

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

This document contains 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 Office of Transportation Sector Network Management, Highway and Motor Carrier Division 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 corporate security reviews (CSR), 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.

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 sharing 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.

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™ means the portion of the TSA-recognized security domain awareness training program specific to school bus transportation, which is available 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.

¹ This classified document was submitted to Congress in February 2010..

² More information is available at www.FirstObserver.com.

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

School Bus Operators or School Student Transportation Providers means public and/or private entities providing 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).

School Transportation Security Awareness (STSA) means a TSA-created and distributed training video developed in cooperation with the school transportation organizations to provide security awareness information and training to the school transportation industry.³

General Security

1. **Complete a Vulnerability Assessment** – School Student Transportation Providers and School Bus Operators can enhance security by conducting a comprehensive security vulnerability assessment of their operation. A vulnerability assessment is not a risk assessment.⁴ In conducting a vulnerability assessment, the critical action is to identify gaps in physical or operational security that could be exploited by someone with malicious intent. Identification of vulnerabilities and identification of the consequences of a terrorist attack against critical assets will allow you to construct a security plan that devotes mitigation efforts based on protecting priority assets and to apply good business rules to the dedication of resources for that mitigation.

2. **Develop and Implement a Security Plan** – An effective security plan includes actions that close gaps identified in a vulnerability assessment (either permanently or as necessary in response to threat information) and provide procedures to mitigate the consequences of a security incident. Comprehensive security plans address known vulnerabilities and mitigation strategies through General Security, Personnel Security, Physical Security, En-Route Security and Training and Exercises during normal operations and increased levels of threat. Security plans are most valuable when they are developed and implemented as both district level and site specific plans and include clearly identify incident management chains of command, and designated persons to fill incident management roles.

³The DVD is available online at www.tsa.gov/highway or by ordering the DVD by e-mailing a request to highwaysecurity@dhs.gov.

⁴ A “risk assessment” is developed using an analysis similar to the following: *Threat x Vulnerabilities x Consequence = Risk*. “Threat” is the credible identification of a person or organization with both the intent to do harm intentionally and the capability to carry out that threat. In most cases, accurate threat information is not readily available absent information provided by DHS, local law enforcement or other entities with access to classified information. “Vulnerabilities” requires recognizing the critical assets and then determining whether they are adequately protected. “Consequence,” of course, represents the damage that can be done to critical assets (persons, property, user confidence, etc.).

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

- a. Designate Primary and Secondary Security Coordinators** – As part of the security planning process, designating primary and secondary Security Coordinators for each district and location, where applicable, can ensure immediate and effective coordination with local, state and federal law enforcement and emergency response agencies on security related activities. In addition to documenting Security Coordinator contact information and individual roles and responsibilities in the appropriate security plan(s), whenever possible, current information regarding Security Coordinators and contact information should be provided to appropriate enforcement and emergency response agencies. Because the role of a Security Coordinator may involve receiving information as well as providing it, it is important that the individual(s) be available twenty-four hours a day, seven days a week.
 - b. Establish Interagency Agreements** – Developing (or updating) a security plan is a good time to establish official agreements with appropriate State and local agencies having jurisdictional authority and responsibilities during transportation security incidents. Examples of agencies may include the State and local Department of Transportation (DOT), State and local Department of Education, State and local Office of Homeland Security, State and local law enforcement or emergency response agencies. Agreements may address deployment of resources, use of Public Information Display Systems (PIDS) or variable message signs.
 - c. Integrate the National Incident Management System (NIMS)** – Security planning at the district level is a critical time to ensure familiarity with the National Incident Management System (NIMS) and Incident Command System (ICS) and how this relates to the security plan. These systems enable School Transportation Officials to be prepared to respond and manage a security incident across all jurisdictions and districts. Information on available training can be found at <http://training.fema.gov/>.
- 3. Maintain Awareness of Industry Security Practices** – As part of overall security efforts, it is important to maintain familiarity and awareness with appropriate and applicable security practices recommended by industry groups, associations or other related public or private entities, as well as maintaining the ability to adapt and incorporate new best practices and recommendations.
 - 4. Protect Business and Security Critical Information** – A comprehensive plan includes protecting both physical assets and critical information; policies and procedures need to protect physical assets and virtual information from unauthorized access. This includes sensitive information shared between school administrators, frontline employees, and appropriate Federal, local and state law enforcement and emergency response personnel. In addition to protecting hard copies of such information in designated and secure areas with limited access, Information Technology (IT) systems should always have protective measures in place (passwords, firewalls, secure areas, *etc.*) to limit access to those with a need to know.

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

Personnel Security

5. **Require Background Checks for Employees** – The Provider or Operators should clearly state in its employment policy the offenses that will disqualify an applicant from employment. TSA is aware many schools conduct background checks for prospective transportation employees and for administrative positions that may deal directly with transportation providers. These checks generally include criminal history, sex offender registries, motor vehicle records, verification of social security numbers, and verification of immigration status. No commercially-available background check, however, has access to the FBI's Terrorist Screening Database (TSDB). If your system uses the FBI's criminal history records check (CHRC), your applicant may be screened for possible affiliations with known terrorist groups. The FBI cannot, however, make this information available to those persons requesting the CHRC. TSA currently checks drivers against the TSDB only if they apply for hazardous materials endorsements on their commercial driver's license or a Transportation Worker's Identification Credential (TWIC). To learn more about either program, go to www.TSA.gov. Providers and Operators should consider a method of redress for adversely affected applicants and personnel, including an appeal and waiver process similar to the system established for holders of a commercial drivers license and transportation workers at ports (see 49 CFR Part 1515). Providers and Operators should consider routing Criminal history records checks through the FBI to allow a check against the TSDB.

Physical Security

6. **Enforce Employee Access Control Systems** - Access control systems, such as those requiring photo identification cards (IDs) or other visible forms of identification to all employees associated with transportation operations, enhance security. In addition to verifying employment (and who should or should not be anywhere on the premises), these IDs can be used to restrict access to designated secure areas (such as facilities, vehicle key control room, *etc.*). To the extent that IDs are issued, their usefulness is dependent on a requirement that they be conspicuously displayed by the holder at all times (a requirement that could be incorporated into a security plan). Photo ID's are especially useful to drivers or others whose duties place them in contact with the public to represent a bona fide employee of the provider. With such procedures, passengers, parents or others who have repeated contact with vehicle operators can be advised to challenge operators who cannot or do not display this ID. Similarly, more employees are then able to enhance security because they are better equipped to challenge individuals who do not display the appropriate identification.
7. **Establish Facility Security Measures** – There are many physical security measures available to School Student Transportation Providers and School Bus Operators that are appropriate for mitigating vulnerabilities identified for critical assets, as defined in the security plan. Measures may include the following:
- Secure area monitoring

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

- Closed-circuit television (CCTV)
- Intrusion detection systems
- Fencing, additional lighting
- Gates
- Keypad or other access control technologies
- Jersey walls, barriers, or bollards
- Security Personnel (*e.g.*, guards)
- Other appropriate security systems and measures when assets are remotely located

En-Route Security

- 8. Establish Appropriate Vehicle Security Program** – Security depends on efforts to ensure all school transportation vehicles (including but not limited to school buses, maintenance vehicles, *etc.*) are secured when unattended. Security methods include:
- Ensuring all unattended vehicles are locked if they have the capability to be locked or are subject to thorough pre- and post-trip security inspections.
 - Adopting a written policy that includes:
 - Procedures such as a key control program when a vehicle is not in active use,
 - Ensuring the vehicle engine is turned off, keys are removed from the vehicle, and windows are closed.
 - Appropriate pre- and post-event reporting for diversions from normal routing.
 - Incorporating other appropriate lockout control methods.
- 9. Establish Security Inspection Policy and Procedures** – School Student Transportation Providers and School Bus Operators should consider establishing a security inspection policy and procedures for drivers to conduct security inspections. Just as the safety inspections required by 49 CFR Part 392 or State and local policies must be completed before operating a vehicle, it is important to conduct a security inspection at the beginning of the driver’s shift or trip (pre-departure) and after any stop en-route in which the vehicle is left unattended. A complete security inspection not only checks to determine if there has been any unauthorized access, it includes inspecting all areas where a suspicious item could be affixed to or placed in a vehicle.
- 10. Planning Alternate Emergency Routes** – Providers and operators should consider implementing and communicating emergency routing protocols for drivers to follow when determined to be necessary by the driver, administrators or other officials. Pre-planning alternate emergency routes can help drivers avoid or minimize proximity to highly populated urban areas or critical infrastructure such as bridges, tunnels, and dams during an emergency situation. When incorporated into the security plan, the alternate route information can include procedures for drivers to notify administrators or appropriate officials when substantial or non-routine deviations from the scheduled route is necessary and allow administrators or appropriate officials to know where the bus may be located or heading if the driver is not able to provide complete information.

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

- 11. Developing Protocols for Increased Alert Levels** – School Student Transportation Providers and School Bus Operators should consider establishing policies governing operations during periods of increased threat conditions, such as if DHS provides information regarding increased threat levels for the school transportation industry). Developing protocols in advance, providing them to appropriate by administrators, law enforcement or other appropriate officials, and documenting them in the appropriate security plans will enable a more rapid, coordinated and effective response if and when the alert levels are increased.
- 12. Establish Emergency Communications Plan** – Emergency communications plans include procedures for communication between drivers, school administrators, and law enforcement or emergency responders during a security related incident accompanied by a meaningful course of instruction to both drivers and dispatchers on the protocol and use of key words or coded verbal commands. Plans include the appropriate methods of two-way communication technologies required to implement the plan, such as land-based or satellite-based systems. Incorporation of this best practice is not intended to support or preclude the use of personal or issued cell phones; providers and operators should encourage and drivers should follow the proper use of cell phones including observing State, Federal and local cell phone laws including those that may involve messaging, texting or other uses.
- 13. Establish Reporting Policy and Procedures** – Responses are more effective when there are clear procedures implemented for drivers and non-driver employees to follow when reporting suspicious incidents, threats, persons, or other security concerns to administrators, School Bus First Observer™ (888-217-5902), or the TSA Transportation Security Operation Center-TSOC (Freedom Center, 866-615-5150) regarding school vehicles or facilities. Effective procedures include appropriate points of contact and information details to be communicated and are documented in the Provider’s and Operator’s security plan.
- 14. Use School Bus Tracking Systems** – Recognizing it may not be possible for a driver to report when they are being hijacked or the bus has been stolen, commercially off-the-shelf (COTS) methods of tracking the school bus or other vehicles can increase security throughout the scheduled route with a land-based or satellite-based Global Positioning System (GPS). If incorporating such systems, features for consideration include ensuring the system can provide:
 - Longitude and latitude
 - Geofencing
 - Real-time/scheduled updating route monitoring
 - Status reporting
 - Route exceptions
 - Unauthorized use of the vehicle.
- 15. Use School Bus Video (surveillance) Cameras** – Security (surveillance) cameras that provide a method to monitor activities while school buses are in operation, such as live

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

video feeds or digital video recorders (DVR). If this technology is used, policies and procedures should be established and communicated to affected personnel or persons as appropriate.

16. **Use Panic Button Capability** – Commercially off-the-shelf (COTS) systems are available for a driver to transmit an emergency alert notification while en-route. This panic button capability enables a driver to remotely send an emergency alert notification message via land-based or satellite-based communication systems, and can utilize a vehicle disabling feature if available. In lieu of electronic or mechanical trouble indicators, providers and operators could implement a capability for drivers to display a distress signal (trouble lights, signs, flags, etc.) capable of alerting observers in the immediate and surrounding area. Use of such trouble indicators should be accompanied by employee and community familiarization campaigns to explain the meaning of the indicators and guide observers to respond appropriately.

Training and Exercises

17. **Establish Security Training** – In addition to providing general security awareness training to all employees, it is valuable to provide training to employees with security-sensitive functions on the aspects of these best practices incorporated into the Student Transportation Provider's or School Bus Operator's security program, including those related to General Security, Personnel Security, Physical Security, En-Route Security, and Training and Exercises security action items. There are many resources and tools available to assist providers and operators in the training of employees, including TSA's School Bus Counterterrorism Guide, the School Transportation Security Awareness DVD, and the TSA sponsored domain awareness training (First Observer™ program (<http://firstobserver.com/>)).⁵ In addition, incorporating training for those responsible for implementing the security training plan will not only provide an opportunity for providers and operators to educate employees regarding their security goals and objectives, but it enables each employee in a security-sensitive function to be aware of their individual roles and responsibilities in identifying, preventing, protecting and responding to a security incident. Training should prepare drivers for incidents ranging from armed or hostile intruders to shots fired at a bus or threats of violence.
18. **Coordinated Security Exercises and Drills** – Coordinating security exercises and drills with other school transportation providers and operators, state and local law enforcement and emergency response agencies, and other appropriate federal officials provides a meaningful training opportunity, method for testing effectiveness of security programs, and can identify vulnerabilities. Security exercises conducted periodically as a discussion-based tabletop exercises can identify strengths, weaknesses, disconnects and security gaps by focusing on the security plan and the appropriate countermeasures and mitigation strategies to be implemented during a heightened level of security or a transportation security incident. Such exercises and drills can have significant benefits to

⁵ Additional information can be found by visiting the TSA website at www.tsa.gov/highway.

**Description of Best Practices for
School Transportation**
Not for Public Dissemination

the extent they include requirements for after-action reports, communication of lessons-learned, and implementation of security improvement efforts based on exercise results.

Summary – These voluntary best practices are not all inclusive but provide a starting point for School Student Transportation Providers and School Bus Operators to consider when conducting security planning. School transportation officials should continue to coordinate with State and local security officials and incorporate the appropriate best practices that fit their operation.

For more information regarding security planning or security training resources, please visit the TSA web site at www.tsa.gov/highway or you may contact TSA by sending an email to highwaysecurity@dhs.gov.