PETROLEUM MARKETERS ASSOCIATION OF AMERICA
1901 N. Fort Myer Drive • Suite 500 • Arlington, VA 22209-1604 • 703-351-8000 • Fax 703-351-9160

# U.S. DOT SECURITY PLAN REQUIREMENTS FOR THE TRANSPORTATION OF PETROLEUM PRODUCTS

**A Compliance Guide for Petroleum Marketers**

Prepared By:

Mark S. Morgan, Esq.
Petroleum Marketers Association of America

4200 Wisconsin Avenue, N.W., Suite 106
Washington, D.C. 20016

(202) 364-6767
mmorgan@pmaa.org

## Introduction

This kit includes everything needed to comply with U.S. DOT written security plan requirements for the transportation of petroleum products. Included you will find a step-by-step process for full compliance along with a security plan template that can be easily tailored your company's specific requirements. If after reading the following material you have any questions relating to security plan compliance, please contact Mark S. Morgan at mmorgan@pmaa.org or at (202) 364-6767.

## I. Establishing A Security Plan for the Transportation of Petroleum Products

The United States Department of Transportation's Research and Special Programs Administration has issued final regulations (FR 68 14509) requiring all companies that transport hazardous materials (including petroleum products) establish a written security plan. The new regulations also require specific training requirements for HAZMAT drivers and HAZMAT employees.

This compliance kit is specifically written to aid petroleum marketers with transportation operations to comply with the new federal regulations. Included in the kit is a risk assessment guidance document, a written security plan, worksheets and a resource list for additional information. While the security plan included in this kit addresses the security risks of the typical petroleum marketing operation, it should be changed to fit any specific or unique security requirements your company may have.

**a) Compliance Dates:**

- Written Security Plan Must be Completed by **9/25/03**
- HAZMAT Employee Training on Security Plan Must be Completed by **12/22/03**

## II. Risk Management Assessment Planning Guide

Given the heightened specter of terrorism, the security of petroleum shipments and other hazardous materials has become a priority for petroleum marketers, carriers, shippers, consignees, emergency responders and government officials. The existing hazardous material transportation process, including personnel, procedures, cargo tank motor vehicles and bulk plant facilities must be reexamined from a security prospective. Addressing security concerns should be part of an overall strategy to manage the risk of hazardous materials, such as petroleum products, during transportation.

The following risk assessment tool can be used to aid petroleum marketers in enhancing security and safeguard shipments of petroleum products against terrorist attack or sabotage. This risk assessment document will help to evaluate and manage risks
and hone practical, common sense knowledge to reduce risk even further.

**a) Principles Applied to Managing Security Risk:**

The following fundamental principals are critical for successfully managing risk:

- Obtaining commitment to reducing security risks on the part of both managers and workers.
- Promoting a "risk reduction culture with a security focus" in day-to-day operations.
- Partnering with all parties involved in securing the petroleum transport distribution chain.
- Prioritizing security risks so that resources can be allocated effectively.

- Taking action to reduce the security risks that have been identified.
- Striving for continuing improvement.
- Communicating with all parties to ensure each knows its role and is aware of relevant security risk information.

**b) Step-by-Step Process for Security Risk Assessment:**

**Step 1: Defining the Scope of Security Requirements –What's Covered?**

Security considerations can cut across the entire petroleum transportation process. However, to effectively focus an effort on security risk, a company should generally characterize its petroleum transportation process, and then make initial decisions as to which transportation activities merit more security scrutiny. The initial decisions may be made based on company perceptions of the greatest security risks or based on previous threats. Key areas of concern for petroleum marketers are cargo tank and bulk plant security, and personnel security screening that focuses on U.S. residency status, criminal background history and the validity of CDL licenses, hazardous material endorsements and driver medical qualification certificates.

Defining the scope of the activities to be considered in terms of security also includes identifying other partners that are interested in the security of the company's petroleum shipments. For petroleum marketers, these partners include terminal operators, for-hire motor carriers, cargo tank motor vehicle repair shops, and local law enforcement officials.

**Step 2: Knowledge of Operations – Making a List**

Step II involves collecting detailed information about the petroleum transportation operations/decisions that will be examined for security risks. Make a list. Describe the quantities of petroleum shipped, who handles the product, the routes used for delivery and where and when the product is handled. For petroleum marketers the quantity of product shipped is easily determined from existing company records. HAZMAT drivers and HAZMAT employees are the primary parties handling product, delivery routes are generally well known and the products are essentially handled at the terminal, bulk plant loading rack and at delivery locations.

Additionally, describe on the list the existing security activities already in place for the transportation of petroleum products. Keep in mind that the new security rules issued by the U.S. Department of Transportation includes storage incidental to shipment (i.e. bulk plants). The inventory of information should cover security issues with personnel (background checks, licensing and training), security procedures and plans, and the security of bulk plant facilities and equipment. Current safety and risk regulations (e.g. parking restrictions) that have security impacts are also important to the list. In determining the security activities to describe, ask how loads are secured. Questions such as Do drivers regularly follow the company's security and safety guidelines? What are the chief causes of transportation related accidents? Have any threats previously been received at the company offices? Are there any trends that can be identified (e.g. areas or type of equipment with a high frequency of theft)? Much of the list is really based on ***common sense and your intimate knowledge of company operations.***

**Step 3. Assessment – What are the risks?**

This assessment step 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. Risk control points for petroleum marketers typically include;

- **Personnel Backgrounds –** Employment history and verification of citizenship of HAZMAT drivers and HAZMAT employees.

- **Cargo Tank Motor Vehicle and Bulk Plant Access Control -** Locking procedures for unattended cargo tank motor vehicles and loading rack equipment, secure parking areas, lighting, fences where necessary, security systems, integrity of access codes and key storage, limiting access to authorized personnel.

- **En Route Security –** Avoiding highly urbanized areas, bridges, tunnels, public schools and hospitals. Prohibiting drivers from changing delivery routes without prior authority, maintaining contact with drivers, forbidding unscheduled and unauthorized stops (except if instructed by a law enforcement official), prohibitions stopping for hitchhikers, assisting roadside motorists in need, parking in secure areas, and removing ignition key, locking doors and rolling up windows at all stops, including delivery.

- **Communications –** Use of cell phones or two radios to reach all drivers, immediate reporting of suspicious activities, providing updated information on security to HAZMAT drivers and HAZMAT employees as it becomes available and informing them of national security threat levels set by the U.S. Department of Homeland Security (i.e. the color code threat level system), loading and unloading activities at bulk plants, en route transportation of product to the customer, delivery into the customer's tank, unattended cargo tank vehicles, ease of and ability to control access to cargo tank vehicles, bulk plant facilities and shipping information, emergency response protocols, and HAZMAT driver and HAZMAT employee criminal, residency and work histories.

- **Emergency Response –** Adequacy of training and resources for response to terrorist type incidents, centralizing emergency response and information through a designated company security contact.

- **Readjustment Based on Changed Circumstances –** Possible Heightened security procedures after terrorist attacks or increased threat levels.

**Step 4. Strategy – The Written Security Plan**

The heart of a strategy to address security risks is to develop a security action plan. The plan prioritizes the security risk control points based on the degree of vulnerability and potential impact. The written security plan also outlines potential and preventative control actions based on the ability to reduce risk and the resources available. The plan should provide for the installation of new equipment (e.g. locks, lights etc.) if appropriate, establish security procedures, assign security response responsibilities to key employees and convey management commitment to enhanced security awareness and risk reduction procedures.

A written security plan developed for small business petroleum marketers is included in this package. It is designed as a template that can be easily changed to fit specific marketing operations and unique security needs.

Petroleum marketers are likely to find that they are already performing many of these security procedures. For example, the requirement for in depth security training for HAZMAT drivers and HAZMAT employees under the new DOT security regulations has been incorporated into existing DOT training programs these employees must already undergo on a periodic basis. Petroleum marketers should simply make certain that the HAZMAT training provider they are currently using has incorporated the in depth security training component as part of the regular curriculum. Get the verification in writing if possible and place it in your security risk assessment files. Also, HAZMAT driver background checks are conducted by state licensing authorities along with the FBI and DOT, so there is no need for petroleum marketers to duplicate this task. Similarly, most drivers already have cell phones or two-way radios to maintain continual contact with dispatchers or company management. Packaging control such as locks for cargo tanks, bulk plant loading racks and valves and security lights are likely to already be in place.

On the other hand, petroleum marketers should focus on upgrading emergency response capabilities relating to security issues. Since such a system is already in place for safety related emergencies, only minor adjustments to fold in the security component will be required.

**Step 5. Implementation – Getting the Plan Activated**

This step is simple. Familiarize HAZMAT drivers and HAZMAT employees with the security plan, ensure that they fully understand it and are committed to implementing it on a daily basis. Make the plan official company policy and require HAZMAT drivers and HAZMAT employees to sign it, attesting to their awareness of the plan's components and commitment to implementing it at all times.

**Step 6. Evaluation – Is the Plan Working?**

This step determines if the goals established for reducing security risks are being met. To measure progress, monitor the plan in action and establish performance indicators to evaluate its effectiveness. Evaluate the plan on a periodic basis. When weaknesses are identified change the security plan as needed. Keep written records of your efforts to evaluate the effectiveness of the plan and maintain them in a security file.

## III. 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. **Lack of a written Risk Assessment Worksheet is the most the most common U.S. DOT penalty in the enforcement of security plan regulations. Keep a written copy in your security file.**

**a) 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



**b) 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.

**c) 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 driers 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.

## IV. Written Security Plan Template

(INSERT COMPANY LOGO, NAME, ADDRESS AND PHONE NUMBER HERE)

(HAZMAT Employee Must Sign, Keep on File as evidence of Training. Keep Second Copy Signed by the Company Owner and Designated Security Contact in a Separate Security File)

**SECURITY PLAN**

**FOR**
**THE TRANSPORTATION OF PETROLEUM PRODUCTS**

**STATEMENT OF PURPOSE**

This written security plan has been developed pursuant to 49 CFR Part 172 Hazardous Materials: Security Requirements for Offerors and Transporters of Hazardous Materials promulgated by the U.S. Department of Transportation's Research and Special Programs Administration (68 FR 14509). (Insert Company Name Here) is committed to the safety and security of every hazardous material shipment conducted by the company and its employees. Petroleum products are extremely volatile materials that alone, or in combination with other chemicals, can produce a catastrophic explosion.

The U.S. Transportation Security Administration has reported that international terrorist groups are interested in obtaining hazardous materials, such as petroleum products through both legal and illegal means in order to use such material in this country as weapons of mass destruction against both civilian and military targets. In fact, fully laden petroleum cargo tank motor vehicles have already been used as weapons of mass destruction in a number of foreign countries over the past several years. The shipment of hazardous material petroleum products by (Insert Company Name Here) puts the company, its employees, our customers as well as our friends and neighbors, at an elevated risk of terrorist attack.

In order to enhance the security of hazardous material shipments, all employees must take the risk of terrorist attack against this company's hazardous materials shipment seriously. It is company policy that all

employees make every effort, on a daily basis, to ensure the security of each hazardous material shipment from the time the product is assigned to company control until it is safely delivered to the ultimate purchaser.

The following written security plan is company policy. All HAZMAT drivers and HAZMAT employees must read it, become familiar with and understand its requirements and implement its procedures at all times as a condition of continued employment. Security of all hazardous material petroleum product shipments, whether in transit via cargo tank motor vehicle or in storage awaiting delivery at the bulk plant, is the company's top priority.

## SECTION ONE
## DESIGNATED SECURITY CONTACT

**Centralizing the Flow of Security Related Information.**

All security related questions, information, reports of suspicious activity or incidents involving the shipment of company controlled petroleum products must be reported immediately to:

(Insert the name and telephone number(s) and other contact information of employee responsible for being the point of contact for all security related information here)

The designated security contact will relay security related information immediately to the appropriate person or persons within the company as well as to state local and federal law enforcement officials.

## SECTION TWO
## PERSONNEL SECURITY

**Security Requirements for Personnel with Access to Petroleum Cargo Tank Motor Vehicles or Storage Areas Where Bulk Petroleum Product is Located.**

(Insert Company Name Here) will implement the following procedures as company policy to ensure that no HAZMAT driver (commercial driver's license holder with hazardous material endorsement) poses a security risk that in any way endangers a company shipment of petroleum product. These procedures also apply to current non-driver HAZMAT employees (and applicants for hire) whose duties require periodic safety training under existing federal hazardous material regulations.

- Ensure that a detailed background check for criminal activity and security risk is performed on all applicants for HAZMAT driver and HAZMAT employee positions with the company,
- Contact previous employers and references of all applicants for HAZMAT driver or HAZMAT employee positions,
- Investigate gaps in applicant employment history or any other information that seem suspicious,
- To the extent possible, require at least ten years consecutive employment and/or education records for all HAZMAT driver and HAZMAT employee applicants,
- Ensure HAZMAT driver applicants have current CDL license with appropriate endorsement and other forms of identification (e.g. current medical qualification certificates, etc.),

- Verify that all HAZMAT drivers, HAZMAT employees and applicants for those positions are U.S. citizens or have appropriate legal alien status and work authorization documents issued by the U.S. Immigration and Naturalization Service,

- Upon termination of employment of any HAZMAT driver or HAZMAT employee, secure petroleum shipments by:

  1) Collecting employee identification cards, photos or other items that demonstrate employment with the company, keys to petroleum cargo tank motor vehicles, bulk plant security equipment, secured buildings and other secured areas, cell phones and two way radios,

  2) Canceling all computer passwords and other access codes that would allow former employees to gain access to hazardous material shipments or to sensitive information such as delivery schedules, routes and destinations,

  3) Updating company records, web sites and other material that lists employee names or authorizes access to hazardous material shipments,

  4) Informing company employees, terminal operators, bulk plant personnel or other product suppliers when a former employee is no longer authorized by the company to have access to hazardous material shipments or information.

**SECTION THREE**
**UNAUTHORIZED ACCESS**

**Preventing Unauthorized Persons From Gaining Access to Petroleum Cargo Tank Motor Vehicles, Storage Areas Where Bulk Petroleum Product is Located and Shipment Information.**

The following procedures are adopted as company policy to prevent unauthorized access to petroleum product shipments and related information:

- All outside visitors and vendors to company facilities where petroleum bulk plants or cargo tank vehicles are present must first obtain a visitor's pass before gaining entry,

- All cargo tank motor vehicles and related equipment, bulk plant security devices and company offices where petroleum shipment information is located must be locked and keys stored in a secure area when unattended or not in use,

- Periodic inspections of cargo tank motor vehicles, bulk plant security equipment and company office buildings where bulk petroleum products are located will be conducted to detect evidence of tampering or vandalism,

- When not in use cargo tank motor vehicles must be emptied of petroleum product intended for sale, locked and parked in a well lit, secure area,

- Access to information regarding delivery schedules, routes and destinations must be limited to employees on a need to know basis,

- The status of, and changes to the nation's threat level as determined by the Department of Homeland Security will be communicated to all employees,

- HAZMAT drivers and HAZMAT employees will receive periodic

information on security precautions for petroleum shipments,

- More stringent security precautions to prevent unauthorized access may be required during periods when the nation's threat level increases,

- In the case of a security emergency or incident, all information must be relayed immediately to the employee responsible for petroleum shipment security (designated security contact). The designated security contact must immediately alert state and local police authorities and the local Office of the FBI of any security incident involving any shipment of petroleum product. The following emergency contact numbers should be called in the order listed:

  a) (Insert name and telephone number of local police or sheriff's department)

  b) (Insert state police name and emergency telephone number)

  c) (Insert the telephone number of the local FBI office)

**SECTION FOUR**
**EN ROUTE SECURITY**

**Protecting the Security of Petroleum Shipments in Transit.**

The following procedures are adopted by (insert company name here) as company policy to enhance the security of petroleum shipments during transportation. All



HAZMAT drivers must learn, fully understand and adhere to these procedures at all times:

- HAZMAT drivers are required to inspect cargo tank motor vehicles for unauthorized alternations, tampering or other suspicious activity at the beginning of each shift as part of the normal daily pre-trip vehicle inspection,

- HAZMAT drivers are required conduct a "walk around" inspection of the cargo tank motor vehicle after each delivery or stop to check for unauthorized alteration, tampering or other suspicious activity,

- Any time a HAZMAT driver leaves the cargo tank motor vehicle (e.g. loading and unloading operations, break time, down time, end of shift, etc.) the keys must be removed from the ignition, the windows fully rolled up and the doors locked,

- HAZMAT drivers are forbidden to pick up hitchhikers, allow any unauthorized person in the truck cab, stop for motorists in distress or pull over at the behest of any person unless instructed to do so by a law enforcement official,

- HAZMAT drivers may not deviate from a planned route or delivery schedule unless the dispatcher is notified before the change is made,

- HAZMAT drivers must notify the dispatcher when the deliveries fall more than one hour behind schedule (e.g. traffic delays, delays at terminal, bulk plant, etc.),

-

- Whenever a HAZMAT driver parks a cargo tank motor vehicle for any reason other than during loading and unloading operations, the parking area selected must be well lit, safe and have reasonable visibility and security,

- HAZMAT drivers should, to the maximum extent practicable, minimize "down time" during the assigned delivery route,

- HAZMAT drivers should not talk to unauthorized persons about the delivery route, delivery schedule or ultimate destination of any petroleum shipment,

- HAZMAT drivers should be alert to any suspicious activities that may endanger the petroleum shipment (e.g. talkative strangers inquiring about the shipment, roadside distractions such as disabled vehicles, occupants of vehicles pulling along side the cargo tank motor vehicle attempting to catch your attention or distract you. Be especially weary of vehicles with three or more male occupants),

- In the case of a security emergency or incident, all information must be relayed immediately to the employee responsible for petroleum product security. The designated security contact must immediately alert state and
local police authorities and the local Office of the FBI of any security
incident involving any shipment of petroleum product. The following emergency contact numbers should be called in the order listed:

    1) (Insert name and telephone number of local police or sheriff's department)

    2) (Insert state police name and emergency telephone number)

    3) (Insert the telephone number of the local FBI office)

**SECTION FIVE**
**EMPLOYEE AWARENESS**

**Understanding Security Risks and Implementing the Security Plan.**

- All HAZMAT drivers and HAZMAT employees are responsible for understanding the security risks associated with transporting petroleum products and learn to identify and respond to those risks should they occur. A security risk assessment is attached to this document to aid in identifying potential risks that may occur during shipment. (attach your risk assessment determination),

- In addition, All HAZMAT drivers and HAZMAT employees who fail to read this security plan, understand its requirements and implement its procedures at all times may be subject to termination of employment,

- This security plan is subject to change as circumstances or federal law requires. An updated copy of the company's security plan will be provided to all HAZMAT drivers and HAZMAT employees as soon as it becomes available,

- If there is any uncertainty regarding the written security plan, the security risk assessment or any other security related matter, it is the duty of all HAZMAT drivers and HAZMAT employees to seek clarification from the company's designated security contact,

- The company will provide news, updates and other pertinent information relating to security matters to HAZMAT drivers and HAZMAT employees on a regular basis,

**SECTION SIX**
**ACKNOWLEDGEMENT**

**Employee Acknowledgement of the Requirements of the Security Plan**

I _____ have read the company's written security plan and
(employee name)

and security risk assessment. I fully understand the risks associated with the transportation of petroleum products. I am able to identify and respond to security risks pursuant to the security plan and the security risk assessment. If at any time, my awareness of security issues becomes unclear or insufficient, I understand that upon request, the company will provide me with any additional training necessary to correct my level of awareness.

_____ _____
Employee Signature Date

_____ _____
Designated Security Contact Signature Date

**END OF SECURITY PLAN TEMPLATE. COMPLIANCE TEXT CONTINUES ON NEXT PAGE.**

## V. In Depth HAZMAT Employee Security Training

**(a)** ***In-depth security training.*** Each hazmat employee of a person required to have a security plan in accordance with subpart I of this part who handles hazardous materials covered by the plan, performs a regulated function related to the hazardous materials covered by the plan, or is responsible for implementing the plan must be trained concerning the security plan and its implementation. Security training must include company security objectives, organizational security structure, specific security procedures, specific security duties and responsibilities for each employee, and specific actions to be taken by each employee in the event of a security breach.

## VI. Hazardous Materials Company Anti-terrorism Tips

When the National Threat Level is raised to Code Orange, the following actions are to be taken:

**a) Personnel Security:**

Brief your employees to report suspicious incidents or events.

- Post the Nation's Threat Level in the Driver's room or other public area.
- Convene a brief security meeting when the Threat Level increases and review security plans and tips with employees.
- Make sure all employees handling or transporting hazardous materials have adequate communication devices in case of emergency. Test these systems.
- If you have a management crisis team, verify their 24/7 contact information and place them on "ready alert."
- Assure that all employees have proper and up-to-date identification.
- Assure that company personnel monitor news and other information sources for events or changes in conditions and respond as appropriate.
- Review Driver Anti-terrorism Tips list.

**b) Facility Security:**

- Cooperate with federal or local law enforcement officials concerning security checks or safety checks.
- Restrict the availability of information related to your facility and employees, and the materials you handle.
- Restrict access to a single entry or gate. Control who enters and leaves your facility, if possible. Require visitors to show photo identification and have someone accompany visitors at all times.
- Reduce your internal tolerance for "security anomalies," such as overdue or missing vehicles, perimeter of physical plant intrusions, unverified visitors, evidence of tampering etc.,
- Install additional security systems on areas containing hazardous materials, if needed.
- Do not preload hazardous materials shipments.
- Require employees to display identification cards or badges while at the facility.
- Conduct spot checks of personnel and vehicles.
- Test your emergency response communications systems.
- Upgrade security procedures for pick-ups and deliveries. Verify all paperwork and require pick-up and delivery appointments from known vendors. Require pick-up drivers to provide driver's name and vehicle number- confirm with vendor. Accept deliveries in designated areas only.
- Confirm legitimacy of new vendors though listings in phone book or industry publications, websites or references.

- If possible or appropriate, secure hazardous materials in locked buildings or fenced areas. Have a sign-out system for keys.
- Secure valves, manways, and other fixtures on transportation equipment when not in use. Secure all rail, truck, and barge containers when stored at your location.
- Use tamper-resistant or tamper-evident seals and locks on cargo compartment openings.
- Maintain current inventories of on-site hazardous materials and check account for shortages or discrepancies.

**c) En Route Security:**

- Verify identify of carrier or driver prior to hazardous materials loading. Ask driver for photo identification and compare with information provided by carrier.
- Ask the driver to tell you the name of the consignee and the destination for the material and confirm with your records before releasing shipments.
- Identify preferred and alternated routing, including acceptable deviations. Make sure routing complies with local routing restrictions.
- If possible, alternate routes to frequent destinations.
- If possible minimize exposure in downtown or heavily populated areas and expedite the shipment to the final destination.
- Minimize stops en route; if you must stop, select locations with adequate lighting on well-traveled roads and avoid high-crime or dangerous areas.
- If materials are stored during transportation, make sure storage facilities are secure.
- Train drivers how to avoid hijackings or theft of property- keep vehicles locked when parked and avoid conversation on open channels or with strangers about route, cargo, and destinations.
- Consider using advanced technology to track or protect your cargo en route to their destination (i.e., satellite tracking systems, anti-theft systems for trailers and tractors and surveillance systems). GPS tracking systems should relay updates more frequently.
- Install tamper-proof seals on all valves and package or container openings.
- Implement a system for a customer to alert the shipper if a hazardous materials shipment is not received when expected.
- When products are delivered, check the carrier's identity with shipping documents provided by the shipper.

**Get to know your customers and their hazardous materials programs. If you suspect you shipped or delivered a hazardous material to someone who may intend to use it for a criminal activity, notify your local FBI office or local law enforcement officials.**

## VII. Hazardous Materials Driver Anti-Terrorism Tips

When the National Threat Level is raised to Code Orange, the following steps should be taken:

**a) On the Road:**

- Be alert when driving. Look for vehicles following you, especially if there are 3 or more people in the car. If you believe you are being followed, call your dispatcher or 911 immediately.
- When leaving your facility, be aware of any possible surveillance of your facility or your truck.
- Don't discuss your cargo, destination, or trip specifics with people you don't know or on open channels.

- When stopped at a traffic light or in traffic, be aware of anyone approaching your vehicle.
- Make sure you have communication devices to contact your dispatcher and emergency officials. Carry a back-up if possible.

**b) Stopping at Facilities:**

- Leave your truck in a secure parking lot or truck stop if possible; if not, be certain someone can watch your vehicle.
- Never leave your vehicle running with the keys in it; shut off the engine and lock the doors.
- If possible, don't stop in unsafe or high-crime areas.
- Use seals or other methods to prevent and identify tampering.
- Don't preload hazardous materials shipments without adequate security.

**c) Protecting Your Vehicle:**

- Consider the use an engine kill switch if possible
- Use tractor and trailer brake locking devices when possible
- If you drop a trailer, use a fifth wheel lock whenever possible.

Perform a quick walk-around to check your vehicle for foreign objects after all stops.

## VIII. Ten Important Facts to Remember About Security Plan Requirements

**1. PLAN REQUIREMENTS:** There are no specific requirements for a security plan other than it must address personnel security, unauthorized access, en-route security and a stated commitment by the company to implement and adhere to the plan at all times.

**2. RISK ASSESSMENT:** It is up to each individual company to assess security risks and develop a written security plan to reduce identified risks.

**3. SCOPE:** The security plan regulations pertain to security risks associated with bulk plant storage and cargo tank transport.

**4. APPLICABILITY:** The regulation applies to all companies involved in the transportation of hazardous materials (including petroleum products) that require a DOT placard.

**5. FILING THE PLAN:** The security plans **do not** have to be sent to the DOT or any other federal agency. However, security plans must be kept on file and made accessible to HAZMAT drivers and HAZMAT employees.

**6. ENFORCEMENT:** During regular DOT on site inspections, inspectors will ask to see a copy of the plan to ensure it meets all the relevant components listed in number one above, but will not delve deeply into the specifics of the plan unless it is on its face, wholly inadequate. DOT inspectors will also ask to see a written risk analysis on which the plan is based.



**7. COVERED EMPLOYEES:** The training requirements in the security regulations apply only to “HAZMAT employees”. The DOT defines HAZMAT employees as any person employed by the company who:

- operates a vehicle containing a hazardous material,
- loads, unloads or handles a hazardous material,
- prepares hazardous materials for transportation,
- is responsible for the safety of a hazardous material shipment,

- tests, modifies, marks, repairs, reconditions a hazardous material packaging for shipment.

Typically, drivers are the only HAZMAT employees in the company. But remember, if any non-driver employee that performs any of the duties above, they must be trained.

**8. TRAINING:** Training requirements are two fold. First, HAZMAT employees must have security awareness training. This training is a component of the current DOT testing requirements that HAZMAT employees must undergo every three years or within 90 days of hiring. Under the new regulations, this training must occur at the HAZMAT employee's next regularly scheduled training date according to the three year testing cycle. However, all HAZMAT employees must complete the initial security training no later than March 25, 2006.

The second type of training, also limited to HAZMAT employees, is on the specifics of the security plan itself. This training can be done in house and need not be a structured lengthy ordeal. This training simply requires that the HAZMAT employee is aware of specifics the security plan, understands its components and will adhere to it on a daily basis. An in house training module is available free of charge from the DOT at http://hazmat.gov/hmt_security.htm. It takes about one hour to complete. This training must be completed by December 22, 2003.

**9. RECORD KEEPING:** Keep written records on any security related issue or action including a copy of the security plan, training certificates, signed copies of the security plan by HAZMAT employees and most importantly, a written evidence showing that you performed a security risk assessment. (See attached Risk Assessment Guideline).

**10. DON'T PANIC.** Most of the requirements under the new regulations are already being performed by you, or in the case of driver background checks, government agencies. All you need to do is centralize security issues in a central file. Focus on the written plan, the written risk assessment, establishing a security emergency response procedure (fold it in with your HAZMAT accident reporting procedure) and making sure that HAZMAT employees understand and are implementing the written security plan.

## IX. Additional Resources:

**1) U.S. DOT Hazardous Material Safety Web Page** – Provides the latest government alert on terrorism: **http://hazmat.dot.gov**. More information on security plan development and risk assessment can be found at: **http://hazmat.dot.gov/rmsef.htm**. A training module for HAZMAT drivers and HAZMAT employees may be downloaded for free at: **http://hazmat.gov/hmt_security.htm.**

**2) The Petroleum Marketers Association of America –** Provides regulatory compliance information regarding all aspects of security planning and other federal regulatory requirements for the petroleum marketing industry. Contact Mark S. Morgan, Regulatory Counsel at: mmorgan@pmaa.org (202) 364-6767

**3) Federal Motor Carrier Safety Administration Security Talking Web Page** – Security talking points including general security information, personnel security, hazardous materials packaging controls, en route security, technical innovations, management prerogatives, communications and readjustment of plans based on changed conditions can all be found at: **www.fmcsa.dot.gov/hazmatsecure.htm**.

**4) National Cargo Security Council Web Page –** Provides theft prevention information, including a list of cargo security links at: **www.cargosecurity.com**.

**5) National Safety Council Web Page –** Presents general safety information including emergency response plan information at: **www.nsc.org.issues/emerg/99esc.htm**

**6) American Trucking Associations (ATA) Web Page –** Provides information on government security warnings, security tips, security of cargo tank motor vehicles and driver security information at: **www.truckline.com**.

**7) Transportation Research Board Security Web Page –** Provides links to documents and other information on general transportation security at: **http://www4.trb.org/trb/homepage.nsf/web/security**.

**8) American Chemistry Council Web Page –** Provides guidance on transportation security and guidelines on chemical plant security at: **http://www.americanchemistry.com**