Security Sensitive Information

Transportation Security Administration
Office of Security Policy & Industry Engagement
Surface Division
Highway & Motor Carrier Branch

T-START

Transportation Security Template and Assessment Review Toolkit

A Security Awareness Guide

October 2013

Security Sensitive Information

Table of Contents

An Overview of the T-START Tool Kit

The ***"Transportation Security Template and Assessment Review Toolkit (T-START)"*** is a **Security Awareness Guide** composed of five (5) separate Security Guidance "Modules" (numbered 1 thru 5) prepared by TSA's Highway & Motor Carrier Branch, that addresses highway transportation security issues. The five Modules are designed to assist companies/ operators in developing effective security practices and in the construction of a *Security Plan*. This plan also has application to political subdivisions or governmental entities having ownership or control over large scale motorcoach, trucking, or student transportation operations. The term "company" also refers to those governmental entities.

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* Security Awareness Guide 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. (Refer to Module 1 – "Understanding Security Management")

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 are vital to effective 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 Self-Assessment Tool," provided as a separate Microsoft Excel™ file attached to this guide, a company can identify and prioritize security weaknesses identified. The security practices reviewed correlate directly with TSA's "Highway Baseline Assessment for Security Enhancements" (Highway BASE) Program. (Refer to attached Microsoft Excel™ "VSAT" File).

Module 4 – *Considering Security Options* – Becoming knowledgeable about 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 guidance and template provided here, or other appropriate source, to record your company's security operations will ensure a strong corporate security posture. (Refer to attached Microsoft Word™ file – "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.

Module 1 – Understanding Security Management

Introduction to Security Management

Security has likely been a concern since the beginning of time. The practice of "crime prevention" has been promoted by police departments for decades, if not centuries. The idea of protecting one's property and one's self has undoubtedly been on the minds of everyone at some point during their lifetime. But the events of September 11, 2001, the attacks that led up to that day, and the world's ever-evolving political climate have forced us to view self-protection and personal security from a different perspective. Security should now be an important, though not all consuming, consideration.

The 9/11 attacks were a campaign of violence against Americans. The terrorists proved they had the intent and capability to cause mass casualties on American soil. Prior heinous terrorist incidents in the U.S such as the bombings at the World Trade Center in 1993 and the Oklahoma City Federal Building in 1995 caused an increased awareness of terrorism, but did not bring about the significant sea-change that resulted from 9/11. After that day security moved more to the forefront in our everyday lives. The attacks against the World Trade Center buildings and the Pentagon and the foiled attempt involving Flight 93 in Pennsylvania marked a tragic and unforgettable day in United States history. The terrorists were successful in causing many fatalities, great economic loss and a lasting wave of fear and concern throughout the nation.

The unexpected and vicious use of commercial airplanes under the control of terrorists raised a new realization of the ability of those who want to maim and kill Americans. This new threat was identified and resulted in the need for organizations to develop security plans designed to protect their facilities, personnel and other assets.

As our memories of 9/11 fade, and those who may do us harm hide behind the cloak of time, there is an even greater need to stay focused and vigilant to protect our country's assets, including its highways and infrastructure. Dozens of plots involving transportation assets have been disrupted since 9/11, ranging from threats targeting highway infrastructure to the use of

vehicles to further terrorist acts. Thanks to the good work of law enforcement officials and the raised consciousness of American citizens, these attacks have largely been unsuccessful. Business and industry, however, must remain ever watchful in preventing, recognizing and reporting potential terrorist activities. Only through proper understanding of the potential threats that exist, planning contingencies to deal with those threats, and providing security training to our workforce can vigilance continue to succeed.

The Transportation Security Administration (TSA) is tasked with protecting the Nation's transportation systems while ensuring freedom of movement for people and commerce. TSA seeks to ensure that no matter what terrorist actions may transpire, the U.S. will be able to maintain a functioning national transportation network.

The ***"Transportation Security Template and Assessment Review Toolkit" (T-START)*** is intended to stimulate thinking and offer helpful ideas for developing a strong Security Plan. It is a resource designed to support TSA's ***Highway Baseline Assessment for Security Enhancement (Highway BASE)*** **Program.** It is not the singular resource for security planning. Other laudable products and resources are available for stakeholders to use. This resource is offered by TSA to introduce uniformity in security practices across all transportation assets. The options offered here are voluntary on the part of stakeholders. If a company so chooses, it may adopt or modify any of the security options offered to fit the company's unique situation. It is an adaptable guide for transportation entities to use as an outline for implementing or updating their security strategy. Your Security Plan should serve as a single-source working document for effectively addressing any transportation security issue that may arise.

Security Endorsement at the Executive Level

Security is a concept that can only be effective if it is top-down driven. Company officials at the executive level must support the idea that strong security is beneficial to overall corporate health and the return is worth the investment. Generally the companies that are identified for inclusion in the Highway BASE program, and are the intended audience of the T-START security guidance, are "for-profit" companies rather than public enterprises. Cost-benefit ratios should be considered, but the realization that a single significant terrorist/criminal incident can have significant consequences should not be minimized. The bottom line is always important, but for sustained survival, companies should be cognizant of the long term positive effects strong security can bring.

Understandably, funding for security is historically found fairly far down on a company's list of priorities. Security at the expense of other important company needs is not the message here. But the need to provide necessary funding to address security weaknesses, particularly those

identified as "high priority," should be given fair consideration when budgetary matters are discussed.

Effective security management also includes ensuring that all employees are engaged somewhere along the security continuum, whether by simply receiving general security awareness training, taking on additional leadership duties during a security incident, or assuming duties as critical as security coordinator or assistant coordinator. The leadership message that "security is the responsibility of all employees" is a message management should clearly communicate to everyone.

Designating a Security Coordinator

A company's security program is only as good as the people responsible for developing and implementing it. Identifying a qualified individual to be responsible for bringing the necessary security measures to bear at your company is the first step toward security success. Identifying an individual who is qualified (or can be trained) to function as the Security Coordinator is an essential first move for the company's chief executive to take. Identifying an Alternate Security Coordinator to act in the Security Coordinator's absence is also important.

Dedicating a person full time to handle security related duties is ideal, but that may not be realistic for all situations. The size of the company is certainly a factor, and in a small operation the CEO may also be the Security Coordinator. A company's operation may require that the title of Security Coordinator or Alternate Security Coordinator be a shared position with other duties or other titles. Ensuring that security is given its due diligence and essential security functions are performed should be management's goal in identifying a Security Coordinator.

Module 2 - Understanding Risk

Introduction to Risk

When reviewing company operations, one of the most important steps is the assessment of possible transportation security risks a company may face. Ask yourself, "What, if anything, is it about my company that could attract the interests of a potential terrorist/criminal?" Most companies have certain "assets" that could be either the target of a terrorist attack or the means toward attacking another target. The nearly unrestricted movement of trucks and buses in America pose a unique security challenge to our country. Additionally, assets that are absolutely essential or "critical" to a company's ability to operate should be identified and secured to the extent possible to ensure the company remains operational at all times. These may include, but are not limited to, personnel, vehicles, and facilities. When assessing risk, it is important to look at the threats against company assets, the vulnerabilities associated with those threats, and the consequences of an attack against those assets.

The methodology used by the Department of Homeland Security (DHS) and TSA to determine the level of risk in all critical U.S sectors, including transportation, is a complicated scenario-based analysis that mathematically computes the level of risk for each sector. In scientific notation, the DHS model for risk is: "Risk (R) equals (=) Threat (T) x Vulnerability (V) x Consequence (C), or R=TVC."

But risk can be explained in a much more simplistic form. For example, the thief, vandal, or terrorist that may target your business represents the "threat" you may be facing. "Mother nature" may also be viewed as a threat. An open window, unlocked vehicle or unprotected computer represents a "vulnerability" your company may have. And the damages, theft or injuries that result from an exploited vulnerability are the "consequences."

Risk is the combination of all three of these components; threat, vulnerability and consequence. The absence of any one eliminates the risk. Unfortunately, while the vulnerability of an open window may be obvious and easily corrected, the threat that lurks outside is very difficult to identify or predict with any certainty. For even the most well established "intelligence" agencies, identifying the presence of a terrorist threat, or determining that none exists, is an extreme challenge. Asking a business to independently determine if they may be targeted for a terrorist attack is an unrealistic expectation.

As part of its mission, DHS (the Department under which TSA falls) has taken on the difficult task of assessing the general level of threat across all transportation modes. After lengthy and arduous analyses of all available risk information regarding threats to the highway transportation sector, DHS has determined that the current (2013) terrorist threat level associated with highway transportation is "low." Any change in that determination would result in an immediate widespread notification to the highway sector. DHS will change the threat level only if: 1) credible threat information of an imminent attack is received, or; 2) an actual attack has occurred.

As of October 2013 DHS has determined that the threat level associated with highway transportation is

While the risk of a terrorist attack within the transportation sector is low, the recognition by stakeholders that some risk does exist, and an appreciation for the tenants of effective security planning, are the goals of this document. TSA understands that security is one of the many components that go into making an entrepreneurial success. Businesses should be ever mindful of events both domestically and internationally that can affect their operations. Monitoring the news, being aware of any changes to the DHS National Threat Advisory System (NTAS) and reviewing informational "alerts" provided by TSA and other government agencies that are specific to transportation should be standard procedures for all transportation stakeholders. Additionally, protecting your business from more traditional known "criminal elements" (as is discussed later) must also be a consideration in security planning. Uncovering and assessing the likelihood of a terrorist attack being launched against any sector, including highway transportation, can originate authoritatively only from intelligence professionals. Businesses, therefore, should routinely monitor news sources and heed government notices regarding terrorist activities, but they should focus their day-to-day security energies toward identifying local threats they may face, reducing their vulnerabilities and minimizing potential consequences.

Examining the Three Components of "Risk"

As previously stated, the process of understanding and assessing the "risk" that a company may be facing from possible terrorist (or other criminal) activity requires an evaluation of the three components that constitute RISK: *Threat, Vulnerability and Consequence*.

Assessing "Threats"

While the threat of a terrorist attack against an individual company is low, some level of threat will always exist. While the possibility of having a vehicle hijacked, a facility broken into, or a company's information compromised by persons identified as "terrorists" does exist, your company

is statistically more likely to be targeted by more "traditional" criminal elements such as theft, vandalism, or burglary. Individual companies are likely aware of conditions they face that put them at risk from non-terrorist influences such as location, high crime rates, deteriorating neighborhoods, or poverty. While TSA focuses exclusively on the prevention of terrorist attacks to the transportation sector, common sense dictates that a company that guards against traditional criminal activity will likely reduce the potential success of an attempted terrorist attack as well. Conversely, implementing strong mitigation strategies to deter terrorism can only reduce the likelihood of a successful traditional criminal attack. Reducing vulnerabilities, regardless of the company's motivation, can only be a win for both the company and the country.

Assessing "Vulnerabilities"

In the context of this T-START document, vulnerabilities are defined as weaknesses in a company's security operation. This Tool looks at vulnerabilities across four (4) broad Categories: Management & Accountability; Facility Security; Personnel Security; and Vehicle Security. TSA/HMC has established twenty (20) "Security Action Items" (SAIs) that are general security measures all transportation entities should evaluate and consider for adoption. Failure to effectively employ any of these twenty security practices may be indicative of a security weakness or vulnerability.

To evaluate and prioritize security weaknesses a company may have, TSA/HMC has also developed a **"Vulnerability Self-Assessment Tool"** (VSAT) using the 20 SAIs. The Vulnerability Self-Assessment Tool lists the 20 SAIs, identifies "Components" specific to each SAI, and establishes a "standard" for each Component. Again, the Vulnerability Self-Assessment Tool follows a process nearly identical to that used during the voluntary **Highway BASE** review process. In short, the Vulnerability Self-Assessment Tool identifies the various security actions a company may take, defines the standard procedures for each action, and asks if these procedures are in place. If the action or procedure is not effectively employed, a security vulnerability is identified.

All vulnerabilities are then identified by TSA as being a "High Priority," "Medium Priority," or "Low Priority" for corrective action. High Priority vulnerabilities should be addressed as quickly as possible, while correcting Medium and Low priority vulnerabilities may be delayed.

Module 3 – "Conducting a Vulnerability Assessment," provides additional information regarding vulnerability identification and actions that can be taken to mitigate them. Most of the security practices shown are applicable to all highway transportation sub-sectors (truck, motorcoach, school bus), while others are modified to be sub-sector specific. Scoring the Vulnerability Self-Assessment Tool as directed can help identify security weaknesses and prioritize your needed security enhancements.

Assessing "Consequences"

Consequences are the final variable to be addressed in determining risk. Consequences are the results associated with exploited vulnerabilities. Consequences can be unique to each company and each security incident. Mathematically determining the direct and indirect consequences associated with a specific security incident can be a complicated process requiring extensive time and calculations. Consequences can be defined as either quantitative or qualitative, and can be direct or indirect.

Understanding consequences from a non-mathematical, general perspective is likely sufficient for a company when developing an effective Security Plan. The consequences a company may suffer as the result of a security incident can be significant, possibly even catastrophic. Employee injuries (or deaths), loss of revenue, loss of resources, or loss of reputation are just some of the setbacks a company could have to endure. Any company can potentially attract the interest of terrorists or criminal elements. Ignoring vulnerabilities or underestimating the lengths to which an advisory may resort can be dangerous; as is the mindset "it can never happen here." A company must be aware of the potential consequences its operation may face from a terrorist event and must act accordingly in reducing vulnerabilities. Companies that may be especially appealing to criminal or terrorist elements because of certain high value assets they have (i.e.; facilities, products, vehicles, cargo, passengers, information) or because of their proximity to targets of interest, must be especially vigilant.

While the consequences to the company itself are of major concern, impact that reaches beyond the walls of the company and affects the neighborhood, the region, or the nation should also be recognized by the company's leadership. These may all be factors that make a company more "attractive" to potential terrorists. The consequences of a security event can expand quickly and potentially have far reaching impact. Companies should be aware of their unique assets and situations and develop their Security Plans accordingly.

Prioritizing "Critical Needs"

After completing the Vulnerability Self-Assessment Tool each company should better understand the extent of their vulnerabilities and the recommended priority for taking corrective actions. Determining if, when, and where to provide resources for enhancing security is a business decision that hopefully can be more easily made based on this vulnerability assessment process. Using this methodology is an essential step in the allocation of security funds as well as in disaster recovery and contingency planning. The overarching goal is to use available resources to reduce vulnerabilities deemed most critical and, in turn, drive down risk. Plans should be developed to direct resources to the most important operations first. Prioritizing and mitigating vulnerabilities can only enhance a company's security posture, improve their Highway BASE score, and reduce risk correspondingly.

Security Sensitive Information

Module 3 – Conducting a Vulnerability Assessment

The Need for a Vulnerability Assessment

A critical part of developing a valid security plan is determining what security vulnerabilities your company has. The T-START Tool Kit provides all companies, regardless of size, with the ability to conduct a free, comprehensive assessment of their security posture by using the "Vulnerability Self-Assessment Tool" (VSAT), provided here as a separately attached Excel file. The Vulnerability Self-Assessment Tool provided evaluates the security practices a company has in place against a list of specific security standards that are available. A qualified company representative (Security Director/Safety Manager/General Manager, etc.) is asked to objectively determine if these practices are being employed. The Vulnerability Self-Assessment Tool further seeks to prioritize the importance of correcting any security weaknesses found. The security practices are examined from a "self-assessment" perspective, and are identical to the security issues addressed and evaluated during the voluntary **Highway Baseline Assessment for Security Enhancement (BASE)** review process conducted by TSA field personnel.

The person(s) conducting the Vulnerability Self-Assessment should be familiar with all security operations of the company being assessed. Responses provided for each security component should be answered in an honest, unbiased manor. The answers should reflect the assessor's informed opinion as it relates to the company's level of security.

This Vulnerability Self-Assessment is for internal company use with no expectation that it be disclosed beyond the corporate need-to-know. The results generated from the Vulnerability Self-Assessment should be handled as Security Sensitive Information (SSI), subject to all applicable federal disclosure requirements governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

NOTE: Conducting a valid Vulnerability Assessment is an essential process for all transportation companies. The Vulnerability Self-Assessment Tool (VSAT) provided here is designed for companies that are self-assessing their security vulnerability level. Companies actively participating in a **Highway BASE Review** conducted by a TSA Surface Inspector will be provided with a Vulnerability Assessment as part of the "Executive Summary" report provided by TSA.

The "Vulnerability Self-Assessment Tool" (VSAT) starts by identifying the four (4) main categories into which all security practices can be divided: Management & Accountability; Personnel Security; Facility Security; and Vehicle Security. The VSAT then presents a comprehensive list of 20 general

security practices or "**Security Action Items" (SAIs)** that a company may or may not be employing to some degree. Each SAI then has several sub-parts or "Components" listed that identify the specific actions that collectively comprise the broader SAI. The acceptable level of proficiency or implementation for each SAI Component is then defined as the "SAI Component Standard."

Below is an excerpt of SAI #1- *"Have a Designated Security Coordinator"* - from the Vulnerability Self-Assessment Tool. The sample shows SAI#1 (Column A), the "SAI Components" that identify the specific actions that make up that SAI (Column C), and then provides the accompanying "Component Standard" (Column D) that further explains the security practice being examined.

Company Name			Person Conducting Assessment	Date Conducted
Your Bus Or Truck Company			John Doe	6/20/2014
Mode: Trucking				
Column A	Col B	Column C	Column D	Column E
SECURITY ACTION ITEMS (SAI'S)	SAI Component #	SAI COMPONENT	SAI COMPONENT STANDARD	Does your company or facility fully meet this standard? *(Yes, No, N/A)*
Management and Accountability Section				
SAI #1		SAI Component	SAI Component Standard	
SAI #1 – Have a Designated Security Coordinator	1	This entity designates a qualified primary Security Coordinator.	A qualified individual with this title must be identified (may be a shared title). PL 110, Sec. 1531 states "Qualified" means a citizen of the United States (unless waived by DHS). Recommended to also have law enforcement, private security, or appropriate military background; or adequate on-the-job experience.	Yes
	2	This entity designates an alternate Security Coordinator.	A qualified individual with this title must be identified (may be a shared title).	No
	3	This entity has policies that specify the transportation related duties of the Security Coordinator.	Should have documented specific transportation security related duties of Security Coordinator. May be found in job description, security plan, or other documents as appropriate. PL 110, Sec. 1531 states Security Coordinator duties include: Implement security actions under the security plan; coordinate security improvements; receive communications from appropriate federal officials.	No
SAI #2		SAI Component	SAI Component Standard	

In column E, for each SAI Component shown, the company representative completing the VSAT is asked to provide a "Yes/No" response to the question:

- **Does your company or facility meet the SAI Component Standard shown?**

If the answer is "no" because your company does not adequately meet the SAI Component Standard shown, the response "No" would be selected from the drop-down options available. Each "No" response indicates that a vulnerability has been identified. A TSA-assigned "Level of Priority" for each vulnerability will then be shown on the "Summary Sheet" tab. Vulnerabilities are identified as either "High," "Medium," or "Low." High Priority vulnerabilities should be addressed as quickly as possible, while Medium and Low Priority vulnerabilities may warrant a less immediate corrective response.

Results Produced by the T-START Vulnerability Self-Assessment Tool

When using the Microsoft Excel™ version of the VSAT, once all of the SAI Components have been reviewed and assessed, a summary of findings is provided on the "Summary Sheet." Only SAI Component Standards that are not being met need to be addressed, corrected or improved. On the Summary Sheet, all SAI components are automatically grouped by their Priority Level and appear together. The Summary Sheet allows the reviewer to see all similarly important SAI components together, with all vulnerabilities readily seen. The Summary Sheet provides a prioritized list of actions that can be taken to improve security. Consistent with business needs and financial constraints, "High Priority" weaknesses should be addressed first to the extent possible, while "Medium" and "Low" priorities" would be next tackled in descending order.

The Vulnerability Self-Assessment Tool (VSAT) is provided in a separate Microsoft Excel File as "T-START Component #2" of the T-START Tool Kit. The Microsoft Excel VSAT product will soon be available for download from the TSA website (www.TSA/Highway/VSAT). Companies wanting more immediate access to the VSAT Excel file should contact their local TSA Surface Inspector or send an E-mail to HighwaySecurity@DHS.gov requesting the file.

Module 4 – Security Options for Consideration

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 VSAT or BASE Review processes. They should be reviewed and considered for incorporation into the company's current security practices.

Management and Administration

1. Designation of Primary and Alternate Security Coordinators

Designate a qualified employee as a *Security Coordinator/Coordinator*. The Coordinator would be ultimately responsible for managing the company's security measures. Duties would include coordinating and working with the other company/agency managers and employees to ensure that security risks are 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.

2. Conduct A Thorough Vulnerability Assessment

Management should conduct and document a site specific Vulnerability Assessment for each company location. In order for companies to properly address security issues and to develop security mitigation policies, the company must first understand what weaknesses (**vulnerabilities**) it possesses. These vulnerabilities should then be prioritized so that the most critical 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.

3. 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". See Section V – "Security Plan Template" below.

4. Plan for Continuity of Operations

Establish a written plan to restore operations to any site following an emergency event. Some recommendations to be considered would be the ability to relocate and work from to an alternate work site and/or an auxiliary power source.

5. 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 company/agency personnel and law enforcement or emergency responders during a security related incident. Contingencies for the loss of all communications should be addressed. This is not intended to preclude the use of personal or issued cell phones.

6. Safeguard Business and Security Critical Information

Procedures for limiting access to 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 company control. Adequate inventory control measures should be in place that can track shipments, product information, material location, passenger information, and delivery/arrival verification.

7. 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."

<u>Personnel Security</u>

8. 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 the freight or 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 company vehicles, the facilities, or critical information. These checks generally include criminal history, sex offender registries, motor vehicle records, verification of social security numbers, and verification of immigration status.

Background checks should also be required on contracted employees and service providers with unescorted access to company facilities, secured areas, or equipment. Appropriate criteria to prohibit a person from becoming employed or continuing employment should be established.

9. 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. 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, en-route security, and IT security. Records should be maintained to ensure employees received the proper training and refresher training.

10. 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.

Facility Security

11. 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. 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.

12. Implement Strong Physical Security

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

13. Enhance Internal and External Cyber Security- Information Technology

Policies and procedures to protect security critical date 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

14. 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. Companies should also consider enhanced security equipment for vehicles such as GPS tracking systems, on-board cameras, and panic button capabilities.

15. Develop a Solid Cargo/Passenger Security Program

Policies should be implemented to protect passenger or cargo areas. Consideration may be given to implementing a seal/lock program (for trucking), screening/ticketing passengers (for motorcoach, where appropriate) or employing additional on-board personnel (motorcoach or school bus). 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.

16. 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.

17. 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 motorcoaches and school buses, passenger ticket verification or passenger count should be required during the boarding and/or re-boarding process.

18. Have Procedures for Reporting Suspicious Activities

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.

19. Chain of Custody/Scheduled Service

Policies for scheduling trucked shipments of cargo should include pre-planning that establishes an estimated time of arrival (ETA) for pick up and deliver of cargo, the load specifics and driver identification information. Motorcoaches and school buses should be required to confirm and report arrival at their final destination or final trip of the day.

20. 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 (Refer to Module 5 – "Security Plan Template").

Security Sensitive Information

Module 5 – Developing a Security Plan

A "Security Plan" can be referred to as the Standard Operating Procedures for your company's security practices, a written "war plan" to address any security contingency that may arise, or your company's security reference manual. The Security Plan should be a written document, or series of documents, that should be thoughtfully prepared and updated regularly. The "Security Plan Template" provided here is a guide that can be adapted to fit the needs of your company. The template provided is broad in scope and is generally comprehensive, but it is not the only source available for stakeholders to use. The template here identifies many areas that should be considered for inclusion in your company's plan, though some may be deemed not applicable. The document is provided in Microsoft "Word" format for ease of use.

See the additional file "TSTART Component #3 - Security Plan Template" to begin developing your company's Security plan.