	HWY-BASE
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.
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	***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.
10.005	This entity has administrative and/or security personnel trained in the National Incident Management System (NIMS) or Incident Command System (ICS).
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 perimeter physical security barriers (fences/gates/walls/planters /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***
13.100	**Developing a Comprehensive Cybersecurity Strategy - Identify**
13.101	Does your agency have a cybersecurity program?
13.102	Does your agency have written and approved cybersecurity policy, plan, process, and supporting procedures?
13.103.00	Do your cybersecurity plans incorporate any of the following approaches/guidance?
13.103.01	National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
13.103.02	NIST 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
13.103.03	NIST 800-82 - Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection
13.103.04	NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
13.103.05	ISO/IEC 27001 - Information Security Management
13.103.06	U.S. Department of Homeland Security Transportation Systems Sector Cybersecurity Framework Implementation Guidance
13.103.07	Industry-specific methodologies (See APTA categories)
13.103.08	Other (if checked elaborate)
13.103.09	None of the above
13.104	Does your agency review, assess, and update as necessary all cybersecurity policies, plans, processes, and supporting procedures at least every 12 months, or when there is a significant organizational or technological change?
13.105.00	Does your organization conduct cyber vulnerability assessments as described in your risk assessment process in the following environments?
13.105.01	OT environment?
13.105.02	IT environment?
13.105.03	None of the above
13.106	Has a written cybersecurity incident response strategy been developed and integrated into the overall cybersecurity program?
13.107	Has your agency taken actions to ensure their supply chain policies, procedures, and processes—include acquisition, receipt, warehouse, inventory control, and distribution—when acquiring vehicles, equipment, goods and services to ensure that cybersecurity risks are addressed?
13.200	**Developing a Comprehensive Cybersecurity Strategy - Protect**
13.201.00	Does your agency have a designated and alternate cybersecurity representative and/or team responsible for the following?
13.201.01	OT environment?
13.201.02	IT environment?

13.201.03	None of the above
13.202.00	Does the agency ensure that recurring cybersecurity training reinforces security roles, responsibilities, and duties of employees at all levels to protect against and recognize cyber threats for the following?
13.202.01	OT environment?
13.202.02	IT environment?
13.202.03	None of the above
13.203.00	Has your agency established and documented policies and procedures for the following?
13.203.01	Access Control
13.203.02	Awareness and Training
13.203.03	Audit and Accountability
13.203.04	Configuration Management/Baseline security controls
13.203.05	Cyber Assett Management and Maintenance/Change Management
13.203.06	Cybersecurity Incident Response
13.203.07	Identification and Authentication
13.203.08	Information Protection
13.203.09	Insider Threat
13.203.10	Media Protection
13.203.11	Patch Management
13.203.12	Personnel Security
13.203.13	Physical Protection (related to cyber systems cyber assets communications)
13.203.14	Recovery (disaster business continuity) plan(s)
13.203.15	Risk Assessment
13.203.16	Security Assessment
13.203.17	Note of the above
13.204	Does the agency prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets by using a multi-factor authentication approach for the identified high-value assets?
13.300	**Developing a Comprehensive Cybersecurity Strategy - Detect**
13.301.00	Has your agency implemented processes to respond to anomalous activity through the following?
13.301.01	Generating alerts and responding to them in a timely manner?
13.301.02	Logging cybersecurity events and reviewing these logs?
13.301.03	Are logs regularly analyzed and maintained for a minimum of 12 months?
13.301.04	None of the above
13.302	Does your agency monitor for unauthorized access or the introduction of malicious code or communications?
13.304	Has your agency established technical or procedural controls for cyber intrusion monitoring and detection?
13.400	**Developing a Comprehensive Cybersecurity Strategy - Respond**
13.401	Has your agency established policies and procedures for cybersecurity incident handling, analysis, and notifications (reporting/alerting), including assignments of specific roles/tasks to individuals and teams?
13.402	Does the organization have procedures in place for reporting incidents through the appropriate channels (i.e. local FBI and CISA cyber incident response office(s)) and also contacting TSA's Transportation Security Operations Center (TSOC) for actual or suspected cyber-attacks that could impact transportation operations?
13.500	**Developing a Comprehensive Cybersecurity Strategy - Recover**
13.501	Has your agency established a plan for the recovery and reconstitution of cyber assets within a time frame to align with the organization's safety and business continuity objectives?
13.502.00	Has the agency developed, separately or as part of another document, recovery plans in the event of a cybersecurity incident for the following?
13.502.01	IT(devices that support communication business enterprise)?
13.502.02	1IT/OT (devices that support the operations and ICS/SCADA environment)?
13.502.03	ICS/SCADA (cyber systems that are used to perform transit operations and management)?
13.502.04	None of the above
13.503	Does your agency review its cyber recovery plan annually and update it as necessary?
13.504	Does the agency document lessons learned and incorporate them into cybersecurity planning and training?
13.505	Does the agency have documented procedures in place to coordinate restoration efforts with internal and external stakeholders (coordination centers, Internet Service Providers, victims, vendors, etc.)?
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 15.101 - 15.103)***
15.101	This entity requires the use of adequate locks on vehicle cargo/ storage areas.
15.102	This entity equips vehicles with a safety/security barrier between the driver and passengers.
15.103	This entity utilizes some type of cargo, baggage or passenger screening system.
15.200	***School Bus Version (Questions 15.201 and 15.203)***
15.201	This entity requires the use of adequate locks on vehicle cargo/ storage areas.
15.203	This entity or the appropriate school board requires the presence of a school official (other than driver) onboard during all extracurricular transports.
15.300	***Trucking Version (Questions 15.301 - 15.303)***
15.301	This entity provides appropriate locks for vehicle cargo doors, valves, and/or hatch openings, and requires their use.
15.302	This entity provides an adequate supply of seals for vehicle cargo doors, valves, and/or hatch openings, and requires their use.
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.).
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.
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 17.101)***
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.
17.200	***School Bus Version (Question 17.201)***
17.201	This entity requires a 'passenger count' be taken any time passengers are allowed to exit and re-enter the bus.
17.300	***Trucking Version (Question 17.301)***

17.301	This entity requires drivers to verify (to the extent possible) that the materials being shipped match the trip manifest/shipping papers.
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 19.101 - 19.102)***
19.101	This entity requires confirmation of arrival upon reaching final destination.
19.102	This entity prohibits the use of alternate drivers without specific entity authorization.
19.200	***School Bus Version (Questions 19.201 - 19.202)***
19.201	This entity requires confirmation upon arrival at final non-school destinations (final drop-offs, field trips, extracurricular activities, etc.)
19.202	This entity prohibits the use of alternate drivers without specific entity authorization.
19.300	***Trucking Version (Questions 19.301 - 19.303)***
19.301	This entity requires confirmation of shipment delivery upon arrival.
19.302	This entity requires that shipments not be subcontracted or turned over to another driver without specific entity authorization.
19.303	This entity requires advance notice to the consignee or point of destination regarding anticipated delivery information.
19.401	This entity requires specific security protocols be followed in the event a trip must be delayed, discontinued, requires multiple days to complete or exceeds hours-of-service regulations.
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.

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.