

RISK ASSESSMENT DETERMINATION WORKSHEET

The risk assessment determination involves analysis of the company's operations and characterization of the nature and magnitude of the security risks. The assessment does not have to be costly or complex, but can begin simply and progress in complexity as needed. It can simply involve reporting the impressions of experienced company staff, brainstorming sessions, or conducting a survey by a diverse team composed of staff from various operations (e.g. drivers, dispatchers, cargo tank and bulk storage equipment vendors). Generally, small business petroleum marketers fully understand the dangers from both a safety and security standpoint involved with transporting petroleum products. Much of it is based on common sense. The risk assessment process can be made as simple as possible but should be memorialized in writing and kept on file for future U.S. DOT inspections. Use the work attached sheet to assist you in this process.

The goal is to identify points in the petroleum distribution chain where security risks exist, but where actions can be taken to reduce the security risk. This does not mean that petroleum marketers in all situations will be required to install expensive security equipment. Simple common sense alternatives may be equally effective. However, in some cases new equipment may be the only way to reduce risk based on assessment considerations unique to each operation. The requirement is to take reasonable steps to reduce (not necessarily eliminate) risk.

1) List all the operations of the company that involves petroleum transportation.

Example:

Loading and unloading operations at bulk plants, terminals or motor carriers.

Delivery of product by cargo tank motor vehicle to:

1. Farmers
2. Airports
3. Marinas
4. Government entities
5. Commercial Fleets
6. Private residences
7. Retail locations
8. Co-ops

2) Characterize the nature and magnitude of security risks to the petroleum shipment operations listed above.

Example:

- Shipments are vulnerable to unauthorized access during loading and unloading, because doors are not locked on cab, keys are left in the ignition.
- There is no current communication procedure in place for receiving security information from employees or reporting security emergencies to law enforcement authorities.
- Driver work histories do not undergo sufficient scrutiny.
- I don't know my motor carrier's security procedure regarding driver screening.
- Bulk plants are vulnerable because access is not controlled. There are no lights, no fence no locks on valves. The plant is vulnerable because it is in a highly populated area, next to a school, public drinking water supply, hospital, bridge or tunnel.

3. What procedures will reduce the risk points identified in number two above?

This is essentially what goes in the written security plan. Select the risk avoiding measure that best suits you individual operation based on risk.

Example:

- Secure access to bulk storage area by unauthorized personnel. This could be accomplished by requiring all visitors (including vendors) to sign in and obtain an ID badge. Or a more expensive solution might be to erect a fence around the bulk plant, install lights or video surveillance equipment. If valves on tank and loading rack are can be locked this may be all that is necessary based on how you determine the risk.
- Secure access to cargo tank vehicles. Require drivers to remove keys, raise windows and lock door of cab during deliveries or whenever the vehicle is unattended. Make sure that the cargo tank is always parked in a secure well lighted area when not in use. Keys should be locked in a safe area. Cargo tanks should be empty when being stored overnight. Consider low risk delivery routes when risk is high. Maintain driver contact with phone or radio. Give driver information on how to recognize a security risk. More expensive alternatives should be considered such as remote ignition kill switches or global tracking systems if you determine that the risk to cargo tank vehicles is particularly high in your situation.
- Centralize system for security information and emergency response procedures. Have a single employee responsible for receiving security information and putting into motion emergency response procedures. Keep HAZMAT drivers and HAZMAT employees informed of security risk code levels.
- Train HAZMAT drivers and HAZMAT employees on how to recognize and respond to security threats.
- Coordinate driver security efforts with suppliers, terminal operators or for hire motor carriers. Make sure they understand and implement security plan.
- Revue and if necessary amend written security plan on a periodic basis.