APPENDIX H: School Transportation Security and Emergency Preparedness

WRITING COMMITTEE EDITS IN RED INK BY SECTION LOCATION:

APPENDIX H: SCHOOL TRANSPORTATION
BEST PRACTICES FOR EMERGENCY MANAGEMENT PLANNING

MANAGEMENT AND ADMINISTRATION

PERSONNEL SECURITY

VEHICLE SECURITY

APPENDIX H: SCHOOL TRANSPORTATION BEST PRACTICES FOR EMERGENCY MANAGEMENT PLANNING

This document contains recommended best practices the Transportation Security Administration (TSA) believes could be useful to public and private School Student Transportation Providers and School Bus Operators to enhance security in each individual district. It is also important for all levels of employees (superintendents, managers, supervisors, administrators, and other frontline employees and those with security-sensitive functions) to be familiar with security practices relevant to their roles and responsibilities (or required by the provider or operator's security plan) and how to implement them.

These best practices have been compiled by TSA's Policy, Plans and Engagement, Highway and Motor Carrier Section, after consultation with individual stakeholders and organizations representing this community, including the National School Transportation Association (NSTA), National Association of Pupil Transportation (NAPT), National Association of State Directors of Pupil Transportation Services (NASDPTS), as well as, other Federal and public security partners. They also reflect information obtained from TSA Baseline Assessment for Security Enhancement (BASE), and the congressionally mandated TSA School Bus Risk Assessment.[1] These practices support the security goals for TSA and this mode identified in DHS sector-specific security plans.

No current federal regulation applies to security provisions within the school transportation industry. The best practices identified in this document are voluntary and are not intended to conflict with or supersede any existing regulatory or statutory requirements. They remain dynamic and subject to revision as experience, continued security partner feedback and the identification of new threats may require. TSA intends to continue to share best practices with school transportation representatives and welcomes ongoing feedback from the industry. To the extent that TSA should develop more official guidance in the future, TSA will consider these ongoing discussions and all received comments as part of those efforts.

TSA highway specialists can be reached by e-mail at HighwaySecurity@tsa.dhs.gov.

The following definitions are applicable to this document:

Critical Assets. TSA understands that the most critical asset in the school transportation business are the student passengers. In this document, however, critical assets also means equipment, facilities, *etc*. managed, owned or operated by School Bus Operators or School Student Transportation Providers that are identified through a Risk Assessment as necessary for the continuity of operation during security incidents.

First Observer Plus™ means the portion of the TSA-recognized security domain awareness training program specific to highway transportation, which is available online at https://www.tsa.gov/for-

[1] This classified document was submitted to Congress in February 2010

industry/firstobserver to providers and school bus operators to enhance provider employee recognition and reporting of suspected security threats.[2].

Security-Sensitive Employee means any employee of a school bus operator or school student transportation provider that performs functions that are connected with, or responsible for, the secure movement of students and/or critical assets. It includes frontline employees such as drivers, security personnel, dispatchers, maintenance and maintenance support personnel.

School Bus Operators or School Student Transportation Providers means public and/or private entities providing home-to-school or school-to-home transportation services for a school or school district.

School Bus Operators or School Student Transportation Provider Employees means both full-time and part-time workers, including contractors, employed by public and/or private entities providing pupil transportation services for a school or school district.

Secure Areas means areas (both physical and virtual) identified, categorized and designated as needing to be protected and thereby restricted from general and public access (access may be limited through implementation of a tiered access control program).

[2] More information is available at https://www.tsa.gov/for-industry/firstobserver.

GENERAL SECURITY

The security recommendations provided below are TSA suggested "Security Options for Consideration" for highway transportation industries to use in an effort to enhance their security posture. These actions are countermeasures designed to minimize vulnerabilities identified during the BASE Review processes. They should be reviewed and considered for incorporation into the district's/company's current security practices.

MANAGEMENT AND ADMINISTRATION

A. Designation of Primary and Alternate Security Coordinators

Designate a qualified employee as a Security Coordinator. The Coordinator would be ultimately responsible for managing the district's/company's security measures. Duties would include coordinating and working with other district/company/agency managers and employees to ensure that security risks are identified and being effectively managed. An Alternate Security Coordinator should also be named to act on security issues in the absence of the primary Security Coordinator. Security duties of the Security Coordinator should be specifically set forth and documented. Both primary and alternate coordinators should be available 24/7/365 for communication with both local administrators and TSA.

B. Conduct A Thorough Vulnerability Assessment

Management should conduct and document a site-specific Vulnerability Assessment for each district/company location. In order for districts/companies to properly address security issues and to develop security mitigation policies, the district/company must first understand what weaknesses (vulnerabilities) it possesses. These vulnerabilities should then be prioritized so that the most critical district/company assets (facilities, vehicles, IT, employees, other) that are necessary for continuation of operations are protected. Funds to correct vulnerabilities should be identified and made available to the extent possible.

C. Develop A Written Security Plan (Security Specific Protocols)

Develop security specific protocols in the form of a Security Plan. The security plan should be reviewed and approved at the management and executive levels. The security plan should be site specific and cover actions to be taken to prevent security breaches, identify who should be notified in the event of a security incident, and how to respond. The security plan should be routinely reviewed (at least once a year) for accurate contact information and current policy updates. Limit access to the security plan to employees with a "need to know". TSA can supply a Security Plan template, if requested.

D. Plan for Continuity of Operations

Establish a written plan to restore operations to any alternate site following an emergency event at their district's/company's primary worksite. Some recommendations to be considered would be the ability to relocate or duplicate important resources and data to allow work from an alternate location and/or an auxiliary power source.

E. Develop a Communications Plan

Management should establish a communication plan to include standard operating procedures (SOP) during normal as well as emergency conditions. The plan should include procedures for communication between drivers, appropriate district/company/agency personnel and law enforcement or emergency responders during a security related incident. Contingencies for the loss of all standard communications should be addressed. This is not intended to preclude the use of personal or issued cell phones.

F. Safeguard Business and Security Critical Information

Procedures for limiting access to district/company/agency internal and external security information should be established. Management should establish policies to secure, control and restrict (need to know) access to sensitive information such as personnel information, unused/blank forms, business information and security policies. Management should implement procedures to maintain accountability for all at-risk assets (cargo, passengers, computers, equipment and vehicles) at all times while in transport or under district/company control. Adequate inventory control measures should be in place that can track shipments, product information, material location, passenger information, and delivery/arrival verification.

G. Be Aware of Industry Security Best Practices and TSA Options for Consideration

Security management should become familiar with and implement security practices recommended by industry groups, trade associations or government transportation entities to further enhance transportation security. The steps outlined in this document are considered "Security Options for Consideration" or “Security Action Items” (SAI).

PERSONNEL SECURITY

A. Conduct Licensing and Background Checks for Drivers/Employees/Contractors

Management should have procedures in place to verify that commercial drivers possess proper commercial driver's licenses with required endorsements for the type of vehicles they operate and passengers they transport. Also verify that drivers possess any other documents required (Health card, TWIC, school bus, etc.).

During the hiring process, an employer should conduct a background check for all employees (both drivers and non-drivers) who have access to district/company vehicles, the facilities, or critical information. These checks generally include criminal history, sex offender registries and motor vehicle records. Background checks should also be required on contracted employees and service providers with unescorted access to district/company facilities, secured areas, or equipment. Appropriate criteria to prohibit a person from becoming employed or continuing employment should be established.

B. Develop and Follow Security Training Plan(s)

General security training for all employees should be conducted, along with additional in-depth security training for personnel having specific security related responsibilities. Districts/Companies should ensure that contracted employees are also trained. Any regulatory requirements for security training should also be met. Refresher training should be conducted not less than every three years. Training should include personnel security, physical security, enroute security, and IT security. Records should be maintained to ensure employees received the proper training and refresher training. TSA recommends all employees view the First Observer Plus^{TM} security awareness video at https://www.tsa.gov/for-industry/firstobserver .

A. Participate in Security Exercises & Drills

In an effort to maintain proper security procedures and correct problems, management should consider security drills and exercises to practice and evaluate security readiness of employees and security procedures. Include outside personnel or agencies (Law Enforcement, Fire Department and/or other First Responders). Include these sources in the evaluation portion of the exercise. These exercises provide a good opportunity to exchange information with first responders and law enforcement about how each other operates. Bus operators can help responders understand how to access vehicle functions or implement evacuation plans. In turn, responders can explain their needs and procedures to make them more effective in emergency events.

FACILITY SECURITY

A. Maintain Facility Access Control

Management should control points of entry to all facilities for both employees and visitors, and should secure all other points of access. District/Company issued photo

IDs or other visible forms of employee identification should be provided to all employees, including drivers. Certain areas within a facility should be designated as "secure" (i.e. dispatch area, computer room, admin areas, etc.) with limited employee access. A safe and secure "challenge procedure" should be established to address unidentified persons. Vendors, contractors, and visitors with unescorted access to restricted areas should be required to follow established security procedures before entry is authorized.

B. Implement Strong Physical Security

Districts/Companies/Facilities should have appropriate physical security measures to prevent unauthorized entry, access, or attack. Consider establishing appropriate physical security measures to protect critical assets as defined in the security plan. Measures may include the following:

- Fencing and barricades
- Video monitoring and intrusion detection alarm systems
- Security Guards
- Delivery control areas
- Adequate locks to control public access
- Security Lighting
- Key Control

C. Enhance Internal and External Cyber Security- Information Technology

Policies and procedures to protect security critical data are important. Strict password requirements and IT security training should be in place. The policy should address current methods for restricting access to data by employees as well as external sources. Information systems should be protected from unauthorized access, tested, and backed up. Awareness of security compromises that originate through social media should also be addressed.

VEHICLE SECURITY

A. Develop a Robust Vehicle Security Program

Policies should be implemented to ensure vehicles are capable of being locked (unless prohibited by law) and are secured when not in service or when parked unattended. The policies should establish a vehicle key control program and secured parking areas. Districts/Companies should also consider enhanced security equipment for vehicles such as GPS tracking systems, on-board cameras, and panic button capabilities. When possible, avoid “single key” purchase where all vehicles use identical keys.

B. Develop a Solid Passenger Security Program

Policies should be implemented to protect passenger or cargo areas. Consideration may be given to implementing and employing additional on-board personnel (school bus or motor coach). Policies should require that drivers and maintenance personnel lock and verify that vehicles are secured when the vehicles are left unattended, while in transport or when out of service.

C. Plan for High Alert Level Contingencies

Establish operational policies that should be implemented during periods of increased threat conditions under the National Threat Advisory System (NTAS). These protocols may include cancelling trips or having vehicles return to the facility; enhancing facility security; initiating enhanced communication protocols; or other actions capable of being implemented when directed by competent government authority or when deemed appropriate by management. Management or security personnel should monitor media or other sources for national or local security threat information that should be shared within the company as warranted.

D. Conduct Regular Security Inspections

Establish a security inspection policy for drivers to conduct security inspections in addition to safety inspections. Security inspections should be performed in conjunction with required pre- and post-trip safety inspections and after any stop in which the vehicle is left unattended. For school buses and motor coaches, passenger ticket verification or passenger count should be required during the boarding and/or re-boarding process.

E. Have Procedures for Reporting Suspicious Activities

Districts/Companies/Facilities should establish reporting policies and procedures for employees (drivers and non-drivers) to follow when they observe suspicious security activities or cargo/passenger anomalies. The procedures should include who is to be notified and require written reports be prepared to maintain accuracy and as much detail as possible.

F. Chain of Custody/Scheduled Service

Policies for scheduling should include pre-planning that establishes an estimated time of arrival (ETA) for pick up drop off times and school buses and motor coaches should be required to confirm and report arrival at their final destination or final trip of the day.

G. Preplanning Emergency Routes

Preplanning routes during normal operations, as well as during heightened alert periods, should be practiced. Travel routes should be evaluated while considering factors such as population, travel distances, threats, condition of highways and roadways, road closures, emergency response capabilities and locations of stops in cities and towns. Consider policies governing operations during periods of heightened alert levels.

The "Security Options for Consideration" shown here are used as the framework for developing the components necessary for an effective Security Plan.

An Overview of the T-START Program

The ***Transportation Security Template and Assessment Review Toolkit (T-START)*** is a compilation of five (5) separate Security Guidance "Modules" prepared by TSA's Surface Division that addresses highway transportation security issues. The five Modules are designed to assist companies in developing effective security practices and in the construction of a *Security Plan*.

A ***Security Plan*** is a written document that sets forth actions to be taken by a given transportation entity to address security related prevention, preparation and recovery issues. While a company may have an overall "corporate" Security Plan that sets company-wide security policies that are to be followed, each company location should also have its own site specific plan, setting forth security practices that are unique to that single location. The five (5) *T-START* Modules are:

Module 1 – Understanding Security Management – Appreciating the value of security and the importance of management endorsement of security protocols are critical. Concerns should range from protecting your company against petty theft to preventing it from being the target of a terrorist attack. Ensuring executive-level support is in place, identifying funding sources, engaging all employees in security practices and identifying who will be responsible for developing and implementing the steps needed to secure your company are all essential tasks.

Module 2 – Understanding Risk - Learning to assess the "Risks" your company may face from possible criminal/terrorist activities by examining and understanding the threats, vulnerabilities and consequences that is a vital step in security planning.

Module 3 – Conducting a Vulnerability Assessment – Completing an assessment of existing security practices and policies to identify potential security weaknesses is important. By using the "Vulnerability Assessment Matrix" provided here, a company can identify and prioritize security weaknesses identified. The vulnerabilities reviewed correlate directly with TSA's "Highway Baseline Assessment for Security Enhancements" (BASE) Program.

Module 4 – *Considering Security Options* – Becoming knowledgeable about the various industry security "Best Practices" or TSA's "Security Options" available to stakeholders in the highway transportation industry, and implementing those deemed appropriate is the critical phase where your company's security practices become operational.

Module 5 – Preparing a Security Plan – Documenting (and maintaining) your security policies, requirements and actions in the form of a "Security Plan" is the final crucial step toward an effective security program. Using the template provided here, or other appropriate source, to record your company's security operations will ensure a strong corporate security posture. (Refer to Module 5 – "Security Plan Template").

Any or all of the five Modules that comprise TSA's ***"****Transportation Security Template and Assessment Review Toolkit" (T-START)* can be referenced for security planning guidance, depending on the needs of the individual company. **To request a complete CD send an email request to highwaysecurity@dhs.gov.**

SAMPLE SECURITY AND PLANNING CHECKLIST

Numbering			Evaluation Criteria	YES	NO
1.			**MANAGEMENT AND OVERSIGHT OF SECURITY PLANS**		
	1.1		Does the school district have a written security policy and crisis response plan including procedures that include transportation personnel, equipment and facilities?		
		1.1.A	What elements does the security plan encompass?		
			Response Plan		
			Emergency Plan		
			Disaster Recovery Plan		
			Other:		
		1.1.B	Does someone review and update the Security Plan?		
			If so, how often?		
			Monthly		
			Quarterly		
			Annually		
			Every three years		
			Every five years		
			As needed		
			Other:		
		1.1.C	Does the student transportation provider/site limit access to the Security Plan to employees with a need to know?		
		1.1.D	Are the plan/policy and procedures communicated to all personnel?		
	1.2		Does the student transportation provider designate a security coordinator?		
		1.2.A	Are the security coordinator's duties documented?		
		1.2.B	Does the student transportation provider exchange unclassified security-related information with industry peers?		
	1.3		Is the security plan site-specific for all school and facility locations?		
	1.4		Does the plan/policy coordinate with procedures in the school buildings?		
	1.5		Does the planning and policy process include appropriate stakeholders (e.g., first responders, law enforcement, fire department and media: print, radio, television, etc.)?		
	1.6		Does the plan/policy provide for any proactive or preventive technology solutions, that are currently available and that can potentially act as early detection or prevention of potential threats?		
	1.7		Is there a plan available that does not require electrical energy?		
	1.8		Does the plan/policy contain directives on incident management and command?		
	1.9		Does the plan/policy include training requirements for school employees?		
	1.10		Does the plan/policy address pre- and post-trip requirements?		
2.			**THREAT ASSESSMENT**		
	2.1		Does the student transportation provider monitor external sources for threat information?		
		2.1.A	If so, what sources?		
			Federal Bureau of Investigation (FBI)		
			Homeland Security Advisory System Threat Level (DHS)		
			Law Enforcement Officer (LEO)		
			News		

			TSA/DHS threat specific information		
			Other:		
	2.2		Does the student transportation provider have a procedure for distributing threat information?		
		2.2.A	If so, is the procedure documented?		
	2.3		Are school bus routes evaluated annually?		
3.			**VULNERABILITY ASSESSMENT**		
	3.1		Does the student transportation provider conduct vulnerability assessments?		
		3.1.A	Where are the vulnerability assessments documented?		
			In the Security Plan		
			Other:		
		3.1.B	If so, how often are they reviewed?		
			Monthly		
			Quarterly		
			Annually		
			Every 3 years		
			Every 5 years		
			As needed		
			Other		
		3.1.C	Do the student transportation provider's vulnerability assessments recommend corrective actions?		
		3.1.D	Does the student transportation provider implement the security measures recommended by its vulnerability assessments?		
	3.2		Is a security coordinator identified for each school and facility?		
	3.3		Do computer and communications systems exist?		
		3.3.A	How is access to computers or systems controlled?		
			What are their limitations?		
		3.3.B	Can the computers be compromised?		
			If so, what can be done to prevent it?		
	3.4		Is the communication system (e.g., two-way radio, land telephone line, cellular telephone, etc.) capable of recording?		
	3.5		Is there a code system to identify emergencies or threats?		
	3.6		Do emergency back-up systems for information and communication exist?		
			If so, what are their limitations?		
		3.6.A	Can emergency back-up systems be compromised?		
			If they can be compromised, what can be done to prevent it?		
		3.6.B	Are the back-up systems stored off site?		
			Are they secure?		
	3.7		Do evacuation plans exist?		
	3.8		Is there a designated place to relocate staff or students?		
4.			**PERSONNEL SECURITY**		
	4.1		Does the student transportation provider conduct background checks?		
		4.1.A	If so, for which employees?		
			Drivers		

			Non-drivers		■
			Management		■
			Contractors		■
		4.1.B	What background information is checked?	■	■
			Driving Records		■
			Criminal Records		■
			Employment History		■
			Employment Eligibility		■
	4.2		Does the student transportation provider have criteria for disqualification for employment based on driving/criminal/employment history checks?		
	4.3		Does the student transportation provider provide identification cards to employees?		
		4.3.A	If so, what technologies do the identification cards incorporate?	■	■
			Photographs		■
			RFID/Proximity		■
			Other:		■
		4.3.B	Does the student transportation provider require employees to display their identification cards while on duty?		
		4.3.C	Does the student transportation provider issue identification cards to contractor personnel?		
	4.4		Is there a “sign in/sign out” system?		
	4.5		Are all employees required to wear uniforms? Do they comply?		
5.			**TRAINING**	■	■
	5.1		Does the student transportation provider conduct security training for new employees? Do they comply?		
		5.1.A	If so, what type?	■	■
			Security Awareness training		■
			Security Plan training		■
	5.2		Does the student transportation provider conduct security training for current employees?		
		5.2.A	If so, when?	■	■
			Annually		■
			Every one-three years		■
			More than three years		■
			Change of job		■
			Other:		■
	5.3		Does the student transportation provider conduct security training based on a formal curriculum?		
			If so, which curriculum?	■	■
			Security Awareness Training CD (DOT)		■
			First Observer (TSA)		■
			School Transportation Security Awareness (TSA)		■
			Secure Transport (TSA)		■
			Security Self-Assessment CD (TSA)		■
			Other:		■
	5.4		Are the student transportation provider’s drivers members of the First Observer program?		
	5.5		Does the student transportation provider maintain employee security training records?		

6.			**PHYSICAL SECURITY COUNTERMEASURES**		
	6.1		Do the student transportation provider’s facilities have physical security barriers?		
		6.1.A	If so, what type?		
			Fencing		
			Locking Gates		
			Keypad/PIN		
			Jersey Wall		
			Bollards		
			Other:		
	6.2		Do the student transportation provider’s facilities have intrusion detection systems?		
		6.2.A	If so, what type?		
			Door/Window Detectors		
			Motion Alarms		
			Siren		
			Silent Alarm		
			Other:		
	6.3		Do the student transportation provider’s facilities have security cameras? If so:		
		6.3.A	Do the security cameras pan/tilt/zoom?		
		6.3.B	How are the security camera feeds monitored?		
			During operation hours		
			24/7		
			Cameras are not monitored		
	6.4		Does the student transportation provider have a key control program?		
		6.4.A	If so, what kind?		
			Facility key control program		
			Vehicle key control program		
		6.4.B	Are keys retrieved from departing employees?		
		6.4.C	Are access codes changed?		
			If so how frequently?		
			Annually		
			Every one-three months		
			Other:		
	6.5		Does the student transportation provider’s facilities have designated secure areas?		
		6.5.A	If so, what kind?		
			Dispatch		
			IT/computer room		
			Admin offices		
			Maintenance		
			Financial		
			Loading dock		
			Warehouse		
			Storage tanks		
			Other:		
		6.5.B	Does the student transportation provider use security measures to protect secure areas?		

			If so, what areas?		
			Keys		
			Keypad/PIN		
			ID cards		
			Guards		
			Other:		
	6.6		Does the student transportation provider record access to secure areas?		
		6.6.A	If so, whose access to secure areas is recorded?		
			Employee access		
			Contractor access		
		6.6.B	Are the access records to secure areas periodically reviewed?		
7.			**ENROUTE SECURITY**		
	7.1		Does the student transportation provider require drivers to conduct pre- and post-trip security inspections?		
	7.2		Does the student transportation provider have measures in place to ensure continuity of operations (including security) during a power/connectivity/facility outage?		
		7.2.A	If so, what measures?		
			Data back-up		
			Uninterruptible power supply		
			Back-up control center Remote access		
			Other:		
	7.3		Are students registered on a particular bus?		
		7.3.A	Do students have passes?		
		7.3.B	Do students have other identification?		
	7.4		Are drivers provided with a list of riders?		
	7.5		Are there procedures for accounting for each individual student, especially on activity trips?		
	7.6		On activity, field or extracurricular or school-chartered bus trips, are students instructed in safe riding practices and on the location and operation of emergency exits?		
		7.6.A	Are students counted at every stop prior to resuming the trip?		
	7.7		Are routes evaluated annually?		
		7.7.A	Are stops evaluated annually?		
		7.7.B	Are bus waiting areas evaluated annually?		
		7.7.C	Are school loading zones evaluated annually?		
8.			**COMMUNICATION**		
	8.1		What lines of communication exist within the operation?		
	8.2		Do they interrelate with local law enforcement, fire and emergency services?		
	8.3		Are they clearly defined and documented?		
	8.4		Are all employees trained and familiar with them?		
	8.5		Have these lines of communication been tested and proven?		
	8.6		Is there an alternate communication plan if the normal systems are unavailable?		
	8.7		Were the communications effective, as tested?		
9.			**SECURITY EXERCISES/DRILLS**		
	9.1		Does the student transportation provider conduct security exercises/drills?		
		9.1.A	If so, how often?		

			Monthly		
			Quarterly		
			Every 6 months		
			Annually		
			Other:		
	9.2		Does the student transportation provider include external personnel or agencies (e.g., law enforcement/first responders) when conducting security exercises/drills?		
	9.3		Does the student transportation provider maintain written documentation of the results/lessons learned from security exercises/drills?		
	9.4		Do the procedures of the plan/policy require routinely conducting security exercises/drills; along with a means for assessment, evaluation and improvement at least annually?		