

MEMORANDUM

DATE: May 3, 2003 (UPDATED 9/30/10) **E-03-11**

TO: State Association Executives

FROM: Laura Tague

SUBJECT: Truck Security Plan Template for Petroleum Marketers

Attached is a template for petroleum marketers to use when developing a truck security plan as required by the new DOT regulations.

U.S. DOT HAZMAT Security Plans:

The U.S. DOT released a final rule that narrows the type of hazardous materials subject to written transportation security plans and clarifies certain requirements to security planning, training and documentation. DOT transportation security plans were first required in 2003 and originally applied to any company that transports placarded loads of hazardous materials including gasoline, distillates, or propane. The final rule narrowed security planning requirements to "high consequence" hazardous materials if stolen or used for terrorist purposes. Beginning October 1, 2010 the transportation security plan and training requirements no longer apply to distillates that are shipped as a flammable or combustible under the "Packing Group III" designation in the U.S. DOT hazardous material table at 49 CFR 172.101 (available at <http://www.phmsa.dot.gov/hazmat/library>.) **In other words, if your company transports distillates such as fuel oil, kerosene or diesel fuel but NOT gasoline or propane, then the U.S. DOT security plan and training requirements no longer apply.** If your company transports gasoline or propane, the security plan and training requirements continue to apply.

In general, the rule requires shippers and carriers of hazardous materials (**gasoline, propane only**) to develop and implement written security plans and train employees to prevent security threats. Under the new rule, PMAA members must have a security plan in place by September 25, 2003. These plans must include measures to confirm information provided by the job applicants hired for positions that involve access to and handling hazardous materials; measures to address unauthorized access to the hazardous materials; and measures to address the assessed security risks of shipments of hazardous materials during a route.

In addition to the above requirement, each hazmat employee must be trained on the company's security plan and its implementation. Keep in mind there are two types of training that must be done, each with different deadlines for implementation.

Comprehensive information on the new rules was sent out by PMAA on April 9, 2003.

TRUCK SECURITY FOR PETROLEUM MARKETERS

Introduction And Purpose of This Document

The purpose of this document is to help petroleum marketers develop a security plan as required by recently published regulations of the Department of Transportation's Research & Special Programs Administration (RSPA). Below are listed a series of suggested elements which may (or may not) be included in your corporate security program.

These suggested elements were developed by the National Tank Truck Carriers Association and have been adapted by PMAA for its members. There is no "one size fits all" security plan for petroleum marketers and you must customize this template to fit your needs. For example, there may be elements in this draft that do not fit your particular situation, or you may want to add to the plan. Remember, as high volume and high profile transporters of hazardous materials, the petroleum industry will be a high priority as far as DOT enforcement is concerned. Therefore, we strongly suggest that you get your plan developed and begin the required training as soon as possible. Also, be sure that you have documentation to demonstrate that your employees who handle hazardous materials have signed off on the training that they have received.

The Regulatory Requirements and Timeline

Shippers and carriers must:

- 1) Have a written security plan in place by September 25, 2003;
- 2) All hazmat employees must be trained on that plan by December 22, 2003 (note: A "hazmat employee" is any person under your corporate control who performs any task covered by RSPA's Hazardous Materials Regulations.);
- 3) In addition to training on the specifics of your security plan, general security awareness training must be provided to anyone as part of 3-year recurrent training beginning March 25 of this year.

SUGGESTED ELEMENTS OF A PETROLEUM MARKETER'S SECURITY PLAN

Statement of Purpose:

(Company name) is committed to the safety and security of our employees, the customers we serve, and the general public. We all are aware of the reasons that we must be more vigilant to prevent or inhibit the use of our equipment, terminals, or the products we transport by terrorists. We urge all employees to help us implement this plan and to continuously improve our security efforts.

Regulations of the United States Department of Transportation require that any employee of this company (including independent contractors) who is a "hazmat employee" be trained and familiar with our company's security plan. According to those regulations, a "hazmat employee" is a person who is employed by a hazmat employer and directly affects hazmat transportation safety, including an owner-operator of a motor vehicle, which transports hazardous materials; a person (including a self-employed person) who:

- loads, unloads, or handles hazmat;
- tests, reconditions, repairs, modifies, marks, or otherwise represents packagings as qualified for use in the transportation of hazmat;
- prepares hazmat for transportation;
- is responsible for safety of transporting hazmat; or
- operates a vehicle used to transport hazmat.

Personnel Security

(Company Name) will implement the following provisions with regard to the employment (including applications for employment) of drivers. Additionally, the company may (at its discretion) implement some or all of these provisions relevant to the employment of non-driver employees who perform functions regulated by the U.S. Department of Transportation's "Hazardous Materials Regulations" within Title 49 of the Code of Federal Regulations.

- 1) Perform detailed background checks on all applicants for any driver or leased operator position.
- 2) To the extent possible, check for criminal convictions.
- 3) Contact previous employers and references.
- 4) Investigate gaps in employment.
- 5) To the extent possible, have at least 10 years consecutive employment/education records.
- 6) Maintain employee information in a confidential and secure manner, and in compliance with all relevant federal and state regulations and statutes regarding confidentiality and individual privacy.
- 7) Verify that drivers are US citizens or that non-citizens have documentation appropriate to their immigration status.
- 8) Ensure drivers have current CDL with appropriate endorsements and another form of identification (i.e. company issued credential; current medical certificate.)
- 9) Collect company identification card and any security materials when a driver/employee leaves the company. Update websites and lists. Cancel passwords to prohibit computer access by former employees.

Unauthorized Access

- 1) Management will designate who is in charge of security for the company and at each facility.
- 2) Management will conduct security awareness training for all employees, including how to report suspicious incidents or events.
- 3) Supervisors will require all visitors and outside vendors to a terminal to sign in and be given a visitor's badge. Designated parking areas for visitor vehicles should be established.
- 4) Designated personnel will perform daily yard checks and equipment reconciliations.
- 5) Designated personnel will remove keys from trucks not in use and have secure key storage.
- 6) All employees should control access to computers, especially those with product or routing information.
- 7) The Company may request periodic checks of facility areas by local law enforcement, especially when facility is not open, and consider professional security force at higher risk terminals or during Orange or Red conditions.
- 8) The Company may develop specific actions for each security level alert that might be set by the Department of Homeland Security. (e.g.. no preloading during condition Red).
- 9) The Company will post nation's threat level in drivers' room and other public areas.
- 10) The Company will post and periodically review driver anti-terrorism tips.
- 11) Management should inspect facility grounds, maintenance areas, and buildings to identify points of possible unauthorized entry to the property. This will be an important consideration, particularly at facilities having more than one point for access and egress.
- 12) Periodically, the Company may test emergency response communications equipment and procedures.

En Route Security

- 1) Sales and supervisory employees should not accept business from an unknown party before verifying company legitimacy.
- 2) Drivers and terminal personnel should lock tractor doors at all times and take keys anytime driver is not with vehicle. Ensure windows are closed.
- 3) If possible, drivers and terminal personnel should lock steering columns when truck is not in service.
- 4) Drivers should perform "walk around" inspection of vehicle after every stop, including deliveries and breaks. Be sure to look under the trailer and in hose tubes where a device could be attached.
- 5) Supervisors should develop "parking instructions" for any locations away from terminal. Look for lighted and fenced areas, visibility, and security.
- 6) Supervisors should include security considerations in route selection and times for pick up and delivery. When possible, avoid bridges, tunnels and dense population areas.
- 7) Dispatchers and supervisors should minimize driver "down-time" while en route. Schedule and dispatch with as few required stops as possible.
- 8) Management will establish procedures to communicate emergency messages to all facilities and to drivers on the road. Options may include satellite communications systems, cell phones, two-way radios, or scheduled call-in times. Management will include communications procedures for drivers to report any unexpected occurrence with equipment, load, or route.

- 9) Drivers (and other knowledgeable employees) should not discuss any details about their load or pick-up points and destinations with unauthorized personnel, such as over the CB radio or at truck stops.
- 10) Drivers should not pick up hitchhikers or allow any unauthorized personnel in the truck cab.
- 11) Drivers should not stop to help disabled vehicles or motorists. Call local authorities and notify them of anyone needing assistance. Be suspicious of motorists trying to get the driver to pull over for an "alleged" traffic accident. Be especially suspicious of vehicles with three or more people in them.
- 12) Supervisors should develop procedure for detecting "late loads." Investigate any late load more than an hour late for a delivery.
- 13) Drivers should not change delivery destination unless authorized by dispatch.
- 14) Supervisors should develop a procedure for drivers when being asked to pull over by law enforcement or unmarked vehicle.
- 15) Supervisors may arrange with shippers to schedule teams for long trips with high hazard materials.
- 16) Supervisors should consult with shippers to ensure security of consignee delivery areas. Request well-lighted and marked delivery area and that customer personnel be available to answer safety or security questions.
- 17) All employees are to report any suspicious events to company and local law enforcement.

Tank Wash Rack Security (If Applicable)

- 1) Control wash rack and facility security:
 - Establish visitor procedures, including drivers and vendors.
 - Establish visitor sign in and visitor badge/pass.
 - Establish vehicle parking area and vehicle parking tags.
- 2) Establish daily chemical and hazardous waste inventory.
- 3) Establish procedures for releasing equipment, including driver ID.
- 4) Perform multiple daily trailer inventory checks at facilities.
- 5) Train all employees, including front office, on security and notification procedures, including the company official and public agency to notify.
- 6) Designate a facility manager and/or shift supervisor in charge of security.
- 7) Develop facility monitoring procedures for during operation hours and when the facility is not open.