

The BASE Resource Kit is designed to help highway transportation agencies effectively prepare for the BASE review process. The document provides direct resources and web-links to TSA, DOT, and other reference documents.

Highway BASE Resource Kit



**Transportation
Security
Administration**

Introduction

Since 2006, the Transportation Security Administration (TSA), through its Surface Transportation Security Inspection Program (STSIP), has been conducting voluntary Baseline Assessment for Security Enhancement (BASE) reviews in an effort to assess and improve the security posture of mass transit systems in the United States. The program has been very successful, resulting in an overall improvement to security in the public transportation sector. TSA has been conducting this same security review concept through local Surface field offices with the larger highway transportation sector over the past four years. This process has improved the working relationship between TSA and our corporate trucking, motor coach, and school bus partners, while at the same time has elevated the overall posture of highway security. In continuance of this effort, TSA respectfully requests your participation in conducting a cooperative Highway BASE review focusing on your security operations.

Highway BASE is a non-regulatory, voluntary program in which local TSA surface field offices work with highway transportation stakeholders across the United States to review their security practices. In return, TSA will provide an Executive Summary report on their findings, assign an overall security “score,” and provide recommended options for consideration designed to mitigate any vulnerabilities identified. Simply stated, the Highway BASE program is designed to drive down the security risks of your company.

Following the review, your company/entity will be provided with a detailed summary of findings that include security strengths, security weaknesses, and two separate security “scores.” Participants will be scored on their “Overall Security Performance” (total score) that looks at the implementation of all possible security initiatives, as well as a second “Critical Element Score” (“critical” score) that measures certain minimally expected security practices that should be in place. Both scores are ranked 0% thru 100%.

Using a risk-based methodology developed by TSA’s Highway & Motor Carrier (HMC) Division, your company/facility was selected as a candidate for this program. The initial focus of the program will be with companies that represent the largest portion of their respective industry before moving on to smaller entities. TSA personnel will review various aspects of your security practices based on twenty (20) recommended “Security Action Items” developed through collaboration with our industry partners.

During the Highway BASE review process, your local TSA surface field office will review relevant security documents, interview you or other designated security personnel, and (if appropriate) observe operations. Once again, the emphasis of this review is to assist your company in increasing their security posture through instituting and implementing smart security practices and establishing a relationship with your local surface field office. Additionally, no information provided will be shared with any entities outside TSA and no enforcement action will be taken as a result of the review.

Participating in the HWY BASE program offers many benefits. Among those are the following:

- Offers a free security assessment and Executive Summary report, which provides non-legally binding recommendations (Options for Consideration) that may increase the company’s overall security posture
- Provides stakeholder with current best security practices
- Hardens assets against both terrorist and criminal elements

- Establishes a relationship with TSAs local Surface office as a security partner and resource
- Enhances the overall transportation security posture of the nation that will, in turn, reduce the risk of terrorism
- Better prepare stakeholders for possible future security regulations
- Employees will benefit from an improved security environment
- Enhances the reputation that the stakeholder is an “industry leader”
- Improves their standing in the community as a “good neighbor”
- Provides data to support congressional rulemaking policies

Documents Needed During the Assessment

The following documents may be needed for review by TSA inspectors during the course of the HWY-BASE review process. Should you have any or all of these documents, please ensure they are readily available at the time of the review.

- Security Plan/Procedures
- Written Risk Assessment Report
- Emergency Response Plan/Procedures
- Safety Plan/Procedures
- Company “Rules & Regulations” Manual
- Continuity of Operations (COOP) Plan
- Company/Facility Contact or Phone Tree List(s)
- Written IT Security Guidelines
- Emergency Services Contact or Phone Tree List(s)
- Training Manual
- Driver’s Manual
- Others unique to your situation
- Previous Corporate Security Review Reports (conducted by TSA)
- Previous BASE review conducted by TSA
- NOTE: One or more of these may be combined into a single document.
- Not all documents are applicable to all entities

Additional Information Needed During Highway BASE Assessment

Company Data

- Company DOT Number (if applicable)
- Company Name
- Company Headquarters Address
- Company Facility address (if different from HQ address)
- Company Website

Security Coordinator

- Security Coordinator Contact Information
- Alternate Security Coordinator Contact Information

Vehicle Data

- Number of Power Units (Trucks, Tractors, Motorcoaches, School Buses) owned/leased by company across all locations
- Number of Power Units owned/leased by company that are assigned to the specific facility/location being assessed (if non-HQ review)

Terminal/Facility Information (for non- headquarters visits)

- Company Name of Terminal Visited
- Company Terminal Address
- Terminal/Facility Manager Contact Information

Management and Accountability	1.000	Have a Designated Security Coordinator
	The purpose of a qualified Security Coordinator is oversee the implementation of a Security Program and ensure its coordination with outside entities, including acting as a single point-of-contact for all security-related issue, both internal and external.	
	Security Action Item Element	
	1.001	This entity designated a qualified primary Security Coordinator/ Director.
	Standard: The entity has fully implemented this element, formally identifying a qualified individual to act as the entity's Security Coordinator and Point-of-Contact. This designation is documented as part of a security plan or part of another document. Recommend that the security coordinator be a citizen of the U.S. and have law enforcement, private security, or appropriate military background, or adequate on-the-job experience.	
	1.002	This entity designated an alternate Security Coordinator/ Director.
	Standard: The entity has fully implemented this element, formally identifying a qualified individual to act as tan alternate Security Coordinator and Point-of-Contact. This designation is documented as part of a security plan or part of another document.	
1.103	This entity has policies that specify the transportation related duties of the security coordinator	
Standard: The entity should have documented specific transportation security-related duties for the Security Coordinator, which may be found in his or her job description, security plan, or other documents as appropriate. Security duties should include the following: (1) Implementing security actions under the security plan; (2) Coordinating security improvements; and (3) Receiving communications from appropriate federal officials.		

2.000	Conduct a Thorough Risk Assessment	
The purpose of a risk management process is to improve security through a structured, proactive program developed to identify, assess, manage, and mitigate the security risks inherent to the system.		
Security Action Item Element		
2.001		This entity recognizes they may have certain assets of specific interest to terrorists (i.e.: vehicles, IT information, passengers, critical personnel, etc.) and considers this factor when developing transportation security practices
Standard: The entity should list its assets and determine which may be of specific interest to terrorists. Assets may include vehicles, platforms, stations, terminals fueling depot, key personnel, information systems, cargo, passengers, storage areas, etc. Consider detailing security measures to implement and protect each asset in order to: (1) Deter security incidents that may result in significant local, regional, or national consequences; and (2) effectively maintain business operations in the event of a loss to asset(s).		
2.002		This entity has conducted a documented, site specific "Vulnerability Assessment" and is generally familiar with any significant threats or consequences they may face.
Standard: The entity should conduct and document a site specific "Vulnerability Assessment" (or improve upon an existing assessment) that addresses vulnerabilities. Additionally, the entity should familiarize themselves with threats their operation faces and the consequences of exploited vulnerabilities. Ideally, vulnerabilities should be assessed against identified threats and weighed with the consequences of exploited vulnerabilities in mind. Identified vulnerabilities should be minimized or corrected as soon as possible.		
2.003		Management generally supports efforts to improve security and provides funding and/or approves corrective actions to security vulnerabilities or weaknesses identified.
Standard: Management for the entity should support efforts to enhance security and should consider ensuring that funds are provided toward mitigation measures designed to address vulnerabilities identified.		

Management and Accountability

	<h3>Security Action Item Resource Library</h3> <p>A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (DOT - Federal Highway Administration)</p> <p>Public Transportation System Security and Emergency Preparedness Planning Guide (DOT-Federal Transit Administration)</p> <p>Threat and Hazard Identification and Risk Assessment Guide (FEMA)</p> <p>Recommendation for Bridge and Tunnel Security (DOT - Federal Highway Administration)</p> <p>FEMA Building and Infrastructure Protection Series</p>	
	3.000	<h3>Develop a Security Plan (Security Specific Protocols)</h3> <p>The purpose of the Security Plan is to ensure a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events.</p>
	<h3>Security Action Item Element</h3>	
	3.001	<p>This entity has a written, site specific transportation Security Plan that addresses, at a minimum, management procedures, personnel security, facility security and vehicle security along with actions to be taken in the event of a security incident or security breach.</p>
	<p>Standard: The entity should have a site specific Security Plan that addresses management procedures, personnel security, facility security vehicle (en route) security, and sets forth actions to be taken in the event of a security incident or security breach.</p>	
3.002	<p>This entity limits access to its security plan or security procedures to employees with a "need-to-know."</p>	
<p>Standard: The entity should limit access to its Security Plan or security procedures to employees with a "need-to-know" (i.e., Safety/Security Coordinators, management). Other employees should have access only to portions of the plan pertaining specifically to the functions of job duties and for implementing security procedures.</p>		

Management and Accountability

3.003	This entity requires that employees with access to security procedures sign a non-disclosure agreement (NDA).
<p>Standard: The entity should require employees with access to any portion of the Security Plan or security procedures to sign a Non-Disclosure Agreement (NDA). Although many NDAs apply to sharing business practices/proprietary information, security-specific items should be documented within the NDA, such as information pertaining to risk assessments, Security Plans, and critical assets.</p>	
3.004	This entity has written security plans/policies that have been reviewed and approved at the entity's executive level.
<p>Standard: Security Procedures, including revisions, should be reviewed and approved at the company's highest (executive) level.</p>	
3.005	This entity has security procedures to be followed by all personnel (i.e., drivers, office workers, maintenance workers, laborers and others) in the event of a security breach or incident.
<p>Standard: Procedures are in place setting forth the expectations, responsibilities, or limitations for all personnel (drivers, office workers, administrators, etc.) in the event of a security incident or breach.</p>	
3.006	The entity has procedures for responding to an active shooter event.
<p>Standard: The entity has well-developed written procedures that specifically address active shooter events.</p>	
3.007	This entity requires that their security policies be reviewed at least annually and updated as needed.
<p>Standard: An annual review of any written security procedure is required, and the date in which they were reviewed and/or updated is noted.</p>	

3.008	Employees are provided with site-specific, up to date contact information for entity management and/or security personnel to be notified in the event of a security incident and this entity periodically tests their notification or "call-tree" procedures.
<p>Standard: Contact lists are provided to employees and should include security personnel to be contacted during a security incident. This information should be current. Additionally, the entity conducts periodic phone-tree exercises to ensure all affected employees can be contacted during a security or emergency incident.</p>	
3.009	This entity has procedures for 24/7 notification of entity security personnel and/or local/state/federal authorities to be notified in the event of a security incident.
<p>Standard: The entity provides employees with guidelines requiring them to notify, at a minimum, local law enforcement authorities and the security coordinator in the event of a security incident or breach.</p>	

Security Action Item Resource Library

TSA Transportation Security Template and Assessment Review Toolkit -T-START
(Provided by Transportation Security Inspectors)

[FTA System Security and Emergency Preparedness Plan \(SEPP\) Template](#)

[DHS Facility Security Plan: An Interagency Security Committee Guide](#)

Management and Accountability	4.000	Plan for Emergency Response & Continuity of Operations
	The purpose of a Continuity of Operations plan is to ensure that an entity can respond to, continue operating during, and recover from a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.	
	Security Action Item Element	
	4.001	Following a significant operational disruption, this entity has procedures designed to ensure an appropriate response and restoration of facilities and services. (May be in the form of a Business Recovery Plan, Continuity of Operations Plan or Emergency Response/Safety Plan).
	Standard: The entity has a comprehensive continuity/recovery plan. Essential business functions (HR, IT, etc.), operational functions (dispatch, communication, etc.), and key facilities have been identified. Policies and procedures (including who is responsible for activating the plan) are detailed and effective in mitigating any disruption to operations, and the plan outlines steps to be taken to return the agency to a “normal” operational status in a timely manner.	
	4.002	This entity ensures all facilities have an auxiliary power source if needed or the ability to operate effectively from an identified secondary site.
Standard: The entity should have procedures in place to ensure the continuity of operations if needed. This should include data backup procedures and uninterruptible power supply (generator, battery backup). A secondary site with full operational capability can substitute a backup power supply. Secondary power methods and relocation procedures should be tested and/or practiced occasionally.		

Security Action Item Resource Library

[FEMA Continuity of Operations Plan Template for Federal Departments and Agencies](#)

[FEMA Continuity of Operations \(COOP\) Multi-Year Strategy and Program Management Plan Template Guide](#)

[Ready.Gov Business Continuity Plan](#)

[NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs](#)

5.000

Develop a Communications Plan

The purpose of a Communications Plan is to ensure that communication is seamless and effective during all situations—including emergency and non-emergency situations.

Security Action Item Element

5.001	This entity has methods for communicating with drivers during normal conditions.
-------	--

Standard: The entity should have documented procedures for communicating with drivers during routine trips. Procedures should include methods of communication, transmitting information (including threat), reporting suspicious activities while en-route, and driver check-in procedures. These procedures should be practiced or discussed regularly to ensure drivers are properly prepared for future events. Radio, cell phone, or public address equipment (if applicable) is available for the company to communicate with drivers and/or customers/passengers during normal conditions.

Management and Accountability

Management and Accountability	5.002	This entity has emergency procedures in place for drivers on the road to follow in the event normal communications are disrupted. Entity should have contingencies in place in the event dispatch system, if applicable, become inoperable.
	Standard: The entity should have documented emergency procedures for drivers to follow in the event normal communications are disrupted while en-route. Entities may consider using back-up technology that will function in the event normal communication is disrupted. Other options include the following: discontinuation of trip, safe harboring, returning to terminal, and/or identifying alternate methods of communication. This should be part of a written Communications Plan.	
	Security Action Item Resource Library	
	Ready.Gov Crisis Communication Plan	
	FCC Emergency Communications	
	6.000 Safeguard Business and Security Critical Information	
	The purpose of this Security Action Item is enhance system security through the identification and protection of employee and contractor document access to critical systems and facilities based upon verified need-to-know access requirements.	
	Security Action Item Element	
	6.001	This entity controls access to business documents (i.e. security plans, critical asset lists, risk/vulnerability assessments, schematics, drawings, manifests, etc.) that may compromise entity security practices.
	Standard: The entity has written policies and procedures designed to control and minimize internal and external access to sensitive business information (Operational Security).	
6.002	This entity controls personnel information (i.e. SSN, address, drivers license, etc.) that may be deemed sensitive in nature.	
Standard: The entity has written policies and procedures to control and minimize internal and external access to personnel information (keeps files or office locked, secure computer access).		

	6.003	This entity maintains and safeguards an up-to-date list of all assets that are critical to the continuation of business operations (i.e. vehicles, IT equipment, products, other equipment, etc.), periodically inventories these assets, and has the ability to determine their general location at any given time.
	Standard: The entity has an adequate inventory control process that ensures accountability for all at-risk assets (products, vehicles, equipment, computers) that may be of specific interest to criminals or terrorists. The entity has a specific, descriptive list of identified "critical assets" along with the knowledge of their general location. These assets are periodically inventoried, and employees receive some sort of training or briefing on critical asset protection.	
	Security Action Item Resource Library	
	Sensitive Security Information Guidance for Transportation Agencies on Managing Sensitive Information	
7.000	Be Aware of Industry Security Best Practices	
Management and Accountability	The purpose of this Security Action Item is ensure that an entity's security practices are up-to-date and effective against current threats and observed vulnerabilities.	
	Security Action Item Element	
	7.001	Personnel at this entity meet/communicate with industry peers, partners or associations that share security related information or best practices. (May include individual or corporate membership with an industry trade association).
	Standard: Security or administrative personnel belong to and meet with one or more industry groups that provide or share resources or security-related guidance (ABA, ACC, ATA, NAPT, NASDOTS, NTTCC, OOIDA, UMA, etc.).	
	7.002	Personnel at this entity have sought and/or obtained transportation related security information or "best practices" guidance from external sources.
	Standard: The entity has used security-related information (best/recommended practices) from or provided security-related information to industry peers or governmental partners.	

8.000	Conduct Licensing and Background Checks for Drivers/ Employees/ Contractors	
The purpose of this Security Action Item is enhance system security through the conduct and documentation of employee and contractor background investigations based upon identified and verified critical access requirement levels.		
Security Action Item Element		
8.001		This entity requires verification and documentation that persons operating entity vehicles have a valid driver’s license for the type of vehicle driven, along with any applicable endorsement(s) needed.
Standard: The entity performs DMV inquiry of drivers upon hire and periodically thereafter (at least biannually) to verify proper class of license and driving history. The entity could also elect to enroll in automatic DMV updates of drivers.		
8.002		This entity requires a criminal history check, verification of Social Security Number and verification of immigration status for personnel operating entity vehicles.
Standard: The entity requires all drivers to receive a background check upon hire. A fingerprint-based background check or similar requirement (TWIC credential or CDL Hazmat Endorsement) is ideal.		
8.003		This entity requires a criminal history check, verification of Social Security Number and verification of immigration status for non-driver employees with access to security related information or restricted areas.
Standard: The entity requires all non-drivers to receive a background check upon hire. A fingerprint-based background check or similar requirement (TWIC credential or CDL Hazmat Endorsement) is ideal.		
8.004		This entity asks prospective drivers if they have been denied a Transportation Worker Identification Credential (TWIC) or a Commercial Driver's License with HazMat Endorsement (CDL-HME) for employment elsewhere specifically as the result of a security background check.
Standard: This entity asks prospective drivers if they have been denied a Transportation Worker Identification Credential (TWIC) or a Commercial Driver's License with HazMat Endorsement (CDL-HME) for employment elsewhere specifically as the result of a security background check.		

Personnel Security

8.005	This entity has security-related criteria that would disqualify current or prospective personnel from employment.
<p>Standard: The entity has documented security-related criteria that would disqualify current or prospective personnel from employment. This could include criminal offenses, financial history, information found in a security threat assessment, etc.</p>	
8.006	This entity has policies to address criminal allegations that may arise or come to light involving current employees.
<p>Standard: The entity has written procedures for reviewing, evaluating, and acting upon any new criminal activity information (allegations and convictions) for current employees that may come to light.</p>	
8.007	The entity requires that contract employees having access to security related information or restricted areas be held to comparable licensing and background checks as those required of regular company employees (contracted employees may include contractual drivers, unescorted cleaning crews, etc.).
<p>Standard: The entity requires that contract employees with security responsibilities or access to security-related information receive background checks that are identical to those of regular employees. This may be built in to the contract management process.</p>	
<p>Security Action Item Resource Library</p>	
<p><u>ASIS International Pre-Employment Background Screening Guidelines</u></p> <p><u>FBI Fingerprint Identity History Check</u></p> <p><u>US Citizenship and Immigration Services</u></p> <p><u>Transportation Worker Identification Credential (TWIC)</u></p> <p><u>HAZMAT Endorsement</u></p>	

Personnel Security	9.000 Develop and Follow Security Training Plans	
	The purpose of developing a Security Training Program is to ensure that all personnel are trained, tested, and monitored in current security protocols appropriate to their position.	
	Security Action Item Element	
	9.001	This entity provides general security awareness training to all employees (separate from or in addition to regular safety training).
	Standard: The entity provides, at a minimum, general security training for all employees, regardless of job function.	
	9.002	This entity provides additional security training to employees having specific security responsibilities.
	Standard: The entity has identified employees having specific security responsibilities, and those individuals have received additional training to effectively perform their assigned duties preventing and/or responding to a security incident.	
	9.003	This entity provides periodic security re-training to all employees.
	Standard: The entity provides periodic security re-training (recurrent training) to all employees no less than every three years or with change of job function.	
	9.004	The security training/re-training offered by this entity is specific to and appropriate for the type of transportation operation being conducted (trucking, school bus, motor coach or infrastructure mode).
Standard: The security training/re-training offered by this entity is specific to and appropriate for the type of transportation operation being conducted (trucking, school bus, motor coach or infrastructure mode).		
9.005	The entity provides Active Shooter training to all employees.	
Standard: The entity provides training specifically focused on "active shooter" scenarios (awareness, mitigation, response, etc.) to all employees, regardless of job function.		

9.006	This entity has comparable security training requirements for both regular employees and contracted employees with security responsibilities or access to security-related information.
Standard: The entity requires that contract employees with security responsibilities or access to security-related information receive security training that is identical to that of regular employees. This may be built in to the contract management process.	
9.007	This entity requires documentation and retention of records relating to security training received by employees.
Standard: The entity has policies requiring the documentation and retention of records related to security training received by employees. These policies include how training record are retained and for how long records are retained.	

Security Action Item Resource Library

- [First Observer](#)

- [DHS State Homeland Security and Emergency Services](#)

- [Nationwide SAR Initiative Training](#)

- [Rural Domestic Preparedness Consortium \(RDPC\) - Training Material](#)

- [FEMA Emergency Management Institute](#)

- [DHS Option For Consideration Active Shooter Training](#)

- [FBI Active Shooter Training](#)

Personnel Security	10.000	Participates in Security Exercises and Drills	
		The purpose of security exercises (tabletop, drills, full-scale) is to further develop skills learned in training by allowing employees to demonstrate these skills in practical environments.	
		Security Action Item Element	
		10.001	This entity meets with outside agencies (i.e.; law enforcement/first responders/Federal officials) regarding security support and or issues.
		Standard: The entity <i>regularly</i> meets with outside entities (i.e. law enforcement/ first responders/ Federal officials) regarding security issues or security exercises/ drills in the event of a terrorist attack.	
		10.002	Personnel at this entity have actually conducted or participated in some type of exercises/drills that involve security related activities.
		Standard: The entity has conducted or participated in some type of security exercise or drill within the last 12 months. Examples could include the following: active participation in tabletop exercises; participation in TSA I-STEP or EXIS exercises; and/or situational drills (bomb threats, hijacking, lock-down, etc.).	
		10.003	The entity has consulted local law enforcement/ first responders when developing active shooter plans and procedures.
		Standard: The entity has consulted local law enforcement/ first responders when developing active shooter plans and procedures.	
		10.004	The entity conducts exercises (tabletop or full-scale) that specifically focus on active shooter scenarios.
	Standard: The entity has conducted or participated in some type of exercise or drill specifically focused on active shooter scenarios within the last 12 months. This could include lockdown/shelter-in-place procedures, "Run, Hide, Fight" scenarios, etc.).		
	10.005	This entity has administrative and/or security personnel trained in the National Incident Management System (NIMS) or Incident Command System (ICS).	
	Standard: The entity has administrative and/or security personnel trained in the National Incident Management System (NIMS) or Incident Command System (ICS).		

Security Action Item Resource Library

[FEMA IS-130 Exercise Evaluation Training](#)

[FEMA Emergency Planning Exercises](#)

[Homeland Security Exercise and Evaluation Program \(HSEEP\)](#)

[DHS FEMA IS-139 Exercise Design Training Course](#)

11.000 Maintain Facility Access Control

The purpose of this Security Action Item is to promote protective measures for critical infrastructure essential to uninterrupted/ uncompromised system operation.

Security Action Item Element

11.001	This entity has controlled points of entry/exit for employees and restricts non-employee access to buildings, terminals and/or work areas.
--------	--

Standard: Employee entrances and exits are controlled and entry to all buildings, terminals and/or work areas is restricted for non-employees at all facilities. Entry (doors) must be capable of being locked or otherwise secured.

11.002	This entity has secured all doors, windows, skylights, roof openings and other access points to all buildings, terminals and/or work areas.
--------	---

Standard: All doors, windows, etc. are inoperable or secured with adequate locking mechanisms, and entry to all buildings, terminals and/or work areas is secure at all facilities at all times.

Facility Security

11.003	This entity restricts employee access into certain secure areas located within their building or site (i.e.; computer room, administrative areas, dispatch, etc.).
Standard: Secure areas are clearly identified and access to these secure areas is restricted to certain employees based on job function.	
11.004	This entity issues photo-identification cards/badges or uses other effective identification methods to identify employees.
Standard: Entity-issued photo ID badges issued to all employees.	
11.005	This entity requires employees to carry and/or display their identification card/badge or other form of positive employee ID while on duty.
Standard: This entity requires that all employees display and/or carry their entity ID card/badge while on duty, and methods of verification are in place.	
11.006	This entity has a challenge procedure that requires employees to safely report unknown persons or persons not having proper identification.
Standard: This entity has a written policy in place requiring employees to safely report unknown persons or those not having proper identification.	
11.007	This entity utilizes advanced physical control locking measures beyond simple locks & keys (i.e.; biometric input, key card, PIN, combination locks) for access to buildings, sites or secure areas (excludes vehicles).
Standard: This entity utilizes personal identifying access control (i.e. biometric, key card and/or PIN). Access is deactivated upon employee separation.	
11.008	Where appropriate, entrance and/or exit data to facilities and/or to secure areas can be reviewed as needed (may be written logs, PIN or biometric data, or recorded camera surveillance).
Standard: This entity captures personal identifiers (PIN, key card, biometric ID, photograph, computer log-in, or other electronic means of identifying who enters the facility or certain restricted areas) and the data can be examined if needed.	
11.009	This entity utilizes visitor control protocols for non-employees accessing non-public areas.
Standard: Visitor positively identified, logged-in, is issued visitor badge and escorted while on premises.	

Security Action Item Resource Library	
FTA Transit Security Design Consideration	
12.000	Implement Strong Physical Security at All Locations
The purpose of this Security Action Item is to promote protective measures for critical infrastructure essential to uninterrupted/ uncompromised system operation.	
Security Action Item Element	
12.001	This entity utilizes perimeter physical security barriers (fences/gates/walls/planters /bollards, etc.) that restrict both unauthorized vehicle and pedestrian access.
Standard: This entity utilizes physical barriers that restrict both unauthorized vehicle and pedestrian access at all locations.	
12.002	All perimeter physical security barriers on site are functional, used as designed, and adequately maintained to effectively restrict vehicle and/or pedestrian access.
Standard: All perimeter physical security barriers on site are functional, used as designed, and adequately maintained to effectively restrict vehicle and/or pedestrian access.	
12.003	This entity utilizes a tamper resistant intrusion detection system(s) (burglary/robbery alarm).
Standard: Windows/doors/interior at all locations are covered and a tamper resistant system is monitored 24/7 when armed.	
12.004	This entity utilizes closed circuit television cameras (CCTV).
Standard: CCTV cameras are deployed to cover all secure areas.	
12.005	The CCTV cameras present are functional and adequately monitored and/or recorded.
Standard: A CCTV system is utilized at all locations and is actively monitored and/or recorded 24/7. Cameras are functional and used as designed.	

Facility Security

12.006	This entity has adequate security lighting.
Standard: The entity has deployed adequate security lighting that functions properly at all locations.	
12.007	This entity utilizes key control procedures for buildings, terminals and gates (excludes vehicles).
Standard: An active key control program for buildings and facilities is in place and all keys are accounted for and regularly inventoried.	
12.008	This entity employs on-site security personnel.
Standard: The entity has on-site security personnel who are adequately armed. "On-site security personnel" should be someone who performs physical security functions (perimeter checks, gate guards, ID badge checks, etc.). This is not a function of the Security Coordinator or Alternate.	
12.009	This entity provides a secure location for employee parking separate from visitor parking.
Standard: This entity provides a secure location for employee parking separate from visitor parking.	
12.010	Clearly visible and easily understood signs are present that identify restricted or off-limit areas.
Standard: Clearly visible and easily understood signs are present that identify restricted or off-limit areas, as well as any facility security practices to which the public may be subjected.	
12.011	Vehicle parking, stopping or standing is controlled, to the extent possible, along perimeter fencing or near restricted areas.
Standard: Vehicle parking, stopping or standing is controlled, to the extent possible, in areas within or adjacent to all facilities.	
12.012	This entity controls the growth of vegetation so that sight lines to vehicles, pedestrians, perimeter fences or restricted areas are unobstructed.
Standard: This entity controls the growth of vegetation so that sight lines to vehicles, pedestrians, perimeter fences or restricted areas are unobstructed.	
12.013	This entity conducts periodic random security checks on personnel/vehicles and/or other physical security countermeasures (i.e. random perimeter checks, breach/trespass tests, bomb threat drills, etc.).

	<p>Standard: The entity uses unique or random security measures that introduce unpredictability into the entity's practices for an enhanced deterrent effect. May be spot inspections, "red alerts," or other random/imaginative security initiative.</p>	
	<p>Security Action Item Resource Library</p> <p>FTA Transit Security Design Consideration</p>	
13.000	<p>Enhance Internal and External Cyber Security</p>	
Facility Security	<p>The purpose of this Security Action Item is to enhance agency security awareness and preparedness to identify and protect against cyber security threats to the system.</p>	
	<p>Security Action Item Element</p>	
	13.001	<p>This entity requires an employee logon and password that grants access to limited data consistent with job function.</p>
	<p>Standard: This entity requires an employee logon that grants access to entity data consistent with job function. Passwords must be reset periodically.</p>	
	13.002	<p>This entity utilizes an Information Technology (IT) "firewall" that prevents improper IT system access to entity information from both internal and external threats.</p>
	<p>Standard: This entity utilizes an IT firewall that prevents improper IT system access to entity information, programs, and automated systems from both internal and external threats. NOTE: Most Windows- and Apple-based operating systems come preloaded with a standard firewall.</p>	
	13.003	<p>This entity has sufficient IT security guidelines.</p>
	<p>Standard: This entity has IT security guidelines that prohibit opening unknown files or emails, revealing/sharing passwords, or introducing unauthorized software or hardware into the company's computer systems.</p>	
	13.004	<p>This entity identifies a qualified IT security officer or coordinator.</p>
	<p>Standard: The entity has identified an IT security officer or coordinator that is trained in IT security. This role is fully implemented and documented (may be a shared title).</p>	

	13.005	This entity tests their IT system for vulnerabilities.
	Standard: The entity regularly conducts penetration testing of their IT systems, keeps firewall systems up to date, and removes/rejects any suspicious data received.	
	13.006	This entity has off-site backup capability for data generated and system redundancy.
	Standard: The entity provides off-site data backup capability for data generated and system redundancy for this and/or all locations.	
Security Action Item Resource Library		
<u>Industrial Control System Cyber Emergency Response Team (ICS CERT)</u>		
<u>ICS CERT Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-In-Depth Strategies</u>		
<u>DHS CERT: Password Security, Protection, and Management</u>		
<u>DHS Cybersecurity Training & Exercises</u>		
14.000	Develop a Robust Vehicle Security Program	
	The purpose of this Security Action Item is to promote protective measures for vehicles essential to uninterrupted/ uncompromised system operation.	
	Security Action Item Element	
Vehicle Security	14.001	The vehicles used by this entity are equipped with appropriate door/window locks and their use is required when unattended (if not prohibited by State law).
	Standard: All vehicles used by this entity have adequate door and window locks, and their use is required.	
	14.002	This entity provides some type of supplemental equipment for securing vehicles, which may include steering wheel locks, theft alarms, "kill switches," or other devices.
	Standard: All vehicles are equipped with supplemental securing devices (steering wheel locks, theft alarms, "kill switches," or other devices.)	

14.003	This entity utilizes a key control program for their vehicles (separate from key control for buildings.)
Standard: An active vehicle key control program is in place (or a unique PIN key code is needed for keyless vehicles), and all keys (or key codes) are protected and accounted for. NOTE: Vehicles that require no key or share keys with other vehicles is not recommended.	
14.004	This entity employs technology that requires the use of key card, PIN or biometric input to enter or start vehicles.
Standard: All vehicles have some type of key card, PIN, or biometric reader to enter or start.	
14.005	This entity equips vehicles or provides drivers with panic button capability.
Standard: All vehicles are equipped with some type of panic button capability.	
14.006	This entity uses unique distress codes or signals to alert dispatch, police or other employees in the event of an emergency situation.
Standard: The entity has instituted a distress code or signals in order to covertly alert dispatch, other drivers/employees, and/or law enforcement in the event of emergency situations. Codes are changed when necessary.	
14.007	This entity uses vehicles equipped with an interior and/or exterior on-board, functioning and recording video camera.
Standard: All vehicles are equipped with a functional onboard camera system with recording capabilities.	
14.008	This entity uses vehicles equipped with GPS or land based tracking system.
Standard: All vehicles are equipped with GPS or land based tracking system.	
14.009	This entity prohibits unauthorized passengers in entity vehicles.
Standard: The entity prohibits unauthorized passengers in entity vehicles.	
14.010	This entity restricts or has policies regarding overnight parking of entity vehicles at off-site locations (i.e.; residences, shopping centers, parking lots, etc.).
Standard: The entity restricts or has policies regarding overnight parking of entity vehicles at off-site locations (i.e.; residences, shopping centers, parking lots, etc.).	

Vehicle Security	15.000	Develop a Solid Cargo/ Passenger Security Program		
	The purpose of this Security Action Item is to promote protective measures for cargo, passengers, and vehicles essential to uninterrupted/ uncompromised system operation.			
	Security Action Item Element			
	15.001MC	This entity requires the use of adequate locks on vehicle cargo/ storage areas.		
	Standard: All vehicles are equipped with locks for cargo/storage areas, and their use is required.			
	15.002MC	This entity equips vehicles with a safety/security barrier between the driver and passengers.		
	Standard: All applicable vehicles are equipped with a safety/security barrier between the driver and passengers.			
	15.003MC	This entity utilizes some type of cargo, baggage or passenger screening system.		
	Standard: This entity utilizes some type of cargo, baggage or passenger screening system.			
	15.001SB	This entity requires the use of adequate locks on vehicle cargo/storage areas.		
	Standard: All vehicles are equipped with locks for cargo/storage areas, and their use is required.			
	15.002SB	This entity or the appropriate school board requires the presence of a school official (other than driver) onboard during all extracurricular transports.		
	Standard: All extracurricular transports require the presence of a school official (other than driver).			
	15.001TR	This entity provides appropriate locks for vehicle cargo doors, valves, and/or hatch openings, and requires their use.		
	Standard: This entity requires the use of adequate locks on vehicle cargo/storage areas.			
15.002TR	This entity provides an adequate supply of seals for vehicle cargo doors, valves, and/or hatch openings, and requires their use.			
Standard: All vehicles are equipped with an adequate supply of seals for vehicle cargo doors, valves, and/or hatch openings, and their use is required.				

	15.003TR	This entity provides or requires some type of supplemental trailer security measures (i.e.; kingpin locks, glad-hand locks, high-grade door locks, any type of cargo alarm system, etc.).
	Standard: All vehicles are equipped with supplemental trailer security measures.	
16.000	Plan for High Alert Level	
Vehicle Security	The purpose of establishing plans and protocols to respond to information received about imminent or elevated security threats is to ensure a pre-determined, organized response by the Agency to prevent, mitigate, and/or respond to a threat.	
	Security Action Item Element	
	16.001	This entity has additional security procedures that take effect in the event of a heightened security alert status from the DHS National Terrorist Alert System (NTAS) or other government source.
	Standard: Additional security measures are documented within Security Plan or security procedures.	
	16.002	This entity monitors news or other media sources for the most current security threat information.
	Standard: The entity monitors TV news, newspapers, Homeland Security website, and other media sources every day for security threat information.	
	16.003	This entity distributes relevant or evolving threat information to affected entity personnel as needed.
	Standard: The entity has procedures to distribute evolving threat information to affected company personnel via direct communications (radio, email, text, in person).	
	16.004	Administrative or security personnel at this entity have been granted access to the unclassified intelligence based internet site such as HSIN (Homeland Security Information Network), Cybercop, or Infragard and they regularly review current intelligence information relating to their industry.
	Standard: The entity has personnel who have been granted access to HSIN, Cybercop, Infragard, or other appropriate network and frequently access the site.	

Vehicle Security	16.005	Administrative or security personnel at this entity/facility regularly check the status of the DHS sponsored National Terrorism Alert System (NTAS) or have enrolled to receive automatic electronic NTAS alert updates at www.dhs.gov/alerts .
	Standard: This entity has personnel who regularly access the DHS NTSA site, or automatically receives updates from an accredited government site.	
	Security Action Item Resource Library	
	<u>DHS National Terrorism Advisory System</u>	
	<u>DHS Homeland Security Information Network</u>	
	<u>Infragard</u>	
	17.000	Conduct Regular Security Inspections
	The purpose of conducting frequent and consistent inspections of vehicles is to ensure prompt identification and resolution of security issues, gaps, or conditions.	
	Security Action Item Element	
	17.001	In addition to any pre-trip safety inspection conducted, this entity requires a pre-trip vehicle security inspection.
Standard: This entity has written, fully implemented procedures in place, and security inspections are documented (i.e. security inspection checklists). (NOTE: This is in addition to DOT-mandated Safety Inspections.)		
17.002	This entity requires a post-trip vehicle security inspection.	
Standard: This entity has written, fully implemented procedures in place, and security inspections are documented (i.e. security inspection checklists). (NOTE: This is in addition to DOT-mandated Safety Inspections.)		
17.003	This entity requires additional vehicle security inspections at any other times (vehicle left unattended, driver change, etc.).	
Standard: This entity has written, fully implemented procedures in place. Vehicles receive a security inspection if left unattended, after a driver change, etc. (NOTE: This is in addition to DOT-mandated Safety Inspections.)		

	17.101MC	This entity requires a "passenger count" or ticket re-verification be taken any time passengers are allowed to exit and re-enter the bus.
	Standard: This entity has a written, fully implemented policy in place, which requires re-verification by name/ticket	
	17.201SB	This entity requires a "passenger count" be taken any time passengers are allowed to exit and re-enter the bus.
	Standard: This entity has a written, fully implemented policy in place, which requires re-verification by name or number.	
	17.301TR	This entity requires drivers to verify (to the extent possible) that the materials being shipped match the trip manifest/shipping papers.
	Standard: This entity has a written, fully implemented policy in place.	
Security Action Item Resource Library		
<u>APTA Conducting Vehicle Security Inspections</u>		
18.000	Have Procedures for Reporting Suspicious Activities	
The purpose of this Security Action Item is to proactively prepare for a security event by ensuring the timely reporting of suspicious activities, both internal and external.		
Security Action Item Element		
Vehicle Security	18.001	This entity has participated in or received some type of domain awareness/SAR/counterterrorism training.
	Standard: All employees receive domain awareness training and employees receive some type of re-training at least every three years.	
	18.002	This entity has policies requiring employees to report security related "suspicious activities" to management and/or law enforcement.
	Standard: This entity has written, fully implemented procedures in place requiring employees to report suspicious activities to management and/or law enforcement.	
	18.003	This entity has notification procedures (who to call, when to call, etc.) for all personnel upon observing suspicious activity.

Vehicle Security	Standard: This entity has written, fully implemented procedures in place. Procedures include who to call, when to call, etc.	
	18.004	This entity has policies requiring a written report be filed for suspicious activities observed.
	Standard: This entity has written, fully implemented procedures in place	
	18.005	The entity has policies requiring employees to report internal suspicious activity to their supervisor or management.
	Standard: This entity has written, fully implemented procedures in place that specifically address internal suspicious activity (insider threat, etc.).	
	19.000	Ensure Chain of Custody & Shipment/ Service Verification
	The purpose of this Security Action Item is to ensure the security of shipments and/or passengers through effective Chain of Custody procedures.	
	Security Action Item Element	
	19.101MC	This entity requires confirmation of arrival upon reaching final destination.
	Standard: The entity has procedures requiring an affirmative telephone, radio, or automated response (more than only location information from GPS)	
19.102MC	This entity prohibits the use of alternate drivers without specific entity authorization.	
Standard: This entity has written, fully implemented procedures in place.		
19.201SB	This entity requires confirmation upon arrival at final non-school destinations (final drop-offs, field trips, extracurricular activities, etc.)	
Standard: This entity has policies requiring confirmation upon arrival at final non-school destinations (final drop-offs, field trips, extracurricular activities, etc.)		
19.202SB	This entity prohibits the use of alternate drivers without specific entity authorization.	
Standard: This entity has policies prohibiting the use of alternate drivers without specific entity authorization.		

19.301TR	This entity requires confirmation of shipment delivery upon arrival.
Standard: The entity has procedures requiring an affirmative telephone, radio, or automated response (more than only location information from GPS)	
19.302TR	This entity requires that shipments not be subcontracted or turned over to another driver without specific entity authorization.
Standard: This entity has policies prohibiting drivers from subcontracting or turning over shipments to another driver without specific entity authorization	
19.303TR	This entity requires advance notice to the consignee or point of destination regarding anticipated delivery information.
Standard: This entity has written, fully implemented procedures in place that require advance notice to the consignee or point of destination regarding anticipated delivery information	
19.401	This entity requires specific security protocols be followed in the event a trip must be delayed, discontinued, requires multiple days to complete or exceeds hours-of-service regulations.
Standard: This entity has written, fully implemented procedures in place.	

20.000	Pre-plan Emergency Travel Routes	
Vehicle Security	The purpose of this Security Action Item is ensure that alternative travel routes are established to use in the event of a security or emergency incident.	
	Security Action Item Element	
	20.001	This entity prohibits drivers from diverting from authorized routes, making unauthorized pickups or stopping at unauthorized locations without justification.
	Standard: The entity has written, fully implemented procedures in place prohibiting drivers from diverting from authorized routes, making unauthorized pickups, or stopping at unauthorized locations without justification.	
	20.002	This entity has identified alternate routes in the event primary routes cannot be used under certain security related emergencies.
Standard: Alternate routes are established and in writing, or dispatch can readily provide alternate routes to drivers.		