees and contractors
13	Conduct physical security inspections
14	Conduct background investigations of employees and contractors
15	Control access to documents of security-critical systems and facilities
16	Ensure existence of a process for handling and access to Sensitive Security Information (SSI)
17	Conduct Security Program audits

Overall Implementation:

State Safety Oversight Agency	<i>Require Security Plan</i>	<i>Require Internal Security Reviews</i>	<i>Require Reporting and/or Investigations of Security Hazards or Incidents</i>
Total	22	21	12
Arizona Department of Transportation	X	X	X
Arkansas Highway and Transportation Department			
California Public Utilities Commission	X	X	
Colorado Public Utilities Commission			
District of Columbia Fire and Emergency Medical Services	X	X	X
Florida Department of Transportation*	X	X	

Georgia Department of Transportation	X	X	X
Hawaii Department of Transportation	X	X	X
Illinois Department of Transportation	X	X	X
Louisiana Department of Transportation and Development			
Maryland Department of Transportation	X	X	
Massachusetts Public Utilities Commission			
Metrorail Safety Commission*			
Michigan Department of Transportation	X	X	

Minnesota Department of Public Safety	X	X	X
Missouri Department of Transportation	X	X	
and Bi-State Safety Oversight Program (MoDOT and IDOT)	X	X	
New Jersey Department of Transportation	X	X	X
New York State Department of Transportation*	X	X	X

North Carolina Department of Transportation	X	X	X
Ohio Department of Transportation	X		X
Oklahoma Department of Transportation			
Oregon Department of Transportation	X	X	X
Pennsylvania Department of Transportation	X	X	X
Puerto Rico Emergency Management Agency			
Tennessee Department of Transportation	X	X	
Texas Department of Transportation			

Utah Department of Transportation	X	X	
Virginia Department of Transportation	X	X	X
Washington Department of Transportation			
West Virginia Department of Transportation	X	X	
Wisconsin Department of Transportation	X	X	

<i>Require Safety and Security Certification</i>	<i>SSOA Conducts Triennial Security Audits</i>	<i>Notes</i>
23	22	<i>Green Rows = 674 certified SSOAs MoDOT & Bi-State counted as one SSO</i>
X	X	<i>Arizona Department of Transportation System Safety Program Standard for Rail Safety and Security Oversight - Sections 3, 4, 5.6.1, 7, 10, 13, Appendix L, M, U, X, and Y</i>
		<i>Arkansas SSO Program Standard - NA</i>
X	X	<i>CPUC Program Standard - Procedures Manual State Safety and Security Oversight of Rail Fixed Guideway Systems – Sections RTSB 1, 3, 4, 5, and 9</i>
		<i>CoPUC 4 Code of Colorado Regulations CCR 723-7: Rules Regulating Railroads, Rail Fixed Guideways, Transportation by Rail, and Rail Crossings - Sections 7344, 7345, 7349, and 7350. Additionally, legislation (Decision C-18-0111) removes Security references, including removal of security plan oversight.</i>
X	X	<i>DC FEMS State Safety and Security Oversight Program Standard and Procedures – Sections 3, 4, 6, 7, and 10</i>
X	X	<i>FDOT Fixed Guideway Transportation Systems State Safety and Security Oversight Program Standard – Sections 4, 5, 9, 12, Appendix D</i>

X	X	<i>Georgia Department of Transportation Program Standard for Rail Safety and Security Oversight – Sections 3, 4, 5, 5.6.1, 7, 10, and 13, Appendix L, M, U, X, and Y.</i>
X	X	<i>Hawaii Department of Transportation Rail Transit Safety Oversight Program Standards & Procedures – Sections 3, 4, 5.6, 10, Appendix E, F, M, P, Q, and R</i>
X	X	<i>IDOT System Safety Program Standard and Procedures for Overseeing Rail Fixed Guideway Systems in Illinois – Sections 4, 6, 7, 8, and 10.</i>
		<i>Louisiana SSO Program Standard – NA</i>
X	X	<i>Maryland Department of Transportation Rail Safety Oversight Program Standard – Section 9.1 and Appendix F</i>
		<i>220 CMR 151.00 Department of Public Utilities Rail Fixed Guideway System: System Safety Program Standard – NA</i>
X		<i>Washington Metrorail Safety Commission State Safety Oversight Draft Program Standard – Sections 1, 3, and 4. Note, the MSC Program Standard does not include structured practices for security, however there are some references to security throughout the document in addition to Safety and Security Certification.</i>
X	X	<i>MDOT System Safety Program Standard for State Safety Oversight of Rail Fixed Guideway Systems - page 6 and Appendix I.</i>

X	X	<i>Minnesota Rail Safety Oversight Program Procedures & Standards – Sections Introduction, 1, 2, 3.3, 4, 5, 6, 7, and Appendix C</i>
X	X	<i>MoDOT State Safety Security Oversight Program Standards Manual for Overseeing the Kansas City Streetcar and the Loop Trolley System – Sections 2, 3, 6.2, and page 2.</i> <i>Bi-State Safety Oversight Program Standards Manual for Oversight of Metrolink - Sections 2, 3, 5.2, 7.5, and page 4.</i>
X	X	
X	X	<i>New Jersey Department of Transportation Rail Transit State Safety Oversight (SSO) Program Standard (SSOPS) – Sections 1.3, 4.2.7, 6.4, 7.1, Appendix I, L, and N. Page 58 specifically references 49 CFR 1580.203 Reporting Significant Security Concerns.</i>
X	X	<i>New York State Department of Transportation (NYSDOT) Public Transportation Safety Board (PTSB) Rail Transit State Safety Oversight (SSO) Program Standard (SSOPS) – Sections 4, 6, Appendix H, J, and page 43. Page 71 specifically references 49 CFR 1580.203 Reporting Significant Security Concerns. Additionally, internal security reviews are required in the SEPP as listed in Appendix H.</i>

X	X	<i>State of North Carolina Department of Transportation State Safety Oversight Program Standards and Procedures – Sections 4.6, 4.7, 5, 5.2.5, 5.2.6, 6.1, Appendix E, and G</i>
X	X	<i>ODOT Rail Transit State Safety Oversight (SSO) Program Standard (SSOPS) – Sections 2, 4, 6, Appendix I, K, and page 41. Page 66 specifically references 49 CFR 1580.203 Reporting Significant Security Concerns.</i>
		<i>Oklahoma Department of Transportation Rail Fixed Guideway Public Transportation System (RFGPTS) State Safety Oversight (SSO) Program Standard - NA</i>
X	X	<i>Oregon State Safety Oversight Program Standard – Sections 1, 2, 3, 5.1.2, 5.5, 5.5.3, 6.3, 11, Appendix G, H,</i>
X	X	<i>Pennsylvania Rail Transit Safety Review Program Procedures & Standards - Sections 1, 4, 5, 6, 7.1, 11, and Appendix E</i>
		<i>Government of Puerto Rico Emergency Management Agency State Safety Oversight Program, Program Standard - NA</i>
X	X	<i>State of Tennessee Rail Fixed Guideway System Safety Oversight Program System Safety Program Standard – Sections 2, 4, 5, and page 26.</i>
		<i>Texas Department of Transportation State Safety Oversight Program Standard - NA</i>

X	X	<i>UDOT Rail Transit State Safety Oversight Program Procedures & Standards – Sections 1.1, 1.4, 2.6, 4, 5.3, 10.4, 11, and Appendix C</i>
X	X	<i>Commonwealth of Virginia Department of Rail and Public Transportation Safety and Security Program Standard (SSPS) and Procedures – Sections 2, 4, 4.3, 4.6, 11, 13, Appendix E, F, I, and P</i>
		<i>Washington State Rail Safety Oversight Program Standard – page 2, “WSDOT will maintain its current oversight role for system security plans and programs until it gains FTA certification under 49 CFR Part 674.”</i>
X	X	<i>WVDOT State Safety Oversight Program Standard – Sections 2, 4, Appendix F (could not locate this Appendix), and page 30.</i>
X	X	<i>WisDOT Transit Safety Oversight for Rail Fixed Guideway Transportation Systems Program Standard – Sections 1.2.2, 1.2.3, 1.3.1, 1.6.2, 1.7, 1.7.1, 2.3, 4, 4.3.1, 4.4, 7.1 and Appendix H, I, L.</i>

Paperwork Reduction Act Burden Statement: This is a voluntary collection of information. TSA estimates that the total average burden per response associated with this collection is approximately 12.5 hours. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The control number assigned to this collection is OMB 1652-0062, which expires on 05/31/2024. Send comments regarding this burden estimate or collection to TSA-11, Attention: PRA 1652-0062 BASE, 6595 Springfield Center Drive, Springfield, VA 20598-6011.

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY		
Transportation Security Administration		
Mass Transit Agency Targeted SAI Overview		MTPR FY2021 V.2 (January 2021)
Agency Name:	Lead Inspector:	0
0	Assessment Date:	1/4/2021

SAI #	SECURITY ACTION ITEM (SAI) DESCRIPTION	Implementation
1	Establish written Security Programs and Emergency Management Plans	0%
2	Define roles and responsibilities for security and emergency management	0%
3	Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control	0%
4	Coordinate Security and Emergency Management Plan(s) with local and regional agencies	0%
5	Establish and maintain a Security and Emergency Training Program	0%
6	Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system	0%
7	Implement and reinforce a Public Security and Emergency Awareness program	0%
8	Establish and use a risk management process	0%
9	Establish and use an information sharing process for threat and intelligence information	0%
10	Conduct Tabletop and Functional Drills	0%
11	Developing a Comprehensive Cyber Security Strategy	0%
12	Control access to security critical facilities with ID badges for all visitors, employees and contractors	0%
13	Conduct physical security inspections	0%
14	Conduct background investigations of employees and contractors	0%
15	Control access to documents of security-critical systems and facilities	0%
16	Ensure existence of a process for handling and access to Sensitive Security Information (SSI)	0%
17	Conduct Security Program audits	0%

Overall Implementation:	0.00%
--------------------------------	--------------

Color Key:

	Requirements have been met.
	Requirements are partially met and/or are in the process of being completed.
	Does not meet requirements as described in reference materials.

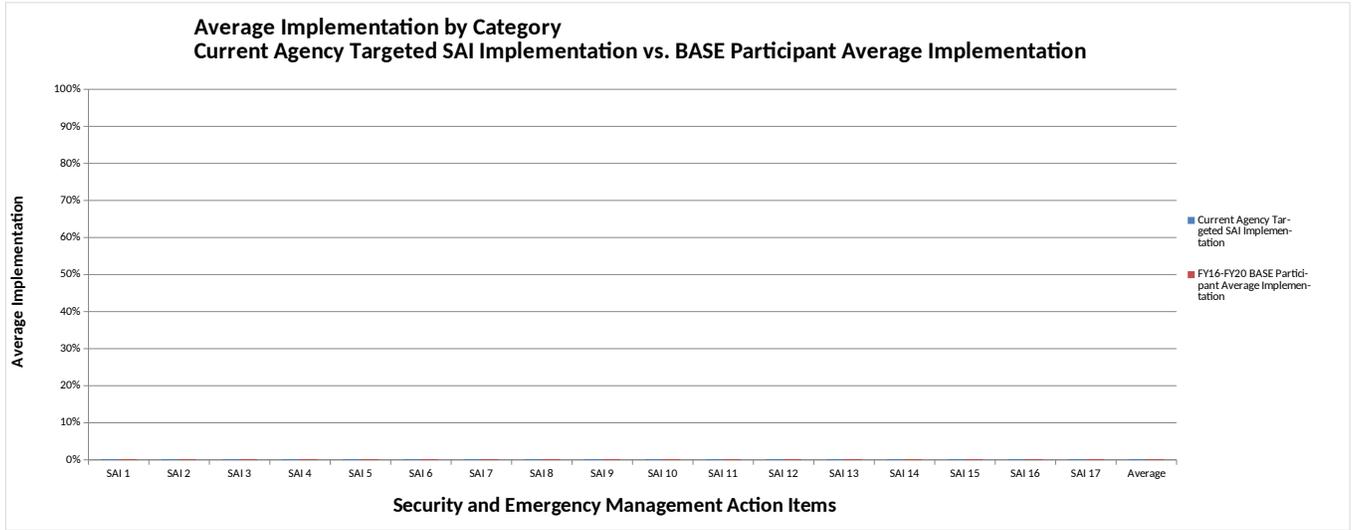
This Agency Did Not Meet the Requirements of the Gold Standard Award.

SENSITIVE SECURITY INFORMATION

Current Agency (Targeted SAI) vs. BASE Participant Average

	SAI 1	SAI 2	SAI 3	SAI 4	SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12	SAI 13	SAI 14	SAI 15	SAI 16	SAI 17	Average
Current Agency Targeted SAI Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
BASE Participant Average Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

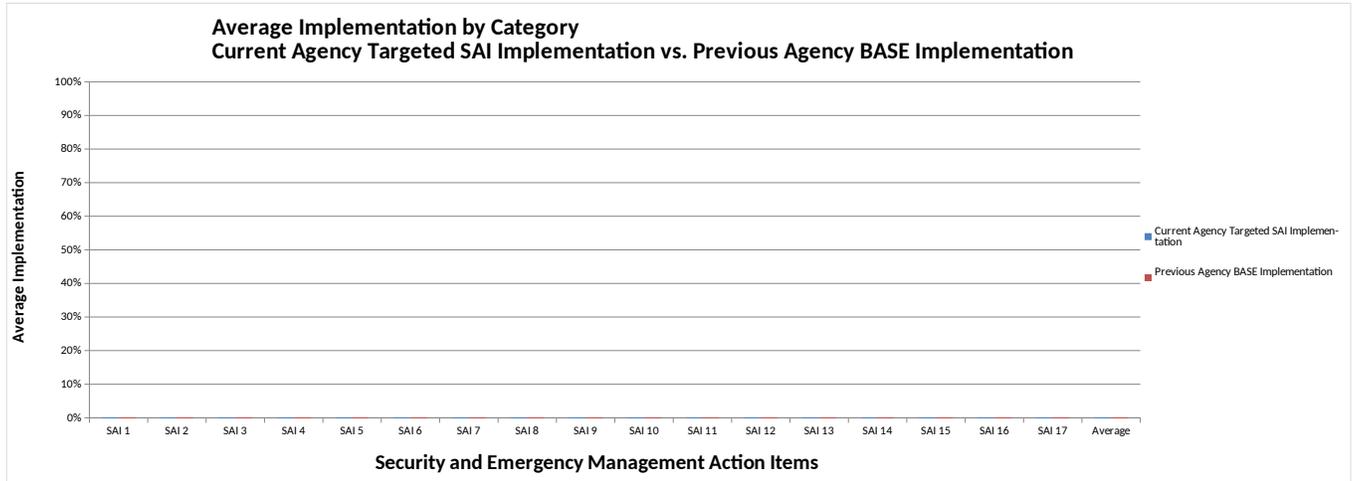
Difference	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
------------	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----



Current Agency BASE (Targeted SAI) vs. Previous BASE Comparison

	SAI 1	SAI 2	SAI 3	SAI 4	SAI 5	SAI 6	SAI 7	SAI 8	SAI 9	SAI 10	SAI 11	SAI 12	SAI 13	SAI 14	SAI 15	SAI 16	SAI 17	Average
Current Agency Targeted SAI Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Previous Agency BASE Implementation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Difference	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
------------	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----



SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY		
Transportation Security Administration		
Mass Transit Agency Targeted SAI Comparison		MTPR FY2021 V.2 (January 2021)
Agency Name:	Lead Inspector:	0
0	Assessment Date:	1/4/2021

SAI #	SECURITY ACTION ITEM (SAI) DESCRIPTION	Previous BASE	Targeted	Improvement
1	Establish written Security Programs and Emergency Management Plans	0%	0%	0%
2	Define roles and responsibilities for security and emergency management	0%	0%	0%
3	Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control	0%	0%	0%
4	Coordinate Security and Emergency Management Plan(s) with local and regional agencies	0%	0%	0%
5	Establish and maintain a Security and Emergency Training Program	0%	0%	0%
6	Establish plans and protocols to respond to the National Terrorism Advisory System (NTAS) alert system	0%	0%	0%
7	Implement and reinforce a Public Security and Emergency Awareness program	0%	0%	0%
8	Establish and use a risk management process	0%	0%	0%
9	Establish and use an information sharing process for threat and intelligence information	0%	0%	0%
10	Conduct Tabletop and Functional Drills	0%	0%	0%
11	Developing a Comprehensive Cyber Security Strategy	0%	0%	0%
12	Control access to security critical facilities with ID badges for all visitors, employees and contractors	0%	0%	0%
13	Conduct physical security inspections	0%	0%	0%
14	Conduct background investigations of employees and contractors	0%	0%	0%
15	Control access to documents of security-critical systems and facilities	0%	0%	0%
16	Ensure existence of a process for handling and access to Sensitive Security Information (SSI)	0%	0%	0%
17	Conduct Security Program audits	0%	0%	0%
Overall Implementation:		0%	0%	0%