

PROVIDING SECURE TRUCK OPERATIONS

Safety recommendations for the commercial vehicle operator.

May 2002

Provided by:

Daecher Consulting Group, Inc.
3780 Trindle Road, Suite 2
Camp Hill, PA 17011
(717) 975-9190
cdaecher@safetyteam.com

&

The American Society of Safety Engineers
Transportation Practice Specialty

For more information contact: www.asse.org
or email customerservice@asse.org

PROVIDING SECURE TRUCK OPERATIONS

Since September 11, 2001, security is on everyone's mind and has become a most important priority. For commercial vehicle operators, this new priority presents many challenges. Nevertheless, this challenge must be met.

In considering truck operations, one must begin to plan for security response at three levels:

- Attacks upon the equipment to cripple our ability to transport goods;
- Attacks upon/use of cargo for terrorist acts;
- The use of equipment to attack larger targets such as warehouses, national monuments, transportation infrastructure, etc.

In order to develop a security program to combat such efforts, a systematic approach to developing procedures, implementing technology, and hiring and training the appropriate people become important centered around two critical organizational points:

- Who handles, touches, or has access to a truck during any 24 hour period;
- How is a truck used and what are the current procedures for its movement from one point to many other points during the course of a day?

What makes this process so difficult is that many of us are not oriented toward thinking and do not want to think as a terrorist. Nevertheless, a far reaching and comprehensive program for security centered around the two above principle points and incorporating as much as we can the thinking of twisted and hateful minds is necessary. The following checklist is an initial attempt to develop systematic thinking toward effective security programs for all truck operations.

In order to begin, a brief description of truck movement is as follows:

- Sits at rest in the company yard;
- Moves into the maintenance area for work;
- Moves into the wash area for cleaning;
- Sits in the company yard;
- Moves onto the street and from point to point based upon predefined schedules or delivery locations;
- Returns to the yard and sits or is parked and put at rest at a remote location during the course of an extended trip;

- Inspection by Commercial Vehicle Inspectors at undefined and undetermined locations.

The people who would most likely operate or interact with the truck during the course of a truck day are:

- The driver;
- Mechanic;
- Truck washers;
- Loaders/unloaders of cargo;
- Commercial Vehicle Inspectors.

The first most basic element in defining an effective security program is to identify truck locations or activities during the course of a typical day or, if you have more than one type of typical day, during the course of multiple typical days and to define those people who will interact with that truck on a daily basis. If you do not do this, significant leaks and gaps in your security plan can exist.

Based upon the above truck activities and people interacting with trucks, the following is a list for security program development:

1. The Tractor and Trailer
 - a. Minimize/remove and keep to a minimum any interior compartments for storage or access to truck systems.
 - b. All trailer doors should be secured with locks or other types of security devices. If these security devices are tampered with, the driver should be required to go through a strict protocol of inspection of the unit and its contents before proceeding.
 - c. Fire extinguishers should have a unique and definable marking, whether it is on the casing or an additional tag, to insure the driver or any other person inspecting it that it is a bonafide and usable fire extinguisher. By providing an identifiable mark, such extinguishers can not be replaced with similar looking encasements which may contain explosive materials.
 - d. All necessary compartments which remain on the interior of the truck should be locked and sealed.
 - e. All compartments on the exterior of the truck (tool boxes, utility compartments, etc.) should be equipped with tamper proof locks and/or electronic means of

surveillance to determine if these locks have been opened while the truck was in a secure shut down mode.

- f. Each truck should have an engine kill switch which is operable not only from the driver's compartment but from a remote location. This will require electronic operation and cell or satellite communication.
 - g. Each truck should have a silent communication/emergency capability.
 - h. Trucks should have vehicle location systems (cell/satellite locators) to know a truck's' actual location at any time from dispatch or some other centralized location.
2. Drivers, Mechanics, Truck Washers, Loaders/Unloaders (including all employees operating powered industrial trucks or working within warehouses containing freight), Etc.
- a. Must have a United States driver's license for at least three years.
 - b. Should not have multiple addresses.
 - c. Must provide five personal references. These references must be contacted for verification of personal identification and as an expanded personal reference check. All references can not be immigrants or citizens of a foreign country.

Note: The above qualification standards and procedures are in conjunction with those procedures already in place.

3. Procedures and Training

- a. Any time an interior compartment is accessed by a mechanic or any other employee, another employee must inspect the interior compartment, reseal it, and sign off. Documentation should be required to show the employee who accessed the compartment and the employee who inspected and resealed.
- b. Regular inspections of fire extinguishers with initials or sign offs by those who inspected them should be documented and records kept at the company's facility. These records should be kept for at least five years.
- c. Pre-trip inspections must be enhanced. They also must be done thoroughly on a daily basis by all drivers. Thorough inspections looking underneath the truck for suspicious items attached to the structure is important. A thorough inspection of each compartment with the truck in a shut down and secure inspection mode must be done. Each compartment must be relocked or sealed.
- d. A means of inspecting the roof of the truck during pre-trip inspections is

important.

- e. Call-in procedures must be enhanced to insure control of the vehicle by the driver and vehicle location. On a regular time basis (such as two hours) every driver must call in and confirm their exact location and operating conditions. During this call-in, any suspicious activities, people, etc. should be noted. This protocol should be in place and never violated. If a driver misses a scheduled call-in, dispatchers must attempt to communicate with the driver and, if that fails, communicate with police to confirm truck location and operations.
- f. Develop a communication protocol for any emergency response related to suspicious people or hijack/terrorist situations. Make sure all people involved in the communication process are trained and prepared for deployment of the process if and when necessary.
- g. Vary routes whenever possible to minimize predictability and ease of hijacking or intervention.
- h. When vehicles are not stored overnight at company facilities, vehicles should be parked in well-lit areas. They should not be parked alone in unsecured areas. Visibility and activity associated with numbers of vehicles is an important security factor.

4. Facilities

- a. Warehousing/storage facilities should be secured and monitored at all times. Enhance security procedures regarding the acceptance of freight, its continued presence, and its reloading for departure must be developed.
- b. Employ bomb sniffing animals for cargo checks at terminals and other cargo collection points.

5. Government Considerations

- a. Trucks owned and operated by companies who are properly registered with USDOT and state agencies could be monitored if security protocols are required by law. The most difficult scenarios within which to gather intelligence are for operators of individual units or for operators of units who do not intend to use them for commercial purposes. It is suggested that for these specific situations, the government do the following:
 - i. The purchase of any truck from a manufacturer must be documented and registered with the USDOT and state within which the unit is to be delivered. This documentation should include the serial number of the unit, date of delivery, and purchaser.

- ii. Within 90 days, the US government and the state to which the vehicle was delivered should have an automatic inquiry into the registration of this vehicle for commercial purposes. If the vehicle has not been registered for use, appropriate investigation should occur to understand the status and operation of the unit.
 - iii. Any truck purchased through any used vehicle dealer should also be documented and sent to the appropriate state within which purchase occurred and within which deliver will be made and to the US Department of Transportation. Again, vehicle registration, states of sale and delivery, and purchaser should be known. This should be done even if the vehicle is purchased with express intention for private use (e.g. a truck purchased as a motor home). Within 90 days, appropriate follow up should be done by state agencies to insure that the vehicle has been registered. Any additional intelligence follow up regarding the purchaser or operation of the vehicle should be done by appropriate federal and state agencies.
- b. A standard procedure for USDOT and/or state agencies should be to conduct a full compliance audit within 90 days of new motor carrier registrations should be established. This review not only could enhance general safety operations, but could incorporate an enhanced security check and balance procedure to understand the legitimacy of these operations.

The above listings are not assumed to be complete. I am sure that these listing will be added to or modified over time.

What these listings intend to do is make you think about developing security processes as part of your everyday business operation. Add, delete, modify the above lists. But most importantly, think about security and implement procedures, install technologies, and inform all employees about security programs for your company and customers.

Keep in mind that some technologies should be deployed without fanfare. Drivers should not be able to override technology operation.

Trucks can be used for attacks on facilities or widespread attacks using chemicals or germ carrying agents. Thus, safeguards against explosive materials and devises, unauthorized hazardous/toxic cargos, and illegal operation of the vehicle is important for all security procedures. We must make every best effort to prevent hijacking from occurring on or with our trucks.

People who perpetrate such acts do not have twisted minds; they have twisted hearts and souls. If courage is death they have much of it since they are so willing to die. But if courage is to lead people in changing their ways of life, especially as it relates to their fellow man, terrorists always fail. Our challenge is not to be fearful but to lead. Our challenge is to show the courage to change within our industry and to protect and defend those who are dear to us - our family, employees, customers, and even our country.

Somehow, we must find ways to do this without increasing our costs so dramatically that we drive ourselves out of business, or limiting ourselves in finding capable employees, etc.

Our compassion is not our weakness; it is our strength. We have the hearts and the souls to respond to those that are empty. All we must do is out think them. While that is a daunting challenge, there is no doubt in my mind that we can do it.

Unfortunately, it is impossible to guarantee the elimination of the use of a truck or a truck for terrorist acts. Nevertheless, through a comprehensive, well defined, and consistently deployed strategy, the commercial motor vehicle industry, including the government, manufacturers, operators, and other relevant organizations can limit this potential and maximize security for employees, customers, and the general public.