

SAMPLE

SECURITY PLAN FOR THE TRANSPORTATION OF HAZARDOUS MATERIALS

NOTE: ILMA has prepared this document to assist members develop a security plan required under the new regulations issued by the U.S. Department of Transportation's Research and Special Programs Administration. Based upon the regulations and information gathered from companies and others involved in the shipment and carriage of hazardous materials, the following are suggested elements of a security plan which must be in place by September 25, 2003. Because there is no "one-size-fits-all" approach to a security plan, the below-mentioned elements may or may not be included in your company's security plan. It is important to remember that a critical step in developing a security plan is the assessment of risk. This sample plan does not contain a methodology for performing such an assessment

Statement of Purpose:

[ILMA member company] ("Company") is committed to the safety and security of our employees, our customers, and the general public. Since the September 11, 2001 terrorist attacks, it has been necessary for everyone, including the Company and our employees, to be more vigilant in preventing or inhibiting the use of our products, transportation equipment, and facilities by international and domestic terrorists and by those who might collude with such terrorists. All of the Company's employees are asked to help implement this security plan and improve continuously the Company's security efforts.

The U.S. Department of Transportation's Research and Special Programs Administration has promulgated regulations (known as "HM-232") that, in part, require that any employee of this Company (including independent contractors) who is a "hazmat employee" be trained and be familiar with the Company's security plan. Our understanding of these regulations is that a "hazmat employee" is any person who performs a task or function covered by the Federal Hazardous Materials Regulations ("HMRs").

Security Risk Assessment

The Company has collected, reviewed and integrated information about potential security risks as part of its attempt to understand site-specific and route-sensitive risks to security. [Discuss generally the facilities, vehicles, routes or assets that have been identified as the most significant security risks.]

Personnel Security

The Company will implement the following provisions with regard to the employment (including applications for employment) of hazmat drivers. Further, the Company, at its

discretion, may implement some or all of these provisions relevant to the employment of non-driver employees who perform functions regulated by the Federal HMRs.

1. Perform detailed background checks on all applicants for any driver 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 U.S. 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 (*e.g.*, company-issued credential or current medical certificate.)
9. Collect company identification card and any security materials when a driver/employee leaves the Company.
10. Update Company websites and lists, as well as cancel passwords to prohibit computer access by former employees.

Unauthorized Access

1. The Company will designate who is in charge of security for the Company [and at each facility, if applicable].
2. The Company will conduct security awareness training for all employees, including how to report suspicious incidents or events.
3. The Company will require all visitors and outside vendors to a Company facility to sign in and/or be given a visitor's badge. [Consider whether designated parking areas for visitor vehicles should be established.]
4. Designated personnel will perform daily checks and equipment reconciliations.
5. All personnel will remove keys from trucks and truck tractors 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. [Consider professional security force at higher-risk facilities or during elevated threat conditions (*e.g.*, Code Red or Code Orange).]
8. The Company may develop specific actions for each security level alert that might be set by the Department of Homeland Security ("DHS").
9. The Company will post the DHS threat level in drivers' room and other public areas.
10. The Company will post and periodically review driver anti-terrorism tips.

11. All employees should be aware of possible points of unauthorized access to Company facilities or buildings.
12. The Company may periodically test emergency response communications equipment and procedures.

En Route Security

1. STAY ALERT!
2. Drivers should lock truck or truck tractor doors at all times and take keys any time the driver is not with vehicle. Ensure windows are closed.
3. Drivers should perform “walk around” inspection of vehicles after every stop, including deliveries and breaks.
4. The Company will develop “parking instructions” for any locations away from Company facilities. Look for lighted and fenced areas, visibility, and security.
5. The Company will attempt to include security considerations in route selection and times for pick up and delivery.
6. Driver “down-time” should be minimized while en route. Schedule as few stops as possible.
7. The Company will establish procedures to communicate emergency messages to all facilities and to drivers on the road. The Company will include communications procedures for drivers to report any unexpected occurrence with equipment, load, or route.
8. 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.
9. Drivers should not pick up hitchhikers or allow any unauthorized personnel in the truck cab.
10. 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.
11. The Company will develop a procedure for detecting “late loads.” The Company will investigate any late load more than an hour late for a delivery.
12. Drivers should not change delivery destination unless authorized.
13. The Company will develop a procedure for drivers when being asked to pull over by law enforcement or unmarked vehicles.
14. All employees are to report any suspicious events to the Company and local law enforcement.
15. If there is an emergency situation, contact 911 or 311 immediately.
16. Don’t allow yourself to be distracted by others during the loading/unloading.
17. Review the FMCSR pocketbook regarding attendance and surveillance of motor vehicles.

Reporting Threats and Incidents

The following information would be helpful to note when reporting any threats or incidents:

- Description of the vehicle(s): Please describe all observables about the truck-size, color, markings, as well as license, registration, and other pertinent identifying information.
- Description of the truck's contents: What is the truck carrying, and in what quantity?
- Description of the event or observation:
 - When did the event occur?
 - Where did the event occur?
 - What direction did the truck head?
 - Describe the individual(s) operating the vehicle?
 - Did the individual(s) involved in the event say anything about what they were doing or where they intended to go?
 - Additional suspects involved, i.e. supporting surveillance vehicle.

General Security Awareness

- Any employee or visitor making unusual or repeated requests for sensitive or important Company-related information.
- Any person asking a driver to make any unauthorized movement (pick-up and delivery) for cash.
- Any person or group loitering outside the Company facility.
- Any person claiming to be a representative of a utility (gas, water, electric) but cannot produce company identification.
- Any person carrying a weapon, such as a gun or knife.
- After hours, any vehicle driving by the Company facility with the lights off.
- Any occupied vehicle parked outside the Company facility – especially if the vehicle has been sitting for a long period or after normal work hours.
- Any unfamiliar vehicle that appears to be abandoned near the Company facility.