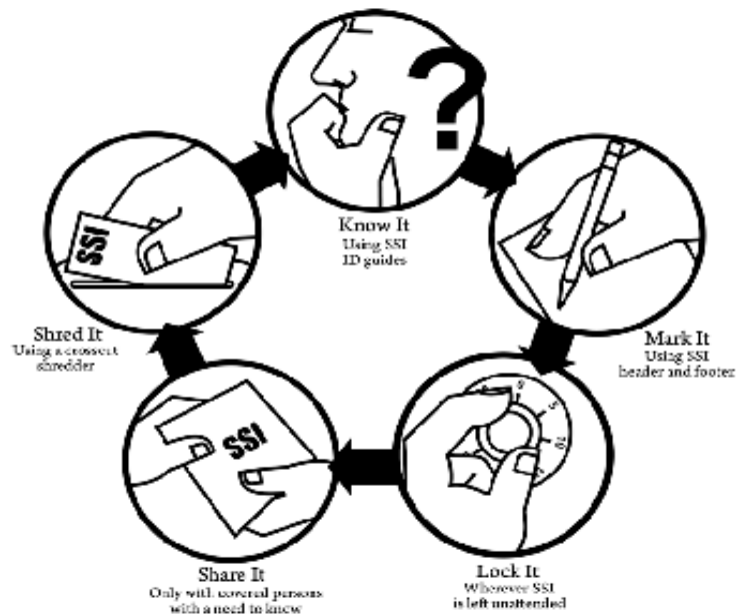


DEPARTMENT OF HOMELAND SECURITY

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.



DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

Highway BASE SCORING GUIDANCE

The following general convention should be referenced when scoring security elements:

- o "0" Security element should be in place but does not exist. (Equates to total non-adherence – 0%)
- o "1" Security element exists, but does not include all essential recommended components. (Equates to minimal adherence – 25-50%)
- o "2" Security element is in place with all essential components but not fully implemented or practiced. (Equates to partial adherence – 50-75%)
- o "3" Security element is in place and practiced but not monitored or periodically reviewed. (Equates to strong adherence, but not full implementation – 75-99%)
- o "4" Security element is in place, fully implemented and regularly reviewed/verified. (Equates to full implementation – 100%) Also assigned to "yes/no" question having a "Yes" response.
- o "N/A" Checked - Security element is not applicable and rational must be given to support the N/A rating.

Question #	SECURITY ACTION ITEMS (SAI'S)	REVIEW/VERIFICATION STEPS	Scoring Criteria
		Management and Accountability:	
Question #	SAI #1 – Have a Designated Security Coordinator	Review Steps	Scoring Criteria
1.001	This entity designates a qualified primary Security Coordinator/ Director.	Verify through a review of documents or interviews that the entity has a qualified person designated as Security Coordinator/Director that is responsible for overall transportation security. Recommended 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. Recognized supplemental certifications in security, safety, or environmental programs may be beneficial.	Someone with this title must be identified (may be shared title). 4 = Fully implemented including this title being documented. 3, 2, 1 = Yes, but with varying degrees of implementation 0 = None
1.002	This entity designates an alternate Security Coordinator/Director.	Verify through a review of documents or interviews that the entity has someone designated to fill this role in the primary Security Coordinator's absence.	Someone with this title must be identified (may be shared title). 4 = Fully implemented including this title being documented. 3, 2, 1 = Yes, but with varying degrees of implementation 0 = None
1.003	This entity has policies that specify the transportation related duties of the Security Coordinator.	Verify through a review of documents or interviews that specific, transportation security-related duties of the Security Director are documented, not merely captured as "other duties." Security Coordinator duties would include: Implementing security actions under the security plan; coordinating security improvements; receiving communications from appropriate federal officials; and other duties.	4 = Documented specific <u>transportation</u> security related duties of Security Coordinator. May be found in job description, security plan, or other documents as appropriate. 3, 2, 1 = Policies are in place, but not documented. Security Coordinator duties assigned and followed with varying degrees of implementation 0 = No transportation security related duties specified.
Question #	SAI #2 – Conduct a Thorough Vulnerability Assessment	Review Steps	Scoring Criteria
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.	Verify through a review of documents, interviews, or physical inspection that the entity has (or does not have) assets that may be of interest to terrorists (passengers, chemicals, vehicles, IT, etc.) and/or may be in physical proximity to other critical assets that could be targeted, and uses these factors in designing their security procedures. Assets may include vehicles, platforms, stations, terminals, fueling depot, key personnel, information systems, cargo, passengers, storage areas, etc.	4 = Yes, entity has identified critical assets and considers this when developing security practices. 3,2,1 = Yes, entity is aware of its potential value to terrorists, and develops security practices with a varying degree of implementation. 0 = if no, or "never thought about it."
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.	Verify through a review of documents, interviews, or physical inspection that the entity has conducted a site-specific security Vulnerability Assessment that includes threat, and consequence components, and note any known risks identified. Assessment must be current and/or reviewed at least annually.	4 = Has a site specific written Vulnerability Assessment" and is familiar with threats and consequences present. This assessment is current or reviewed at least annually. 3 = Has a written "Vulnerability Assessment" & is aware of T&C, but is outdated or not reviewed at least annually. 2 = Poorly Written "Vulnerability Assessment" that does not address all necessary elements and/or is outdated. 1 = General vulnerability assessment (physical "walk around") 0 = Not conducted
2.003	Management generally supports efforts to improve security and provides funding and/or approves corrective actions to security vulnerabilities or weaknesses identified.	Verify through a review of documents or interviews if entity management generally supports efforts to improve security and has implemented corrective actions and/or provided funding for security enhancements.	4 = Management generally supports security improvements and corrective actions have been taken; or no vulnerabilities or weaknesses were identified. 3,2, 1 = Vulnerabilities or weaknesses were identified and corrective actions taken with varying degrees of implementation. 0 = No corrective actions identified

Question #	SAI # 3 - Develop a Security Plan (Security Specific Protocols)	Review Steps	Scoring Criteria
3.001	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.	Verify through a review of documents or interviews that the entity/facility has written, site specific Security Plan to be followed in the event of a security incident or terrorist event. Note: Keep in mind the "Security Plan" is a general term and an entity may refer to this plan as another title. The TSI should ensure that the plan being reviewed deals specifically with transportation security elements and use this information for their scoring justification.	4 = Security Plan is either a standalone document or clearly segmented part of another plan that is readily available. This plan addresses transportation security elements including; 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. 3 = Documented security procedures are in place, incorporated as part of another document, but are not in a clearly segmented section. 2, 1 = Some, but not all security procedures are documented and addressed. 0 = No security plan / procedures documented.
3.002	This entity limits access to its security plan or security procedures to employees with a "need-to-know."	Verify through a review of documents or interviews that confidential security measures used, vulnerabilities identified, and known threat concerns are made known only to employees having a valid "need to know." Note: Generally not all employees may have a "need-to-know."	4 = Yes, security procedures are compartmentalized and made known only to employees with a need to know. 3 = Yes, security procedures are partially guarded and are generally made available only to employees with a need to know 2, 1 = Partially with unique variations 0 = No
3.003	This entity requires that employees with access to security procedures sign a non-disclosure agreement (NDA).	Verify through a review of documents or interviews that employees having access to security information are required to sign a non-disclosure agreement designed keep confidential information confidential.	4= Security specific NDA 3 = General corporate NDA 2, 1 = Partially, with unique variations 0 = No NDA
3.004	This entity has written security plans/policies that have been reviewed and approved at the entity's executive level.	Verify through a review of documents or interviews that executive level officials have approved all security procedures at this entity/facility and their endorsement is documented.	4 = Security Procedures have been approved and signed at the entity's executive level. 3 = Reviewed and signed at lower level without executive endorsement. 2, 1 = Verbal plan/policies discussed and approved without signature. 0 = No security plan to be reviewed.
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.	Verify through a review of documents, interviews, or physical inspection that 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 at this entity.	4 = Yes, written security procedures for all employees 3, 2, 1 = Partially, with unique variations 0 = No procedures in place
3.006	The entity has procedures for responding to an active shooter event.	Verify through a review of documents and interview that the entity has policies and procedures for responding to an active shooter (Run/Hide/Fight, etc.).	4 = Yes, the entity has well-developed written procedures that specifically address active shooter events 3, 2, 1 = Partially, with varying degrees of implementation 0 = No procedures in place
3.007	This entity requires that their security policies be reviewed at least annually and updated as needed.	Verify through a review of documents or interviews that an annual review of any written security procedures is required, and note the date they were last reviewed or updated to determine how often updates are actually being conducted.	4 = Documented review within past year 3, 2, 1 = Documented review occurred but not within past year and/or with unique variations 0 = No security policies exist and/or reviewed
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.	Verify through a review of any "contact lists" provided to employees that entity/facility security personnel are included on the list and that the data is regularly updated.	4 = Yes, documented, updated, and readily available. Phone-tree exercises in place. 3 = Yes, documented and readily available. May be outdated or no phone-tree exercises in place. 2, 1 = Partially, with unique variations 0 = No
	This entity has procedures for 24/7 notification of entity security personnel and/or local/state/federal	Verify through a review of documents or interviews that guidelines are provided to employees requiring	4 = Yes, documented and readily available. Note: If 911 is the only notification number, this does not qualify as a 4.

3.009	authorities to be notified in the event of a security incident.	them to notify, at a minimum, local law enforcement authorities and the entity/facility security coordinator in the event of a security incident or breach.	3,2 = Partially, with unique variations 1 = 911 is the only notification made 0 = No
Question #	SAI # 4 – Plan for Emergency Response & Continuity of Operations	Review Steps	Scoring Criteria
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).	Verify through a review of documents or interviews that this entity/facility has a plan to address the appropriate response to and recovery of business operations (Continuity of Operations Plan) in the event of a significant operational disruption.	4 = 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. 3 = The entity has a well-developed document, missing only a few minor elements or details. The document addresses both operational continuity and business recovery. 2 = The entity’s has a comprehensive plan that covers operational continuity or business recovery. On the other hand, a score of 2 could apply to a generic plan that appears to be a commonly available “template” with only general procedures. 1 = Plan is vague, incomplete, and generally lacking any substance. 0 = No plan / procedures in place.
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.	Verify through a review of documents, interviews, or physical inspection that this entity/facility has an auxiliary power source if needed, and/or the ability to operate effectively from another identified secondary site. (Secondary site must be named and immediate availability must be confirmed).	4 = Full facility auxiliary power source on site/tested or secondary site named and immediately available. Procedures are tested or practiced occasionally. 3 = Secondary site/ auxiliary power source is identified and in place, but not tested or practiced. 2, 1 = Varying degrees of auxiliary power for certain assets on-site/tested or varying degrees of functionality at secondary site. 0 = No auxiliary power available and no secondary site considered.
Question #	SAI # 5 – Develop a Communications Plan	Review Steps	Scoring Criteria
5.001	This entity has methods for communicating with drivers during normal conditions.	Verify through a review of documents or interviews that adequate equipment is available for the entity to communicate with drivers during normal conditions. Radio, cellphone or public address equipment (if applicable) is available for the company to communicate with drivers and/or customers/passengers during normal conditions.	4 = Yes, documented methods are in place and practiced/discussed regularly. 3 = Documented methods are in place, but there are no methods of preparation employed (practice, discussion, etc.) 2,1 = Yes, but with varying degrees of implementation 0 = No
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.	Verify through a review of documents or interviews that this entity has alternative emergency procedures for drivers on the road to follow in the event normal communications with dispatch/management are disrupted.	4 = Yes, documented methods in place, and the entity utilizes back-up technology that will function in the even normal communications are disrupted. 3 = Back-up technology is lacking but the entity has documented, clearly-defined steps for drivers to take in the event normal communications are lost. 2,1 = Yes, but with varying degrees of implementation 0 = No
Question #	SAI # 6 - Safeguard Business and Security Critical Information	Review Steps	Scoring Criteria
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.	Verify through a review of documents or interviews if this facility controls and minimizes internal and external access to sensitive business information (Operational Security – OPSEC).	4= Has written policy to address Operation Security (OPSEC) 3,2,1 = Yes, but with varying degrees of implementation 0 = Issue not addressed
6.002	This entity controls personnel information (i.e. SSN, address, drivers license, etc.) that may be deemed sensitive in nature.	Verify through a review of documents, interviews, or physical inspection if this facility controls and minimizes internal and external access to personnel information (keeps files or office locked).	4= Has written policy to address personnel information 3,2,1 = Yes, but with varying degrees of implementation 0 = Issue not addressed
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.	Verify that the facility/entity has an adequate inventory control process that ensures accountability for all at-risk assets (i.e.; products, vehicles, equipment, computers) that may be of specific interest to criminals and/or terrorists.	4 = A specific, descriptive list of identified “critical assets” along with the knowledge of their general location. These “critical assets” are also periodically inventoried, employees receive some sort of training or briefing on critical asset protection.

			3 = A specific list of critical assets without known locations and/or periodic inventory. 2, 1 = A general inventory of equipment 0 = No inventory control
Question #	SAI # 7 - Be Aware of Industry Security Best Practices.	Review Steps	Scoring Criteria
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).	Determine through interview or documentation if security or administrative personnel at this entity/facility belong to one or more industry groups that provide or share resources or security related guidance. (ATA, NTTC, ACC, NASDPTS, NAPT, OOIDA, others)	4 = Is a member of and actively participates with a trade group(s). 3 = Meets with industry peers and partners, but not a member of an association. 2, 1 = Informal interaction on occasion with industry peers. 0 = No peer involvement.
7.002	Personnel at this entity have sought and/or obtained transportation related security information or "best practices" guidance from external sources.	Determine through interview or documentation if this entity has used or provided security related information (best practices) to or from industry peers or partners.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No
		Personnel Security:	
Question #	SAI # 8 - Conduct Licensing & Background Checks for Drivers / Employees / Contractors	Review Steps	Scoring Criteria
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.	Review through interview or documentation that this entity verifies and documents that persons operating entity vehicles have a valid driver's license for the type of vehicle driven, along with any applicable endorsement(s) needed.	4 = DMV inquiry required upon hire and periodically (multiple times per year) thereafter or is enrolled to receive automatic updates. 3 = DMV inquiry required upon hire and reviewed annually. 2, 1 = DMV inquiry required upon initial hire and not periodically reviewed. 0 = No DMV record required
8.002	This entity requires a criminal history check, verification of Social Security number and verification of immigration status for personnel operating entity vehicles.	Review through interview or documentation that this entity requires a criminal and/or TSA recognized background check for personnel operating entity vehicles. <u>Note: E-Verify gives verification of immigration</u> Some jurisdictions authorize background checks only after an official offer of employment has been made. These after-employment background checks should be rated using the scoring criteria listed.	4 = A fingerprint based FBI background check, CDL-HME or TWIC 3 = Background check thru reputable private entity w/o fingerprints 2 = State or federal "Name Only" background check 1 = Local PD name check only 0 = No check
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.	Review documentation confirming that this entity/facility requires some type of criminal and/or TSA recognized background check on non-driver employees with access to security related information or restricted areas. Some jurisdictions authorize background checks only after an official offer of employment has been made. These after-employment background checks should be rated using the scoring criteria listed.	4 = A fingerprint based FBI background check, CDL-HME or TWIC 3 = Background check thru reputable private entity w/o fingerprints 2 = State or federal "Name Only" background check 1 = Local PD name check only 0 = No check
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.	Verify through interview or a review of documents that this entity asks all applicants if they have been denied a Transportation Worker's Identification Credential (TWIC) or a Commercial Driver's License with HazMat Endorsement (CDL-HME) specifically as the result of a security background check. Asking this is applicable to all modes, designed to identify persons denied employment in	4 = Yes, in application process 3, 2, 1 = Partially, with unique variations 0 = No, not part of application process
8.005	This entity has security-related criteria that would disqualify current or prospective personnel from employment.	Verify through interview or a review of documents that this entity/facility has security criteria that would disqualify current or prospective personnel from employment. Criminal history, credit	4 = Yes, written policies 3, 2, 1 = Yes, but with varying degrees of implementation 0 = No
8.006	This entity has policies to address criminal allegations that may arise or come to light involving current employees.	Verify through interview or a review of documents that this entity reviews and evaluates any new criminal activity information for current employees that may come to light.	4 = Has written policy to address issue 3, 2, 1 = Informal process in place with varying degrees of implementation 0 = Not been addressed
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 employees and contracted employees. Contract	Verify through interview or a review of documents that this entity/facility has comparable licensing and background check requirements for both entity employees and contracted employees. Contract	4 = Yes, contractor and entity standards are identical 3, 2, 1 = Partially, with varying degrees of implementation 0 = No

Question #	SAI # 9 – Develop and Follow Security Training Plan(s)	Review Steps	Scoring Criteria
9.001	This entity provides general security awareness training to all employees (separate from or in addition to regular safety training).	Verify through interview or a review of documents that this entity provides general security awareness training for all employees.	4 = Provides security training for all employees 3 = Provided to employees with security related duties and front line employees (i.e. drivers, ticket agents, station managers, etc.) 2, 1 = Minimal training provided during safety meetings 0 = No security training provided
9.002	This entity provides additional security training to employees having specific security responsibilities.	Determine if this entity conducts more in-depth security training to familiarize certain employees with their specific responsibilities in the event of a security incident as outlined in the entity security plan. May be applicable to security coordinator, assistant security coordinator, management, guard staff, individuals with unique duties (fire drill coordinators, evacuation monitors, etc.)	4 = Yes, certain employees have been identified and trained to perform assigned security duties in the event of a security incident 3,2,1 = Yes, with variations (i.e.; certain employees have been informed of unique duties but have not been trained; training is not current; trained employees have left company and not replaced, etc.) 0 = No
9.003	This entity provides periodic security re-training to all employees.	Review through interview or a review of documents to determine if this entity provides periodic security re-training (recurrent training) no less than every three years.	4 = Yes, at least every 3 years for all employees. 3 = Provided every 3 years to employees with security related duties and front line employees (i.e. drivers, ticket agents, station managers, etc.) 2, 1 = Minimal informal security re-training provided occasionally. 0 = No security re-training.
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).	Verify through interview or a review of documents that the security training/re-training being offered by this entity/facility is specific to the type of transportation operation being conducted (trucking, school bus, motor coach or infrastructure).	4 = Yes, security specific and specific to appropriate mode. 3, 2, 1 = Partially, with unique variations. May be some type of general transportation security training. 0 = No
9.005	The entity provides active shooter training to all employees.	Verify through interview or a review of documents that this entity provides training to all employees that is specifically geared toward active shooter events (Run/Hide/Fight, etc.).	4 = All employees, regardless of job function, receive initial training, which is focused on Active Shooter. 3 = Provided to employees with security related duties and front line employees (i.e. drivers, ticket agents, station managers, etc.) 2, 1 = Minimal training provided during safety meetings 0 = No training is provided that specifically addresses active shooter scenarios.
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.	Verify through a review of documents or interviews that this facility requires identical training requirements for both entity employees and contracted employees.	4 = Yes, contractor and entity standards are identical 3, 2, 1 = Partially, with varying degrees of implementation 0 = No
9.007	This entity requires documentation and retention of records relating to security training received by employees.	Verify through interview and/or a review of documents that this entity/facility documents and retains records relating to security training received by employees.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No
Question #	SAI # 10 –Participate in Security Exercises & Drills	Review Steps	Scoring Criteria
10.001	This entity meets with outside agencies (i.e.; law enforcement/first responders/Federal officials) regarding security support and or issues.	Verify through interview or a review of documents that this entity meets with outside agencies (i.e.; law enforcement/first responders) regarding security issues or security exercises/ drills.	4 = Meets regularly regarding security matters 3, 2, 1 = Score based on frequency and/or degree of interaction. Safety drills/exercises/meetings with first responders generally have security related components and should warrant partial credit. 0 = Does not meet with outside agencies
10.002	Personnel at this entity have actually conducted or participated in some type of exercises/drills that involve security related activities.	Verify through interviews or a review of documents that this entity has conducted or participated in some type of security exercises/drills. Examples would include active participation in exercises/drills such as: Tabletops, ISTEP, Situational Drills (bomb threats, hijacking, lock downs, etc.).	4 = Yes, within last 12 months 3, 2, 1 = Score based on frequency and/or degree of interaction. Safety drills/exercises/meetings with first responders have taken place and generally have security related components that should warrant partial credit. 0 = No
10.003	The entity has consulted local law enforcement/ first responders when developing active shooter plans and procedures	Verify through interview that this entity has consulted law enforcement or first responder agencies when developing active shooter plans.	4 = Yes. 0 = No.
10.004	The entity conducts exercises (tabletop or full-scale) that specifically focus on active shooter scenarios.	Verify through interview, review of documents, or observation that this entity has conducted exercises that specifically focus on active shooter scenarios (lockdown, Run/Hide/Fight, etc.).	4 = Yes, within last 12 months 3, 2, 1 = Score based on frequency and/or degree of interaction 0 = No.
10.005	This entity has administrative and/or security personnel trained in the National Incident Management System (NIMS) or Incident Command System (ICS).	Verify through interview or a review of documents that this entity has security personnel trained in the National Incident Management System (NIMS) or Incident Command System (ICS).	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No

		Facility Security:	
Question #	SAI # 11 - Maintain Facility Access Control	Review Steps	Scoring Criteria
11.001	This entity has controlled points of entry/exit for employees and restricts non-employee access to buildings, terminals and/or work areas.	Verify through interview, a review of documents, or physical inspection that this entity/facility controls or limits the points of entry available to employees and restricts non-employee access to the buildings, terminals or work areas. Note: If this is a BASE conducted on the corporate office, scores should be rated as it applies generally to all of their facilities (not just the corporate office/facility visited).	4= Yes, employee entrances and exits are controlled and entry to all buildings, terminals and/or work areas is restricted for non-employees at all facilities. 3 = Entry is restricted to most areas, but not all. 2, 1 = Access is partially restricted, with varying degrees of implementation 0 = Access is not restricted.
11.002	This entity has secured all doors, windows, skylights, roof openings and other access points to all buildings, terminals and/or work areas.	Verify through interview, a review of documents, or physical inspection that this entity/facility has secured all doors, windows, skylights, roof openings, and other access points to all buildings, terminals, and/or work areas.	4= Yes, 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. 3= Access points are secure in most areas, but not all. 2, 1 = Access is partially restricted, with varying degrees of implementation 0 = Access is not restricted.
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.).	Verify through interview, a review of documents, or physical inspection that this entity/facility restricts employee access to certain secure areas located within their building or site. Note: If this is a BASE conducted on the corporate office, scores should be rated as it generally applies to all of their facilities (not just the corporate office/facility visited).	4= Secure areas are clearly identified and access to these secure areas is restricted to certain employees based on job function. 3 = Access to these secure areas is restricted to certain employees based on job function. 2 = Secure areas are clearly identified, but access is not restricted. 1 = Restricted access is implied but not adhered to. 0 = Secure areas are needed, but not identified by entity.
11.004	This entity issues photo-identification cards/badges or uses other effective identification methods to identify employees.	Verify through interview, a review of documents or physical inspection that this entity/facility issues identification cards/badges or other effective identification methods to identify all employees.	4 = Entity-issued photo ID badges issued to all employees. 3 = Other effective ID badges are issued to all employees. 2 = Photo ID badges issued to some employees, but not all. 1 = Non-photo ID badges issued to some employees 0 = Badges are needed, but not issued.
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.	Verify through interview, a review of documents, or physical inspection that this entity/facility requires employees to carry and/or display an identification badge while on duty	4 = 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. 3 = Requirements are in place, but no measures of verification take place. 2,1 = Some employees are required to display/carry ID cards/badges, but not all (i.e. drivers, warehouse workers, office workers, etc.) 0 = No ID cards/badges issued or there is no requirement in place.
11.006	This entity has a challenge procedure that requires employees to safely report unknown persons or persons not having proper identification.	Verify through interview, a review of documents, or physical inspection that this entity/facility requires employees to report unknown persons or persons not having proper identification.	4 = This entity has a written policy in place requiring employees to safely report unknown persons or those not having proper identification. 3 = This entity has a verbal policy requiring employees to report unknown persons or those not having proper identification. 2,1 = Varying degrees of implementation. No specific policy, but a general understanding is in place.

			0 = No policy in place.
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).	Verify through interview, a review of documents or physical inspection that this entity/facility requires biometric input, key card, PIN, combination locks, for access to buildings, sites or secure areas.	4 = This entity utilizes personal identifying access control (i.e. biometric, key card and/or PIN). Access is deactivated upon employee separation. 3 = This entity utilizes combination type locks and combinations are changed periodically and upon employee separation. 2,1 = Personal identifying access control or combination locks are in use, but not deactivated or periodically changed. 0 = No advanced physical control locking measures are used.
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).	Verify through interview, a review of documents or physical inspection that this entity/facility records entrance/exit data for persons accessing restricted areas, and the data can be reviewed, if needed, either manually or electronically.	4 = 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. 3 = The entity requires the use of an entry/exit written log, time card or signature of personnel entering that is retained for review as needed. 2,1 = Entry/Exit requirements are sporadically used or other unique variations in place. 0 = The entity captures no info on persons entering or exiting.
11.009	This entity utilizes visitor control protocols for non-employees accessing non-public areas.	Verify through interview, a review of documents or physical inspection that this entity/facility requires documented visitor control protocols for visitors/guests. TSA site visit should verify procedures used.	4 = Yes, visitor positively identified, logged-in, is issued visitor badge and escorted while on premises. 3 = Visitors are positively identified, but not escorted –OR– Visitors are escorted, but not positively identified. 2, 1 = Unique variations of above. 0 = No protocols in place.
Question #	SAI # 12 - Implement Strong Physical Security at all Locations	Review Steps	Scoring Criteria
12.001	This entity utilizes perimeter physical security barriers (fences/gates/walls/planter/bollards, etc.) that restrict both unauthorized vehicle and pedestrian access.	Verify through observations or a review of documents, interviews that perimeter physical security barriers to restrict unauthorized vehicles and pedestrians are utilized. Note: If this is a BASE conducted at the corporate office, scores should be rated as it generally applies to all of their facilities (not just the corporate office/facility visited).	4 = This entity utilizes physical barriers that restrict both unauthorized vehicle and pedestrian access at all locations. 3 = Entity utilized physical barriers that somewhat restrict either vehicles or pedestrians at all/most entry points. 2, 1 = This entity utilizes physical barriers to a varying degrees of effectiveness. 0 = No physical barriers are utilized.
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.	Verify through a review of documents, interviews, or physical inspection that the physical barriers used by this entity/facility are functional, used as designed, and adequately maintained to effectively restrict vehicle and/or pedestrian access at this	4 = Yes 3, 2, 1 = Varying degrees of functionality. 0 = No
12.003	This entity utilizes a tamper resistant intrusion detection system(s) (burglary/robbery alarm).	Verify through a review of documents, interviews, or physical inspection that this entity has an intrusion detection system (burglary/robbery alarm) at this and/or all locations.	4 = Windows/doors/interior at all locations are covered and a tamper resistant system is monitored 24/7 when armed. 3 = Some , but not all facilities are covered and system is monitored 24/7 when armed. 2 = Entity only has audible alarm at all locations, not monitored. 1 = Entity only has audible alarm at some locations, not monitored. 0 = No intrusion detection system.
12.004	This entity utilizes closed circuit television cameras (CCTV).	Verify through a review of documents, interviews, or physical inspection that this entity/facility has closed circuit television cameras (CCTV).	4 = Yes, and adequate coverage is maintained at all locations 3, 2, 1 = Yes, but adequate coverage is not provided at all locations 0 = No
12.005	The CCTV cameras present are functional and adequately monitored and/or recorded.	Verify through a review of documents, interviews, or physical inspection that the CCTV cameras used by this entity/facility are functional, used as designed, provide effective coverage, and are adequately monitored.	4 = A CCTV system is utilized at all locations and is actively monitored and/or recorded 24/7. Note: To warrant a 4 the CCTV system must cover all applicable areas. 3 = Some , but not all locations are covered by CCTV systems and system is monitored 24/7 and/or recorded. 2 = CCTV systems are only passively monitored. 1 = Utilizing non functional cameras as a general deterrent. 0 = No intrusion detection system.
	This entity has adequate security lighting.	Verify through a review of documents, interviews,	4 = Yes, lighting is clearly adequate.

12.006		or physical inspection that this entity/facility has adequate security lighting at this and/or all locations.	3,2,1 = Level of lighting varies. 0 = Not adequate or none.
12.007	This entity utilizes key control procedures for buildings, terminals and gates (excludes vehicles).	Verify through a review of documents, interviews, or physical inspection that this facility has a key control program for <u>buildings, terminals and gates</u> .	4 = Yes, an active key control program for buildings & facilities is in place and all keys are accounted for and regularly <u>maintained</u> . 2 = An active key control program for buildings & facilities is in place, but not strictly enforced. Some keys may be unaccounted for. 0 = No key control program is in place.
12.008	This entity employs on-site security personnel.	Verify through a review of documents, interviews, or physical inspection that this entity on-site security guards. Note: "On-site security personnel" should be someone who performs physical security functions (i.e. perimeter checks, gate guards, ID badge checks, etc.) This is in addition to the Security Coordinator/Alternate.	4 = This entity has dedicated security personnel who are effectively deployed and equipped with firearms. 3 = This entity has dedicated security personnel who are effectively deployed and not equipped with firearms. 2 = This entity has security personnel who are used on a part-time basis only (e.g. may visit the site randomly at unannounced intervals, may share security responsibilities with other companies in the area, may be deployed only during heightened levels of concern or for special events/occasions, has personnel who perform security duties as function secondary to their main responsibilities, or other part-time deployment pattern.) 1 = Procedures have been established with local law enforcement personnel or security contractors to quickly deploy security assets if needed. 0 = No on-site security personnel are utilized.
12.009	This entity provides a secure location for employee parking separate from visitor parking.	Verify through a review of documents, interviews, or physical inspection that this facility provides a secure location for employee parking.	4 = Yes 3, 2, 1 = Partially, with varying degrees of implementation. 0 = No
12.010	Clearly visible and easily understood signs are present that identify restricted or off-limit areas.	Verify through a review of documents, interviews, or physical inspection that clearly visible and easily understood signs are used that identify restricted or <u>off-limit areas at this entity/facility</u> .	4 = Yes 3,2 or 1 = Partially, with varying degrees of implementation 0 = No
12.011	Vehicle parking, stopping or standing is controlled, to the extent possible, along perimeter fencing or near restricted areas.	Verify through a review of documents, interviews, or physical inspection that vehicle parking, stopping or standing is adequately restricted, to the extent possible, in areas within or adjacent to all facilities.	4 = Yes 3,2,1 = Partially, with varying degrees of implementation. 0 = Not restricted. N/A = If parking problems exist that facility has no authority to control
12.012	This entity controls the growth of vegetation so that sight lines to vehicles, pedestrians, perimeter fences or restricted areas are unobstructed.	Verify through a review of documents, interviews, or physical inspection that this entity adequately controls growth of vegetation so that sight lines to <u>vehicles, pedestrians or restricted areas remain</u>	4 = Yes 3,2,1 = Partially, with varying degrees of implementation. 0 = No
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.).	Verify through a review of documents, interviews, or physical inspection that this 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 initiatives.	4 = Random security checks are <u>regularly</u> conducted by entity or outside agencies. 3 = Random security checks are <u>occasionally</u> conducted by entity or outside agencies. 2, 1 = Random security checks are occasionally conducted, but only on certain security countermeasures. 0 = None are conducted.
Question #	SAI # 13 - Enhance Internal and External Cyber Security	Review Steps	Scoring Criteria
13.001	This entity requires an employee logon and password that grants access to limited data consistent with job function.	Verify through a review of documents, interviews, or physical inspection that this entity requires an employee logon and password that grants access to limited entity data consistent with job function.	4 = Yes, logon required giving limited access based on job function and must be reset periodically. 3= Yes, logon required giving limited access based on job function, but no password resets are required. 2 = Yes, but logon gives unrestricted access to all employees. 0 = No logon/password is required.
13.002	This entity utilizes an Information Technology (IT) "firewall" that prevents improper IT system access to entity information from both internal and external threats.	Verify through a review of documents, interviews, or physical inspection that this entity/ facility utilizes an IT "firewall" that prevents improper IT system access to entity information from both internal and external threats. Note: Most Windows and Mac based operating systems come preloaded with a standard "firewall." Companies should/may want to consider speaking with an IT Security Consultant to ensure adequate system security.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No


13.003	This entity has sufficient IT security guidelines.	Verify through a review of documents, interviews, or physical inspection that this entity has sufficient IT security guidelines.	4 = Yes, IT security guidelines are written and fully 3, 2, 1 = With varying degrees of implementation. 0 = No
13.004	This entity identifies a qualified IT security officer or coordinator.	Verify through a review of documents, interviews, or physical inspection that this entity identifies an IT security officer or coordinator.	Someone trained and competent in IT security with this title must be identified (may be shared title). 4 = Fully implemented including this title being documented. 3, 2, 1 = Yes, but with varying degrees of implementation 0 = None
13.005	This entity tests their IT system for vulnerabilities.	Verify through a review of documents, interviews that this entity tests its IT system for vulnerabilities.	4 = Yes, IT tests are conducted regularly by a qualified individual. 3, 2, 1 = Partially, with varying degrees of implementation 0 = No
13.006	This entity has off-site backup capability for data generated and system redundancy.	Verify through a review of documents, interviews, or physical inspection that this entity provides off-site backup for data for this and/or all locations.	4 = Yes 3, 2, 1 = Partially, with varying degrees of implementation 0 = No
Vehicle Security			
Question #	SAI # 14 - Develop a Robust Vehicle Security Program	Review Steps	Scoring Criteria
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).	Verify through a review of documents, interviews, or physical inspection that this entity equips vehicles with adequate door/window locks and requires their use (if not prohibited by State law) when vehicles are unattended	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No N/A = if prohibited by State law.
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.	Verify through a review of documents, interviews, or physical inspection that this entity provides some type of supplemental equipment for securing vehicles (i.e.; steering wheel locks, theft alarms, "kill switches," other devices).	4 = Yes, all vehicles have some type of supplemental securing equipment. 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
14.003	This entity utilizes a key control program for their vehicles (separate from key control for buildings.)	Verify through a review of documents, interviews, or physical inspection that, based on the level of risk and the assets present, this entity/facility has an adequate key control program for their vehicles. Use of a unique PIN key code specific to one person to start keyless vehicles would be an acceptable alternative.	4 = Yes, an active <u>vehicle</u> 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. 3 = An active <u>vehicle</u> key control program is in place, but not strictly enforced. Some keys may be unaccounted for or key codes may be shared. 2, 1 = Partially, with unique variations 0 = No key control program is in place.
14.004	This entity employs technology that requires the use of key card, PIN or biometric input to enter or start vehicles.	Verify through a review of documents, interviews, or physical inspection that this entity uses key card, PIN or biometric input to enter or start vehicles.	4 = Yes, all vehicles have some type of key card, PIN or biometric reader to enter or start. 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
14.005	This entity equips vehicles or provides drivers with panic button capability.	Verify through a review of documents, interviews, or physical inspection that this entity equips vehicles with any type of panic button capability or provides keychain push button initiator for drivers to carry.	4 = Yes, all vehicles have panic button capability. 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No

14.006	This entity uses a unique distress code or signals to allow dispatch and drivers or other employees to communicate in the event of an emergency situation.	Verify through a review of documents, interviews, or physical inspection that this entity uses unique distress codes or signals to alert dispatch, police or other employees in the event of an emergency situation; and that codes are changed as necessary.	4 = Yes, all drivers using and all persons receiving the distress codes/signals are trained in their use; codes are changed when necessary. 3, 2, 1 = Partially, with unique variations. 0 = No
14.007	This entity uses vehicles equipped with an interior and/or exterior on-board, functioning and recording video camera.	Verify through a review of documents, interviews, or physical inspection that this entity equips vehicles with any type of interior or exterior on-board video camera.	4 = Yes, all vehicles have on-board video camera(s). 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
14.008	This entity uses vehicles equipped with GPS or land based tracking system.	Verify through a review of documents, interviews, or physical inspection that this entity equips vehicles with some type of GPS or land based tracking system.	4 = Yes, all vehicles are equipped with GPS or land based tracking system. 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
14.009	This entity prohibits unauthorized passengers in entity vehicles.	Verify through a review of documents, interviews, or physical inspection that this entity prohibits unauthorized passengers in entity vehicles.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No
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.).	Verify through a review of documents, interviews, or physical inspection that this entity prohibits the overnight, unsecured parking of entity vehicles at off-site locations (i.e.; residences, shopping centers, parking lots, etc.).	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No policies exist
Question #	SH-15 - Develop a Solid Cargo/Passenger Security Program	Review Steps	Scoring Criteria
	Motor Coach Version	Motor Coach Version	Motor Coach Version
15.101	This entity requires the use of adequate locks on vehicle cargo/ storage areas.	Verify through a review of documents, interviews, or physical inspection that this entity requires the use of locks on cargo or storage doors or other openings.	4 = Yes, all vehicles 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
15.102	This entity equips vehicles with a safety/security barrier between the driver and passengers.	Verify through a review of documents, interviews, or physical inspection that this motor coach entity equips vehicles with a safety/security barrier between the driver and passengers.	4 = Yes, all vehicles 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
15.103	This entity utilizes some type of cargo, baggage or passenger screening system.	Verify through a review of documents, interviews, or physical inspection that this entity uses some type of supplemental passenger/baggage screening system on motorcoaches .	4 = Yes, the entity regularly utilizes some type of cargo, baggage or passenger screening system. 3, 2, 1 = Partially, with varying degrees of implementation. 0 = No
15.104	This Question Deleted - left blank	This Question Deleted - left blank	This Question Deleted - left blank
	School Bus Version		School Bus Version
15.201	This entity requires the use of adequate locks on vehicle cargo/storage areas.	Verify through a review of documents, interviews, or physical inspection that this entity requires the use of locks on cargo or storage doors or other openings.	4 = Yes, all vehicles 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No N/A = if vehicles are not equipped with exterior cargo/storage bays
15.202	N/A - This Question Intentionally left blank.	N/A - This Question Intentionally left blank	N/A - This Question Intentionally left blank.
15.203	This entity or the appropriate school board requires the presence of a school official (other than driver) onboard during all extracurricular transports.	This school system requires a school official (other than driver) during all extracurricular transports (i.e. field trips, off campus sporting events, etc.) Note: A school official may be a designated employee (i.e. teacher, coach, etc.) of the school or	4 = Yes, all extracurricular transports require the presence of a school official (other than driver). 3, 2, 1 = Partially, with varying degrees of implementation. 0 = No
15.204	This Question Deleted - left blank.	This Question Deleted - left blank	This Question Deleted - left blank
	Trucking Version		Trucking Version
15.301	This entity provides appropriate locks for vehicle cargo doors, valves, and/or hatch openings, and requires their use.	Verify through a review of documents, interviews, or physical inspection that this entity requires the use of locks on cargo or storage doors or other openings.	4 = Yes, all vehicles 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No
15.302	This entity provides an adequate supply of seals for vehicle cargo doors, valves, and/or hatch openings, and requires their use.	Verify through a review of documents, interviews, or physical inspection that this trucking entity provides an adequate supply of appropriate seals for cargo doors.	4 = Yes, all vehicles 3, 2, 1 = Partially, provided for use on some vehicles, but not all. Or other unique variations. 0 = No N/A = Locks are used in lieu of seals
15.303	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.).	Verify through a review of documents, interviews, or physical inspection that supplemental trailer security measures are used for trucks.	4 = Yes, all vehicles 3, 2, 1 = Partially, provided for use on some vehicles, but not all. 0 = No
15.304	This Question Deleted - left blank	This Question Deleted - left blank	This Question Deleted - left blank

Question #	SAI # 16 - Plan for High Alert Level Contingencies	Review Steps	Scoring Criteria
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.	Verify through a review of documents, interviews, or physical inspection that this entity has enhanced procedures that take effect in the event of an elevated security alert status from the DHS National Terrorist Alert System (NTAS) or other government source.	4 = Yes, written within Security Plan or security procedures. 3 = Has procedures, but they are not documented. 2, 1 = Partially, with varying degrees of implementation. 0 = No
16.002	This entity monitors news or other media sources for the most current security threat information.	Determine through a review of documents, interviews or physical inspection if this facility monitors TV news, newspapers, homeland security website, or other media sources daily for security threat information.	4 = Yes 3,2,1 = Partially with varying degrees of implementation. Having a general awareness of local, national and/or world events gained through regular exposure to public news sources (newspapers/TV/radio) should warrant partial credit. 0 = No
16.003	This entity distributes relevant or evolving threat information to affected entity personnel as needed.	Determine if and how this entity distributes relevant or evolving threat information to affected entity personnel.	4 = Yes 3, 2, 1 = Yes, with varying degrees of implementation. 0 = No
16.004	Administrative or security personnel at this company have been granted access to an unclassified intelligence based internet site such as HSIN, Cybercop, or Infragard and they regularly review current intelligence information relating to 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	Verify through a review of documents, interviews, or physical inspection that this entity has personnel who have been granted access to HSIN, Cybercop, Infragard, or other appropriate network and frequently accesses the site.	4 = Yes, they have access and regularly review 3, 2, 1 = Yes, some employees have access, but intelligence information is not regularly reviewed. 0 = No
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	Verify through a review of documents, interviews, or physical inspection that this entity has personnel who regularly access the DHS NTSA site.	4 = Yes, They have access and regularly reviewed 3, 2, 1 = Yes, some, but not all employees have access and may not be regularly checked. 0 = No
Question #	SAI # 17 - Conduct Regular Security Inspections	Review Steps	Scoring Criteria
17.001	In addition to any pre-trip safety inspection conducted, this entity requires a pre-trip vehicle security inspection.	Verify through a review of documents, interviews, or physical inspection that this entity, in addition to any pre-trip safety inspection conducted, requires a pre-trip vehicle security inspection. Note: This is in addition to DOT <u>safety</u> requirements.	4 = Yes, procedures are written, fully implemented, and security inspections are documented (i.e. security inspection checklists). 3 = Procedures are written and fully implemented, but no documentation is completed upon inspection. 2 = Unwritten procedures are in place. 1 = Inspections are occasionally conducted. 0 = No pre-trip security inspections are conducted
17.002	This entity requires a post-trip vehicle security inspection.	Verify through a review of documents, interviews, or physical inspection that this entity requires a post-trip vehicle security inspection. Note: This is in addition to DOT <u>safety</u> requirements.	4 = Yes, procedures are written, fully implemented, and security inspections are documented (i.e. security inspection checklists). 3 = Procedures are written and fully implemented, but no documentation is completed upon inspection. 2 = Unwritten procedures are in place. 1 = Inspections are occasionally conducted. 0 = No post-trip security inspections are conducted
17.003	This entity requires additional vehicle security inspections at any other times (vehicle left unattended, driver change, etc.).	Verify through a review of documents, interviews, or physical inspection that this entity requires additional vehicle security inspections at any other times (vehicle left unattended, driver change, etc.).	4 = Yes, every time the vehicle is left unattended, driver change, etc. 3, 2, 1 = Partially, with varying degrees of implementation. 0 = No
	<i>Motor Coach Version</i>	<i>Motor Coach Version</i>	<i>Motor Coach Version</i>
17.101	This entity requires a "passenger count" or ticket re-verification be taken any time passengers are allowed to exit and re-enter the bus.	Verify through a review of documents or interviews that this Motor Coach entity requires a "passenger count" or ticket re-verification be taken any time passengers are allowed to exit and re-enter the bus.	4 = Yes, written policy in place and fully implemented requiring re-verification by name/ticket 3,2,1 = Partially, with varying degrees of implementation (policy may be loosely in place, erratically implemented requiring only headcount) 0 = No
	<i>School Bus Version</i>	<i>School Bus Version</i>	<i>School Bus Version</i>
17.201	This entity requires a "passenger count" be taken any time passengers are allowed to exit and re-enter the bus.	Verify through a review of documents or interviews that this School Bus entity requires a "passenger count" or ticket re-verification be taken any time passengers are allowed to exit and re-enter the bus.	4 = Yes, written policy in place and fully implemented requiring re-verification by name or number. 3,2,1 = Partially, with varying degrees of implementation (policy may be loosely in place, or sporadically implemented requiring only headcount) 0 = No
	<i>Trucking Version</i>	<i>Trucking Version</i>	<i>Trucking Version</i>
17.301	This entity requires drivers to verify (to the extent possible) that the materials being shipped match the trip manifest/shipping papers.	Verify through a review of documents, interviews, or physical inspection that this trucking entity requires drivers to verify (to the extent possible) that the materials being shipped match the trip	4 = Yes, written policy in place and fully implemented 3, 2, 1 = Partially, with unique variations 0 = No
Question #	SAI # 18 - Have Procedures for Reporting Suspicious Activities	Review Steps	Scoring Criteria

18.001	This entity has participated in or received some type of domain awareness/SAR/counterterrorism training.	Verify through a review of documents or interviews that this entity has participated in or received some type of domain awareness, suspicious activity reporting (SAR), or counterterrorism training.	4 = Yes, all employees receive domain awareness training and employees receive some type of re-training at least every three years. 3, 2, 1 = Yes, but with varying degrees of implementation 0 = No
18.002	This entity has policies requiring employees to report security related "suspicious activities" to management and/or law enforcement.	Verify through a review of documents or interviews that this entity has policies requiring employees to report suspicious activities to management and/or law enforcement.	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 0 = No
18.003	This entity has notification procedures (who to call, when to call, etc.) for all personnel upon observing suspicious activity.	Verify through a review of documents or interviews that this entity has written notification procedures (who to call, when to call, etc.) for all personnel upon observing suspicious activity.	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 1 = No
18.004	This entity has policies requiring a written report be filed for suspicious activities observed.	Verify through a review of documents or interviews that this entity requires a police or internal company report be filed for suspicious activities observed.	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 0 = No
18.005	The entity has policies requiring employees to report internal suspicious activity to their supervisor or management.	Verify through a review of documents and interview that the entity requires employees to report internal suspicious activity to their supervisor or management	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 0 = No.
Question #	SAI # 19 - Ensure Chain of Custody & Shipment/ Service Verification	Review Steps	Scoring Criteria
	<i>Motor Coach Version</i>	<i>Motor Coach Version</i>	<i>Motor Coach Version</i>
19.101	This entity requires confirmation of arrival upon reaching final destination.	Verify through a review of documents or interviews that this entity requires confirmation upon arrival at final destination.	4 = Yes, affirmative telephone, radio, or automated response (more than only location information from GPS) 3, 2, 1 = Partially, with unique variations 0 = No
19.102	This entity prohibits the use of alternate drivers without specific entity authorization.	Verify through a review of documents or interviews that this motor coach entity requires confirmation shipment or arrival of passengers at final destination.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No
19.103	This question is intentionally left blank. N/A	This question is intentionally left blank. N/A	This question is intentionally left blank. N/A
	<i>School Bus Version</i>	<i>School Bus Version</i>	<i>School Bus Version</i>
19.201	This entity requires confirmation upon arrival at final non-school destinations (final drop-offs, field trips, extracurricular activities, etc.)	Verify through a review of documents or interviews that this entity requires confirmation upon arrival at final non-school destination.	4 = Yes 3, 2, 1 = Partially, with unique variations 1 = No N/A = Entity conducts only scheduled daily, recurring student pickup/drop off service - no extracurricular trips
19.202	This entity prohibits the use of alternate drivers without specific entity authorization.	Verify through a review of documents or interviews that this school bus entity requires confirmation shipment or arrival of passengers at final destination.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No
19.203	This question is intentionally left blank. N/A	This question is intentionally left blank. N/A	This question is intentionally left blank. N/A
	<i>Trucking Version</i>	<i>Trucking Version</i>	<i>Trucking Version</i>
19.301	*94TR. This entity requires confirmation of shipment delivery upon arrival.	Verify through a review of documents or interviews that this entity requires confirmation upon arrival at final destination.	4 = Yes, affirmative telephone/radio response (more than just location information from GPS) 3, 2, 1 = Partially, with unique variations 0 = No
19.302	95TR. This entity requires that shipments not be subcontracted or turned over to another driver without specific entity authorization.	Verify through a review of documents or interviews that this trucking entity does not allow shipments to be subcontracted or turned over to another driver without specific entity authorization.	4 = Yes 3, 2, 1 = Partially, with unique variations 0 = No
19.303	96TR. This entity requires advance notice to the consignee or point of destination regarding anticipated delivery information.	Verify through a review of documents or interviews that this entity requires confirmation upon arrival at final destination.	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 0 = No
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.	Verify through a review of documents or interviews that 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. Note: These are separate from safety procedures. Example – Where and how do they secure vehicles when they have to be parked overnight.	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 0 = No
Question #	SAI # 20 - Pre-plan Emergency Travel Routes.	Review Steps	Scoring Criteria
20.001	This entity prohibits drivers from diverting from authorized routes, making unauthorized pickups or stopping at unauthorized locations without justification.	Verify through a review of documents or interviews that this entity/ facility prohibits drivers from diverting from the scheduled route and stopping at unauthorized locations.	4 = Yes, written policies are in place and fully implemented. 3 = Policies are in place, but are unwritten. 2, 1 = Partially, with varying degrees of implementation. 0 = No
20.002	This entity has identified alternate routes in the event primary routes cannot be used under certain security related emergencies.	Verify through a review of documents or interviews that this entity has identified alternate routes drivers can use in the event of a security related emergency.	4 = Alternate routes are established and in writing or dispatch can readily provide alternate routes to drivers. 3, 2, 1 = Partially, with unique variations 0 = No

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY Transportation Security Administration											
Highway Baseline Assessment for Security Enhancements (HWY-BASE)								HMC FY2021 V.2 (March 2021)			
 <div style="font-size: 24pt; font-weight: bold; margin-top: 10px;">Transportation Security Administration</div>				Date of Visit		Company DOT #		TSA Field Office		Region #	
				3/4/2021							
				FSD AOR Field Office (Optional)							
				Fill in only if Applicable							
				Company/Facility/Location Address							
TYPE OF VISIT				<Company Name Here>							
Corporate Review				Street							
Revisit?	Virtual?	Date of Last Interview/Visit?		City			State			Zip Code	
				Company Website:							
Transportation Mode				Company Chosen By:							
< Select Mode Here >				HTUA Name:							
EXIS Conducted				RMAST Conducted							
Company Assets:											
Motorized (Power) Units owned/leased/contracted:						# of Company Facilities owned/leased/contracted:					
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		Date		E-mail			
		STSI									
		AFSD-I									
Headquarters Approval											
Name		Title		Airport Code		Date		E-mail			

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Baseline Assessment & Security Enhancement Review Checklist

HMC FY2021 V.2 (March 2021)

Company Name:

<Company Name Here>

Lead Inspector:

0

Assessment Date:

3/4/2021

Description		Findings		Justification	
SECURITY ACTION ITEMS (SAI'S)		N/A	Score	Source	Score Rational
1.000 Management and Accountability					
1.000 SAI #1 – Have a Designated Security Coordinator					
1.001	This entity designates a qualified primary Security Coordinator/ Director.				
1.002	This entity designates an alternate Security Coordinator/Director.				
1.003	This entity has policies that specify the transportation related duties of the Security Coordinator.				
2.000 SAI #2 – Conduct a Thorough Vulnerability Assessment					
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.				
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.				
2.003	Management generally supports efforts to improve security and provides funding and/or approves corrective actions to security vulnerabilities or weaknesses identified.				
3.000 SAI # 3 - Develop a Security Plan (Security Specific Protocols)					
3.001	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.				
3.002	This entity limits access to its security plan or security procedures to employees with a "need-to-know."				
3.003	This entity requires that employees with access to security procedures sign a non-disclosure agreement (NDA).				
3.004	This entity has written security plans/policies that have been reviewed and approved at the entity's executive level.				
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.				
3.006	The entity has procedures for responding to an active shooter event.				
3.007	This entity requires that their security policies be reviewed at least annually and updated as needed.				
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.				
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.				
4.000 SAI # 4 – Plan for Emergency Response & Continuity of Operations					
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).				
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.				
5.000 SAI # 5 – Develop a Communications Plan					
5.001	This entity has methods for communicating with drivers during normal conditions.				
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.				

SENSITIVE SECURITY INFORMATION

6.000	SAI # 6 - Safeguard Business and Security Critical Information			
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.			
6.002	This entity controls personnel information (i.e. SSN, address, drivers license, etc.) that may be deemed sensitive in nature.			
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.			
7.000	SAI # 7 - Be Aware of Industry Security Best Practices.			
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).			
7.002	Personnel at this entity have sought and/or obtained transportation related security information or "best practices" guidance from external sources.			
8.000	Personnel Security			
8.000	SAI # 8 – Conduct Licensing & Background Checks for Drivers / Employees / Contractors			
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.			
8.002	This entity requires a criminal history check, verification of Social Security number and verification of immigration status for personnel operating entity vehicles.			
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.			
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.			
8.005	This entity has security-related criteria that would disqualify current or prospective personnel from employment.			
8.006	This entity has policies to address criminal allegations that may arise or come to light involving current employees.			
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.).			
9.000	SAI # 9 – Develop and Follow Security Training Plan(s)			
9.001	This entity provides general security awareness training to all employees (separate from or in addition to regular safety training).			
9.002	This entity provides additional security training to employees having specific security responsibilities.			
9.003	This entity provides periodic security re-training to all employees.			
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).			
9.005	The entity provides Active Shooter training to all employees.			
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.			
9.007	This entity requires documentation and retention of records relating to security training received by employees.			
10.000	SAI # 10 –Participates in Security Exercises & Drills			
10.001	This entity meets with outside agencies (i.e.; law enforcement/first responders/Federal officials) regarding security support and or issues.			
10.002	Personnel at this entity have actually conducted or participated in some type of exercises/drills that involve security related activities.			
10.003	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.			

SENSITIVE SECURITY INFORMATION

10.005	This entity has administrative and/or security personnel trained in the National Incident Management System (NIMS) or Incident Command System (ICS).				
--------	--	--	--	--	--

SENSITIVE SECURITY INFORMATION

11.000 Facility Security					
11.000 SAI # 11 - Maintain Facility Access Control					
11.001	This entity has controlled points of entry/exit for employees and restricts non-employee access to buildings, terminals and/or work areas.				
11.002	This entity has secured all doors, windows, skylights, roof openings and other access points to all buildings, terminals and/or work areas.				
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.).				
11.004	This entity issues photo-identification cards/badges or uses other effective identification methods to identify 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.				
11.006	This entity has a challenge procedure that requires employees to safely report unknown persons or persons 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).				
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).				
11.009	This entity utilizes visitor control protocols for non-employees accessing non-public areas.				
12.000 SAI # 12 - Implement Strong Physical Security at all Locations					
12.001	This entity utilizes <u>perimeter</u> physical security barriers (fences/gates/walls/planter /bollards, etc.) that restrict both unauthorized vehicle and pedestrian access.				
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.				
12.003	This entity utilizes a tamper resistant intrusion detection system(s) (burglary/robbery alarm).				
12.004	This entity utilizes closed circuit television cameras (CCTV).				
12.005	The CCTV cameras present are functional and adequately monitored and/or recorded.				
12.006	This entity has adequate security lighting.				
12.007	This entity utilizes key control procedures for buildings, terminals and gates (excludes vehicles).				
12.008	This entity employs on-site security personnel.				
12.009	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.				
12.011	Vehicle parking, stopping or standing is controlled, to the extent possible, along perimeter fencing or near restricted areas.				
12.012	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.).				
13.000 SAI # 13 - Enhance Internal and External Cyber Security					
13.001	This entity requires an employee logon and password that grants access to limited data consistent with job function.				
13.002	This entity utilizes an Information Technology (IT) "firewall" that prevents improper IT system access to entity information from both internal and external threats.				
13.003	This entity has sufficient IT security guidelines.				
13.004	This entity identifies a qualified IT security officer or coordinator.				
13.005	This entity tests their IT system for vulnerabilities.				
13.006	This entity has off-site backup capability for data generated and system redundancy.				

SENSITIVE SECURITY INFORMATION

Vehicle Security					
14.000	SAI # 14 - Develop a Robust Vehicle Security Program				
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).				
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.				
14.003	This entity utilizes a key control program for their vehicles (separate from key control for buildings.)				
14.004	This entity employs technology that requires the use of key card, PIN or biometric input to enter or start vehicles .				
14.005	This entity equips vehicles or provides drivers with panic button capability.				
14.006	This entity uses a unique distress code or signals to allow dispatch and drivers or other employees to communicate in the event of an emergency situation.				
14.007	This entity uses vehicles equipped with an interior and/or exterior on-board, functioning and recording video camera.				
14.008	This entity uses vehicles equipped with GPS or land based tracking system.				
14.009	This 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.).				
15.000	SAI # 15 - Develop a Solid Cargo/Passenger Security Program.				
15.100	Motor Coach Version (Questions 77MC-80MC)				
15.101	X	X			
15.102	XXX XXX	X			
15.103	XXX XXX	X			
15.104	This Question Deleted - left blank	X			
15.200	School Bus Version (Questions 77SB-80SB)				
15.201	XXX XXX	X			
15.202	N/A - This Question Intentionally left blank.	X			
15.203	XXX XXX XXX	X			
15.204	This Question Deleted - left blank	X			
15.300	Trucking Version (Questions 77TR-80TR)				
15.301	XXX XXX	X			
15.302	XXX XXX	X			
15.303	XXX XXX XXX	X			
15.304	This Question Deleted - left blank	X			
16.000	SAI # 16 - Plan for High Alert Level Contingencies				
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.				
16.002	This entity monitors news or other media sources for the most current security threat information.				
16.003	This entity distributes relevant or evolving threat information to affected entity personnel as needed.				
16.004	Administrative or security personnel at this company have been granted access to an unclassified intelligence based internet site such as HSIN, Cybercop, or Infragard and they regularly review current intelligence information relating to their industry.				
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.				

SENSITIVE SECURITY INFORMATION

17.000	SAI # 17 - Conduct Regular Security Inspections					
17.001	In addition to any pre-trip safety inspection conducted, this entity requires a pre-trip vehicle security inspection.					
17.002	This entity requires a post-trip vehicle security inspection.					
17.003	This entity requires additional vehicle security inspections at any other times (vehicle left unattended, driver change, etc.).					
17.100	Motor Coach Version (Question 89MC)					
17.101	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
17.200	School Bus Version (Question 89SB)					
17.201	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
17.300	Trucking Version (Question 89TR)					
17.301	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
18.000	SAI # 18 - Have Procedures for Reporting Suspicious Activities					
18.001	This entity has participated in or received some type of domain awareness/SAR/counterterrorism training.					
18.002	This entity has policies requiring employees to report security related “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.					
18.004	This entity has policies requiring a written report be filed for suspicious activities observed.					
18.005	The entity has policies requiring employees to report internal suspicious activity to their supervisor or management.					
19.000	SAI # 19 - Ensure Chain of Custody & Shipment/ Service Verification					
19.100	Motor Coach Version (Questions 94MC-96MC)					
19.101	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
19.102	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
19.103	This question is intentionally left blank. N/A	X				
19.200	School Bus Version (Questions 94SB-96SB)					
19.201	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
19.202	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
19.203	This question is intentionally left blank. N/A	X				
19.300	Trucking Version (Questions 94TR-96TR)					
19.301	X	X				
19.302	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
19.303	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	X				
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.					
20.000	SAI # 20 - Pre-plan Emergency Travel Routes.					
20.001	This entity prohibits 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.					

SENSITIVE SECURITY INFORMATION

Date of Visit	Company DOT #	TSA Field Office
3/4/2021	0	0
Company/Facility/Structure Name		
<Company Name Here>		
Additional Information		
General Description of the Entity		
INSPECTOR SHALL PROVIDE A GENERAL NARRATIVE OVERVIEW OF THE ENTITY'S SCOPE OF OPERATIONS, FACILITIES, ETC.:		
Other information obtained during BASE assessment:		
Smart Practice Information:		
Did you observe anything significant or "cutting edge" in the area of corporate/facility security?		
1. Would you be opposed to TSA conducting a BASE assessment at other sites/facilities affiliated with your company?		
2. Please provide the facility name, address, telephone number and Point of Contact for your Top 5 facilities located in or around major metropolitan areas?		
a.		
b.		
c.		
d.		
e.		
3. Where do you, as an industry, feel vulnerable?		
a.		
b.		
4. What concerns do you have?		
a.		
b.		
5. In what Federal programs or security initiatives does your company participate?		
a.		
b.		
c.		
6. Has this entity previously participated in a DHS/TSA sponsored security assessment (CSR, BASE, etc.)?		
a.		
b.		
Other Persons Interviewed or in Attendance		
Name		
Title:		
Office Tel#		
Email		
Name		
Title:		
Office Tel#		
Email		
Other TSA Personnel in Attendance		
Name		
Title:		
Office Tel#		
Email		
Name		
Title:		
Office Tel#		
Email		

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

For a BASE Assessment targeting all of the levels of implementation BASE Assessment. Then place the number directly below the SAI to be targeted for BASE Assessment.

If this is NOT a Targeted SAI BASE Assessment, enter the previous BASE levels of implementation. Disregard the number to the right.

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

If you have specific SAI's, please enter in the box below. If not, enter the number (1-5) in the box below to identify the current targeted SAI.

For the BASE Assessment, fill in the box below. Leave it as "1".

In the box below, enter the targeted BASE Assessment.

1

SAI 13	SAI 14	SAI 15	SAI 16	SAI 17	SAI 18	SAI 19	SAI 20

enter the current
assessment (1-5)

Overall

SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY	
Transportation Security Administration	
Highway & Motor Carrier BASE Overview	HMC FY2021 V.2 (March 2021)
Lead Inspector:	0
Assessment Date:	3/4/2021
<Company Name Here>	
SAI #	SECURITY SECTIONS
1-7	Management and Accountability
8-10	Personnel Security
11-13	Facility Security
14-20	Vehicle Security




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'S) DESCRIPTION	Implementation
1	Have a Designated Security Coordinator	0%
2	Conduct a Thorough Vulnerability Assessment	0%
3	Develop a Security Plan (Security Specific Protocols)	0%
4	Plan for Emergency Response & Continuity of Operations	0%
5	Develop a Communications Plan	0%
6	Safeguard Business and Security Critical Information	0%
7	Be Aware of Industry Security Best Practices.	0%
8	Conduct Licensing & Background Checks for Drivers / Employees / Contractors	0%
9	Develop and Follow Security Training Plan(s)	0%
10	Participates in Security Exercises & Drills	0%
11	Maintain Facility Access Control	0%
12	Implement Strong Physical Security at all Locations	0%
13	Enhance Internal and External Cyber Security	0%
14	Develop a Robust Vehicle Security Program	0%
15	Develop a Solid Cargo/Passenger Security Program.	N/A
16	Plan for High Alert Level Contingencies	0%
17	Conduct Regular Security Inspections	0%
18	Have Procedures for Reporting Suspicious Activities	0%
19	Ensure Chain of Custody & Shipment/ Service Verification	0%
20	Pre-plan Emergency Travel Routes.	0%

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

Critical Elements Implementation:	0.00%
--	--------------

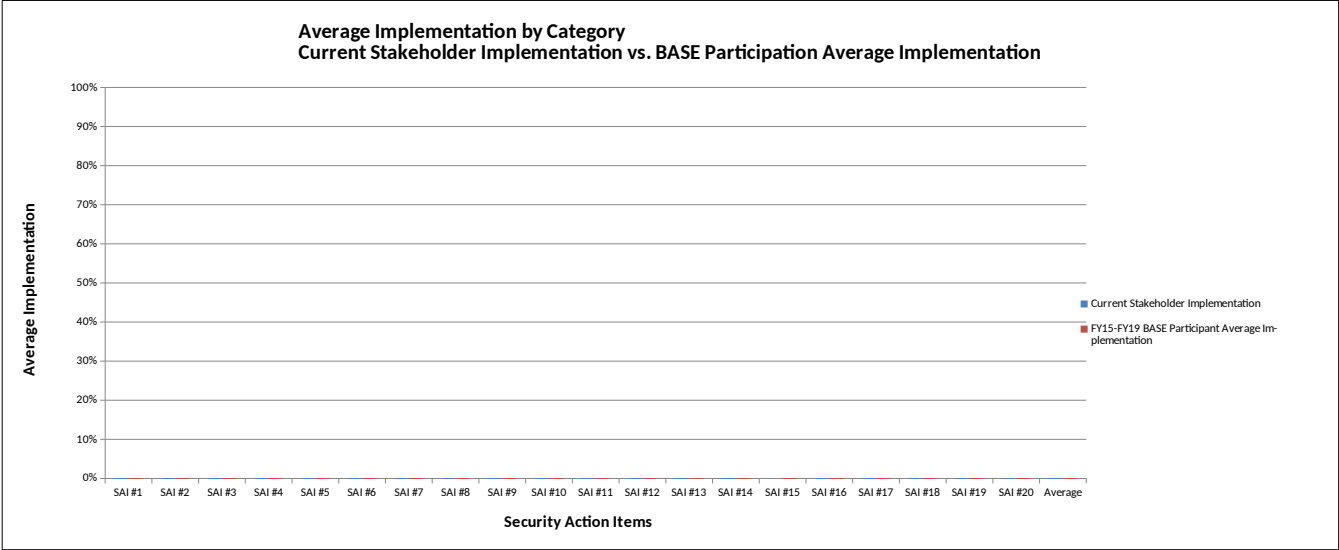
Color Key:

	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.

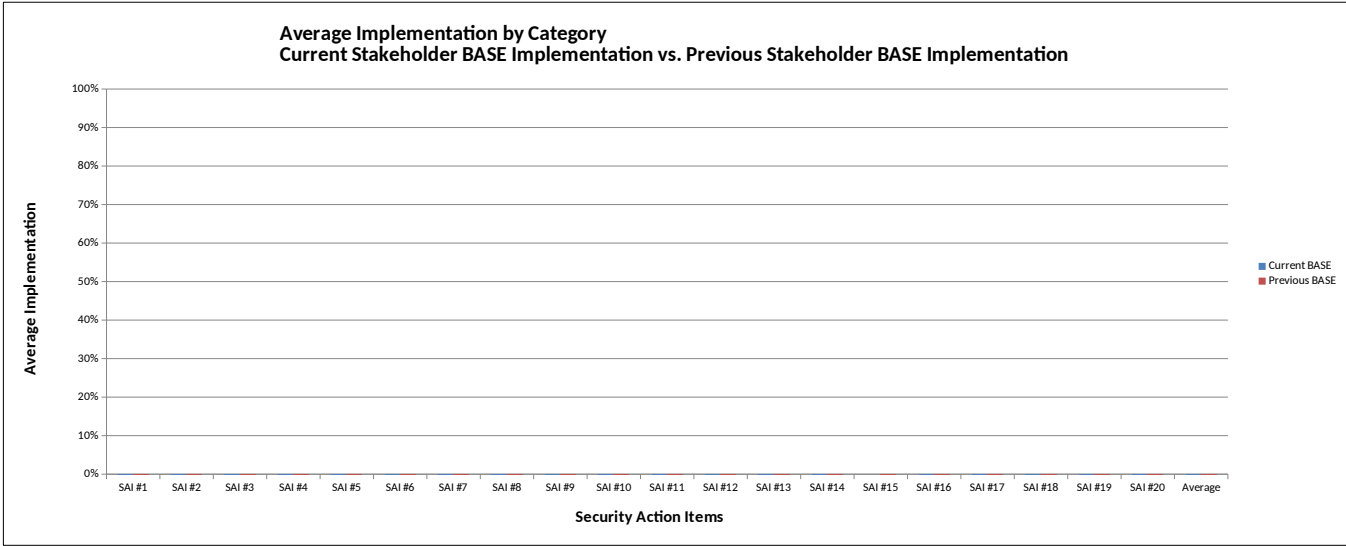
This Agency Did Not Meet the Requirements of the Gold Standard Award.

SENSITIVE SECURITY INFORMATION

Stakeholder vs. Industry Participant Comparison																						
	Mode	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	SAI #18	SAI #19	SAI #20	Average
Current Stakeholder Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	N/A	0%	0%	0%	0%	0%	0.00%
BASE Participant Average Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%
Difference		0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	#VALUE!	0%	0%	0%	0%	0%	0.00%



Current BASE vs. Previous BASE Comparison																						
	Mode	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	SAI #18	SAI #19	SAI #20	Average
Current Stakeholder Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	N/A	0%	0%	0%	0%	0%	0.00%
Previous Stakeholder BASE Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%
Difference		0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	#VALUE!	0%	0%	0%	0%	0%	0.00%



DO NOT MODIFY OR ENTER ANY DATA

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Highway & Motor Carrier Comprehensive Security Assessment

<Company Name Here>

SAI #	SECURITY ACTION ITEM (SAI'S) DESCRIPTION
1	Have a Designated Security Coordinator
2	Conduct a Thorough Vulnerability Assessment
3	Develop a Security Plan (Security Specific Protocols)
4	Plan for Emergency Response & Continuity of Operations
5	Develop a Communications Plan
6	Safeguard Business and Security Critical Information
7	Be Aware of Industry Security Best Practices.
8	Conduct Licensing & Background Checks for Drivers / Employees / Contractors
9	Develop and Follow Security Training Plan(s)
10	Participates in Security Exercises & Drills
11	Maintain Facility Access Control
12	Implement Strong Physical Security at all Locations
13	Enhance Internal and External Cyber Security
14	Develop a Robust Vehicle Security Program
15	Develop a Solid Cargo/Passenger Security Program.
16	Plan for High Alert Level Contingencies
17	Conduct Regular Security Inspections
18	Have Procedures for Reporting Suspicious Activities
19	Ensure Chain of Custody & Shipment/ Service Verification
20	Pre-plan Emergency Travel Routes.

Overall Implementation:

ON THIS SHEET!

SECURITY

stration

AI Comparison	HMC FY2021 V.2 (March 2021)
---------------	--------------------------------

Lead Inspector:	0
-----------------	---

Assessment Date:	3/4/2021
------------------	----------

e>

--

Previous BASE	Implementation	Improvement
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	N/A	#VALUE!
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%
0%	0%	0%

0%	0%	0%
----	----	----

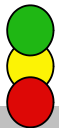
Paperwork Reduction Act Burden Statement: This is a voluntary collection of information. TSA estimates that the total average burden per response associated with this collection is approximately 2 hours. An agency may not conduct or sponsor, and a person is not required to respond to a collection of 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		
Highway & Motor Carrier Targeted BASE Overview		HMC FY2021 V.2 (March 2021)
Lead Inspector:		0
Assessment Date:		3/4/2021
<Company Name Here>		
SAI #	SECURITY ACTION ITEM (SAI'S) DESCRIPTION	Implementation
1	Have a Designated Security Coordinator	0%
2	Conduct a Thorough Vulnerability Assessment	0%
3	Develop a Security Plan (Security Specific Protocols)	0%
4	Plan for Emergency Response & Continuity of Operations	0%
5	Develop a Communications Plan	0%
6	Safeguard Business and Security Critical Information	0%
7	Be Aware of Industry Security Best Practices.	0%
8	Conduct Licensing & Background Checks for Drivers / Employees / Contractors	0%
9	Develop and Follow Security Training Plan(s)	0%
10	Participates in Security Exercises & Drills	0%
11	Maintain Facility Access Control	0%
12	Implement Strong Physical Security at all Locations	0%
13	Enhance Internal and External Cyber Security	0%
14	Develop a Robust Vehicle Security Program	0%
15	Develop a Solid Cargo/Passenger Security Program.	0%
16	Plan for High Alert Level Contingencies	0%
17	Conduct Regular Security Inspections	0%
18	Have Procedures for Reporting Suspicious Activities	0%
19	Ensure Chain of Custody & Shipment/ Service Verification	0%
20	Pre-plan Emergency Travel Routes.	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.

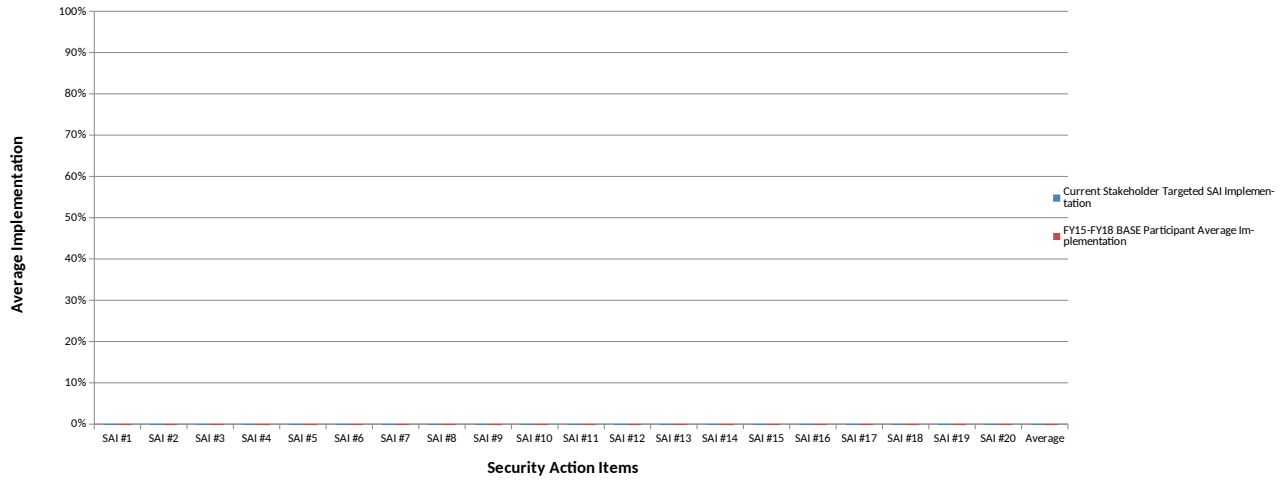
This Agency Did Not Meet the Requirements of the Gold Standard Award.

SENSITIVE SECURITY INFORMATION

Current Stakeholder (Targeted SAI) vs. Industry BASE Participant Comparison

	Mode	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	SAI #18	SAI #19	SAI #20	Average
Current Stakeholder Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%
BASE Participant Average Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%
Difference		0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%

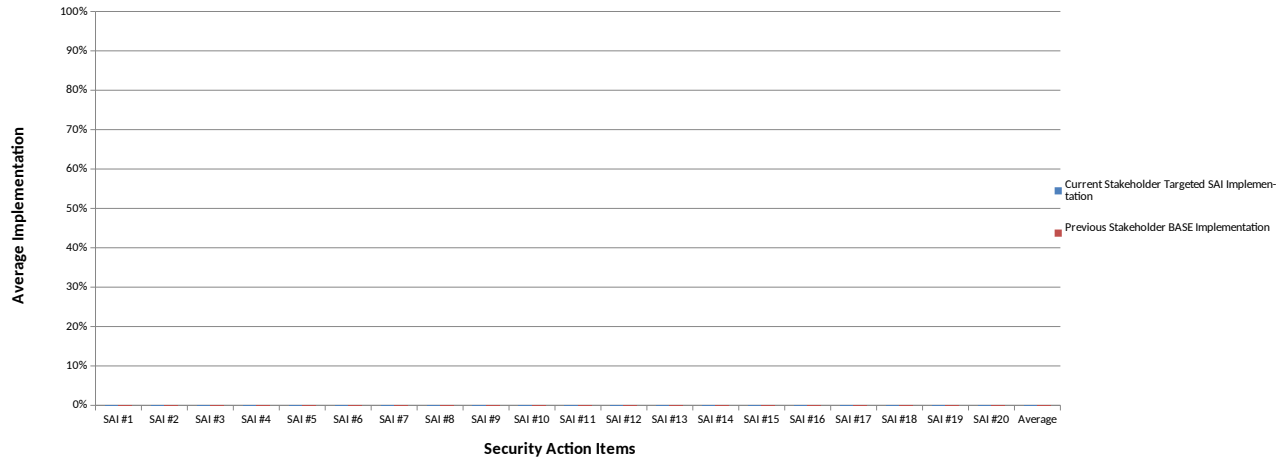
Average Implementation by Category Current Stakeholder Targeted SAI Implementation vs. BASE Participation Average Implementation



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

	Mode	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	SAI #18	SAI #19	SAI #20	Average
Current Stakeholder Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%
Previous Stakeholder BASE Implementation	< Select Mode Here >	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%
Difference		0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.00%

Average Implementation by Category Current Stakeholder Targeted SAI Implementation vs. Previous Stakeholder BASE Implementation



SENSITIVE SECURITY INFORMATION

DEPARTMENT OF HOMELAND SECURITY					
Transportation Security Administration					
Highway & Motor Carrier Targeted SAI Comparison					HMC FY2021 V.2 (March 2021)
Lead Inspector:					0
Assessment Date:					3/4/2021
<Company Name Here>					
SAI #	SECURITY ACTION ITEM (SAI'S) DESCRIPTION	Previous BASE	Implementation		Improvement
1	Have a Designated Security Coordinator	0%	0%		0%
2	Conduct a Thorough Vulnerability Assessment	0%	0%		0%
3	Develop a Security Plan (Security Specific Protocols)	0%	0%		0%
4	Plan for Emergency Response & Continuity of Operations	0%	0%		0%
5	Develop a Communications Plan	0%	0%		0%
6	Safeguard Business and Security Critical Information	0%	0%		0%
7	Be Aware of Industry Security Best Practices.	0%	0%		0%
8	Conduct Licensing & Background Checks for Drivers / Employees / Contractors	0%	0%		0%
9	Develop and Follow Security Training Plan(s)	0%	0%		0%
10	Participates in Security Exercises & Drills	0%	0%		0%
11	Maintain Facility Access Control	0%	0%		0%
12	Implement Strong Physical Security at all Locations	0%	0%		0%
13	Enhance Internal and External Cyber Security	0%	0%		0%
14	Develop a Robust Vehicle Security Program	0%	0%		0%
15	Develop a Solid Cargo/Passenger Security Program.	0%	0%		0%
16	Plan for High Alert Level Contingencies	0%	0%		0%
17	Conduct Regular Security Inspections	0%	0%		0%
18	Have Procedures for Reporting Suspicious Activities	0%	0%		0%
19	Ensure Chain of Custody & Shipment/ Service Verification	0%	0%		0%
20	Pre-plan Emergency Travel Routes.	0%	0%		0%
Overall Implementation:		0%	0%		0%