



# Recognizing & Managing Carrier Security



A Handbook For Hazardous Material Transporters

**F**REBERG  
**E**NVIRONMENTAL  
**I**NSURANCE  
INSURANCE PROGRAM MANAGERS



FIRST EDITION

**F**REBERG  
**E**NVIRONMENTAL  
**I**NSURANCE

**Insurance Program Managers**

***Recognizing & Managing  
Carrier Security:  
A Handbook for Hazardous  
Material Transporters***

December 2001



Printed on recycled paper.

*The material in this publication is provided for information purposes only and is not intended to be representative of coverage that may exist in any particular situation under your insurance policy. Please read your insurance policy carefully. All conditions of coverage, terms and limitations are defined and provided for in your insurance policy. All terms may vary by state or by insured.*

# TABLE OF CONTENTS

	<u>Page</u>
<b>PREFACE.....</b>	<b>v</b>
<b>ABOUT THE AUTHORS .....</b>	<b>vii</b>
<b>CHAPTER 1. INTRODUCTION.....</b>	<b>1-1</b>
Who the Handbook Is For .....	1-1
Benefits of Carrier Security .....	1-2
Resources for This Handbook.....	1-2
How the Handbook Is Organized.....	1-4
<b>CHAPTER 2. ENSURING PERSONNEL SECURITY .....</b>	<b>2-1</b>
Conducting Pre-Employment Screening.....	2-1
Understanding Driver's License Requirements for Transportation of Hazardous Materials .....	2-4
Identifying On-Site and En Route Employees.....	2-5
Implementing Personnel Communications Policies.....	2-6
Terminating Employment .....	2-6
Preventing and Responding to Workplace Violence .....	2-7
<b>CHAPTER 3. ASSURING SITE AND PACKAGE SECURITY.....</b>	<b>3-1</b>
Controlling Access .....	3-1
Protecting the Perimeter.....	3-3
Providing Security Officers .....	3-4
Controlling Packages .....	3-5
<b>CHAPTER 4. ASSURING EN ROUTE SECURITY .....</b>	<b>4-1</b>
Planning Transportation Operations .....	4-1
Ensuring Vehicle Security .....	4-2
Communicating.....	4-4
Complying with DOT Regulations .....	4-4
<b>CHAPTER 5. ESTABLISHING A CARRIER SECURITY PROGRAM.....</b>	<b>5-1</b>
Developing and Maintaining A Security Policy .....	5-2
Communicating and Collaborating .....	5-2
Providing Employee Security Training Programs .....	5-3
Reporting and Analyzing Incidents.....	5-4

## TABLE OF CONTENTS (Continued)

	<u>Page</u>
Using Technical Innovations .....	5-5
Investigating Security Breaches and Enforcing Discipline.....	5-6
Managing Incidents.....	5-7
Reassessing the Security Programs.....	5-8
<b>CHAPTER 6. ASSESSING SECURITY RISK FOR COMMODITIES.....</b>	<b>6-1</b>
Making a List of Commodity Chemicals .....	6-1
Ranking Chemical Hazard .....	6-2
Ranking Exposure .....	6-3
Prioritizing Transportation Security Risk .....	6-5
Reviewing Transportation Security Risk .....	6-7
 <b>APPENDIX A PERSONNEL SECURITY SAMPLE DOCUMENTS</b>	
 SAMPLE DRIVER'S APPLICATION FOR EMPLOYMENT.....	A-2
SAMPLE REQUEST FOR INFORMATION FROM PREVIOUS EMPLOYER.....	A-8
SAMPLE EMPLOYEE DISCLOSURE FORM .....	A-9
SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT.....	A-10
SAMPLE PRE-EMPLOYMENT SCREENING POLICY .....	A-11
SAMPLE WORKPLACE VIOLENCE POLICY .....	A-13
SAMPLE EMPLOYEE MISCONDUCT POLICY.....	A-14
 <b>APPENDIX B CARRIER SECURITY PROGRAM DOCUMENTS</b>	
 SAMPLE GUIDANCE ON SUSPICIOUS LETTERS AND PACKAGES.....	B-2
SAMPLE GENERAL WEAPONS POLICY .....	B-3
SAMPLE BOMB THREAT PROCEDURES .....	B-4
COMPACT, UNIFIED SECURITY POLICY AND PROCEDURES: SAMPLE 1 .....	B-8
COMPACT, UNIFIED SECURITY POLICY AND PROCEDURES: SAMPLE 2....	B-10
 <b>APPENDIX C DEPARTMENT OF TRANSPORTATION HAZARD CLASSIFICATIONS</b>	

## LIST OF TABLES

<b><u>Table No.</u></b>		<b><u>Page</u></b>
5-1	INCIDENT REPORTING INFORMATION .....	5-5
6-1	TRANSPORTATION SECURITY RISK RANKING.....	6-5
6-2	HOW TO RANK TRANSPORTATION SECURITY RISK.....	6-7
C-1	DOT HAZARD CLASSES .....	C-1

## LIST OF FIGURES

<b><u>Figure No.</u></b>		<b><u>Page</u></b>
1-1	CARRIER SECURITY MANAGEMENT PROGRAM: ASSURANCE MEASURES AND BENEFITS .....	1-3
4-1	EXCERPT FROM CFR 49 PART 397.....	4-6

## ABBREVIATION/ACRONYM LIST

CFR	Code of Federal Regulations
CRA	consumer reporting act
DOJ	Department of Justice
DOT	Department of Transportation
FCRA	Fair Credit Reporting Agency
FEI	Freberg Environmental, Inc.
INS	Immigration and Naturalization Service
LPG	liquid petroleum gas

## Preface

Years ago, carrier security was a phrase that most trucking firms did not use or they defined it in different ways. Large carriers formerly addressed security in terms of preventing theft to high value cargo or protecting deliveries in high crime areas. But the definition of security has taken on a new meaning. Large and small carriers now need to recognize existing exposures from a new perspective, and decide on steps to minimize these exposures. Owners and employees are becoming more alert to their surroundings using this new awareness. The threat of harm to a carrier, its cargo, and employees is more prevalent than ever in the hazardous carrier industry. This handbook offers common sense information to hazardous materials carriers. It compliments your experience in hazardous hauling and highlights small changes to every day operations. Carrier success is related to the recognition, understanding, and managing all aspects of security in the workplace.

While insurance companies are pioneering this new aspect of carrier operations, Freberg Environmental, Inc. has compiled examples from experts in the field and government entities that deal with carrier trucking risks. This handbook has been written to help you operate in a more secure environment.



We encourage you to read this handbook, and to think about exposures or situations that may be specific to your operation. Our intent is to provide a good basis for recognizing and managing security measures for hazardous materials and waste carriers. As this topic develops, carriers will be more prepared, more educated, and more likely to avoid costly claims or situations.

A handwritten signature in black ink that reads "Gayle A. Watson". The signature is written in a cursive style with a large initial "G".

Gayle Watson  
Senior Trucking Underwriter  
Freberg Environmental, Inc.

## About the Authors

Gayle Watson is a Senior Trucking Underwriter at Freberg Environmental, Inc., an environmental insurance underwriting agency based in Denver. She has over 18 years of insurance industry experience. Her work has included administration and underwriting. Ms. Watson began her career with TIG Insurance Company and has worked for USF&G and The St. Paul Companies. She has worked on standard commodity trucking programs and is responsible for underwriting hazardous materials trucking accounts. Ms. Watson completed the Insurance Institute of America Program in General Insurance and the Associate in Underwriting (AU) designation. She holds a Bachelor of Arts degree in English from the Metropolitan State College of Denver.

Avery Grimes has over 28 years of experience in the transportation industry including engineering, finance, operations, and environmental and emergency management. Mr. Grimes has served in senior management positions in the transportation industry and provides consulting services to a variety of United States and international transportation clients. His expertise includes emergency response planning and management, transportation risk assessment, transportation operations management, security risk

management, environmental engineering, and transportation economics. Mr. Grimes is published in the proceedings of the Bureau of Explosives, the Transportation Research Forum, and Contaminated Soils Conference Journal.

Mr. Grimes holds a Bachelor of Science degree in transportation and civil engineering from the University of Illinois and a Masters of Science in civil engineering from the University of Nebraska. He is a regular presenter at forums on emergency management and is a visiting lecturer at the University of Illinois. Mr. Grimes is a registered professional engineer and is on the faculty of University of Denver's Intermodal Transportation Institute where he lectures on a variety of transportation issues.

# CHAPTER 1. INTRODUCTION

In this handbook, Freberg Environmental, Inc. (FEI) provides guidelines for security issues related to truckers that transport hazardous materials. These guidelines reduce the risk of harm posed by distribution of hazardous materials to the general public, carriers, distributors, employees, and the environment. This handbook incorporates guidelines established by the Federal Motor Carrier Safety Administration.

This chapter provides information about Recognizing and Managing Carrier Security: A Handbook for Hazardous Material Transporters in the following sections:

- ◆ Who the Handbook Is For
- ◆ Benefits Of Carrier Security
- ◆ Resources for This Handbook
- ◆ How The Handbook Is Organized

## Who the Handbook Is For

This handbook is written for carrier owners and managers responsible for security at their sites and their transportation operations. The handbook helps carriers better manage their workplace and en route security, and in doing so, protect employees, the public, the environment, and the company. This handbook

addresses security for en route transportation of hazardous material shipments and at fixed facilities. The guidelines in this handbook can be implemented for a carrier security program.

## **Benefits of Carrier Security**

The benefits of a security program come from a reduced likelihood of large and small incidents. Both types of incidents can result in costly losses to the carrier. The cost of implementing a carrier security program is significantly less than the costs that may follow a major or even minor incident resulting from a security breach.

A carrier security program benefits the public, the environment, the carriers' employees, and the carrier. These benefits are listed in Figure 1-1.

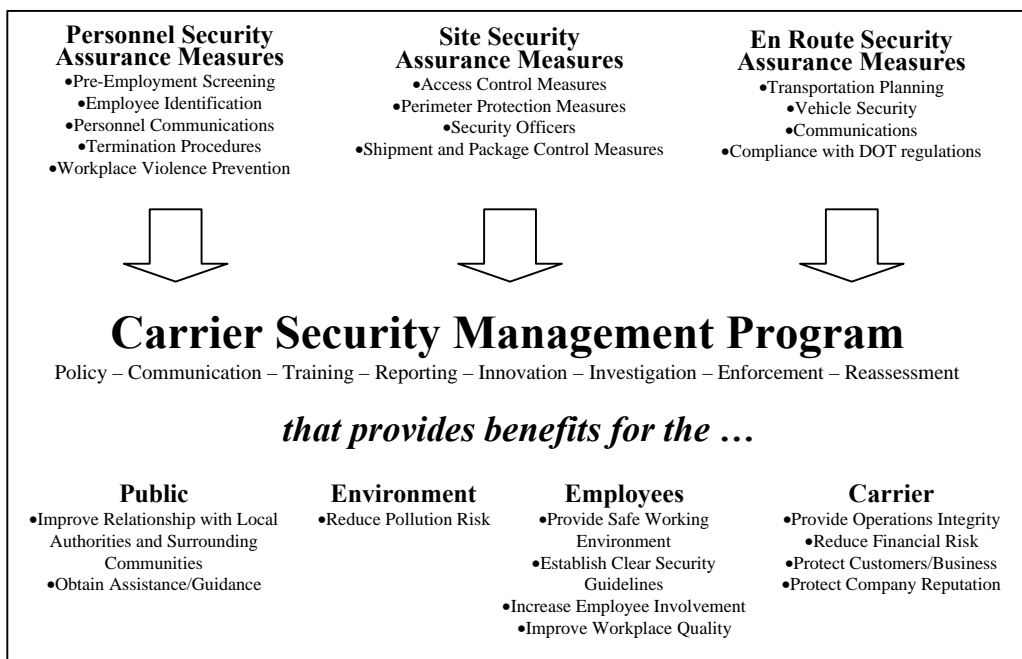
## **Resources for This Handbook**

Several aspects of this handbook are developed from the following resources:

- ◆ "Security Talking Points," Federal Motor Carrier Safety Administration (2001)
- ◆ "Site Security Guidelines for the U.S. Chemical Industry "by the American Chemistry Council (October 2001)

- ◆ "Transportation Security Guidelines for the U.S. Chemical Industry" by the American Chemistry Council (2001)
- ◆ Interviews with selected hazardous material transportation carriers
- ◆ Federal Motor Carrier Safety Administration
- ◆ Selected law enforcement officials

**Figure 1-1. Carrier Security Management Program: Assurance Measures and Benefits.**



## How the Handbook Is Organized

This handbook includes examples of types of activity carriers should evaluate for their security program, but does not include all

transportation security considerations for hazardous material transporters. The implementation of the guidelines vary according to the chemical being distributed, the mode and route of transportation, the activity involved, the type of vehicle, the size of the carrier, and the type of operations of the carrier.

Elements of a carrier security program vary depending on a number of considerations such as size, operational characteristics, and commodity hazards, but includes the following elements presented in this handbook:

- ◆ Ensuring Personnel Security
- ◆ Assuring Site and Package Security
- ◆ Assuring En Route Security
- ◆ Establishing a Carrier Security Program
- ◆ Assessing Security Risk for Commodities

Each of these elements are presented in the following chapters. Sample documents and reference information referenced in these chapters are provided in the following appendices:

- A. Personnel Security Sample Documents
- B. Carrier Security Program Documents
- C. Department of Transportation Hazard Classifications

Tables and figures referenced in the handbook appear as close as possible to where they are first referenced.

## CHAPTER 2. ENSURING PERSONNEL SECURITY

Personnel security management is a fundamental element of a company security program. Contractors including owner-operators used by the carrier should be required to screen their employees before they can access the carrier's facilities. Guidelines for personnel security are provided in the following subsections:

- ◆ Conducting Pre-employment Screening
- ◆ Understanding Driver's License Requirements for Transportation of Hazardous Materials
- ◆ Identifying On-Site and En Route Employees
- ◆ Implementing Personnel Communications Policies
- ◆ Terminating Employment
- ◆ Preventing and Responding to Workplace Violence

### Conducting Pre-Employment Screening

Stringent pre-employment screening is the most critical element of an effective carrier security program. To ensure that applicants do not pose a security risk, conduct thorough background record checks and in-depth face-to-face interviews of applicants for employment. Provide the following documents to the applicant to read and complete:



- ◆ Driver's License Application for Employment
- ◆ Request for Information from Previous Employer
- ◆ Employee Disclosure Form
- ◆ Summary of Your Rights Under the Fair Credit Reporting Act

Samples of these documents are provided in Appendix A along with a Sample Pre-Employment Screening Policy.

Conduct more detailed background record checks for applicants if any of the following suspicious indicators are found.

- ◆ Gaps in employment. Federal requirements require a 3-year employment review. FEI recommends that carriers conduct a 10-year employment review that includes direct communication with previous employers.
- ◆ Frequent job shifts. Frequent job shifts may indicate applicants with a potential for unstable behavior.
- ◆ Different names used by applicant. Carefully screen applicants who use different names or aliases. Include all aliases when conducting criminal background checks.
- ◆ Unsatisfactory military discharge.
- ◆ Non-United States (U.S.) citizenship. Consider lack of U.S. citizenship as a

significant indicator because of the difficulty in verifying non-U.S. employment history. Verify citizenship for all applicants and current employees. For noncitizens, verify that all immigration papers are on file at the Immigration and Naturalization Service (INS) office and properly documented.

- ◆ Frequent changes in residence. Moves from state to state could indicate a legal or driving history problem.
- ◆ Lack of or insufficient personal references. Review and contact personal references to verify accuracy of the references and evaluate applicant characteristics.
- ◆ Criminal history. Conduct a criminal background check for all applicants and all current employees. Consider significant and/or frequent infractions as a significant indicator for security concern. Criminal background checks vary in cost. Include all of the applicant's aliases in the request for a criminal background check.
- ◆ History of driver logbook violations. Evaluate all driver logbook violations. Disqualify any driver with a history of falsifying driver's logbook.



*Conduct face-to-face interviews with all applicants.*

Require the applicant to inform the carrier of any of these suspicious indicators. Confirm the correctness of his/her information so that the carrier can subsequently disqualify the applicant if a discrepancy is found.

Conduct face-to-face interviews to appraise the applicant's personality, character, motivation, honesty, integrity, and reliability. Psychological tests may be conducted by the carrier or third-party contractors.

Report any significant suspicious findings immediately to the local police, Department of Justice (DOJ), or Federal Bureau of Investigation office. Management may want to fingerprint and photograph all applicants to firmly establish a traceable identity record.



*DOT is implementing rules for the USAPATRIOT Act of 2001.*

## **Understanding Driver's License Requirements for Transportation of Hazardous Materials**

Section 1012 of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USAPATRIOT) Act of 2001" [Public Law 107-56, October 26, 2001] amends the Hazardous Materials Transportation Act. The amendment prohibits states from issuing or renewing a license to operate a motor vehicle transporting a hazardous material in commerce unless the Department of Transportation (DOT) has first determined that the applicant does not pose a security risk warranting denial of a license. It also requires the DOJ to perform a background records check on anyone requesting a license or renewal to transport hazardous materials. DOT

has not implemented full rulemaking for Section 1012.

## **Identifying On-Site and En Route Employees**

FEI recommends requiring photo identification badges for all employees, including drivers, handlers, supervisors, and management. Photo identification badges may also be considered for nonemployees who regularly use the carrier's facilities including maintenance contractors, interline carriers, shipper, or consignee personnel.

## **Implementing Personnel Communications Policies**

Include security topics in all safety meetings with employees and managers. Clearly post security-related policies in prominent locations at terminals and driver locker rooms. Obtain employee's signatures to acknowledge that they have read policies regarding carrier security. Record attendance meetings where important security topics are discussed. Place signed copies in drivers' personnel files.

## **Terminating Employment**

When terminating employees, observe the following guidelines.

- ◆ Treat the person with respect.
- ◆ Collect the employee's keys to the facility and vehicles and photo identification.
- ◆ Change locks that the employee may have had access to.
- ◆ Change computer passwords if appropriate.

For involuntary terminations, perform the following additional tasks.

- ◆ Assess the employee's violence potential before termination and, if appropriate, take additional security precautions.
- ◆ Escort the departing employee out of the facility.

## **Preventing and Responding to Workplace Violence**

Attempt to stop workplace violence before any employee is harmed or a threat develops to the company and/or the public. Take actions against threats and intimidation as well as actual violence.

Consider the following measures to prevent and respond to workplace violence.

- ◆ Adopt a policy of prohibiting (and responding to all reports of) physical violence, verbal abuse, willful destruction of company property, and intimidation.  
Consider suspending suspects from work

while the reports are investigated. Respond to confirmed reports with counseling, reprimands, or termination of employment.

- ◆ Teach employees how to recognize the early warning signs of a troubled or potentially violent person and how to respond.
- ◆ Require employees who have obtained court-issued restraining orders to notify management immediately. Managers can then take steps to protect all employees and can notify law enforcement of any violations.
- ◆ Limit former employees' access to the workplace as appropriate.
- ◆ Strictly enforce policies forbidding the use and possession of drugs at any time and the possession of alcohol and weapons at work.
- ◆ Train managers on appropriate ways to handle difficult employee terminations, layoffs, and discipline.
- ◆ After a violent incident, evaluate the potential for further violence at the facility.
- ◆ Help employees with the psychological consequences of workplace violence. Doing so not only is humane, but also helps reduce losses caused by absence, loss of productivity, and workers' compensation claims.
- ◆ Support prosecution of offenders by accommodating employees who are needed

for court appearances and cooperation with the prosecution.

- ◆ To avoid a defamation suit by accused employees who are acquitted, managers investigate allegations quickly and quietly.

Appendix A provides a sample policy on employee misconduct and workplace violence.

## **CHAPTER 3.     ASSURING SITE AND PACKAGE SECURITY**

Site and package security is an important consideration wherever hazardous materials are stored, trans-loaded, accumulated, transferred, or otherwise in the transportation process. This chapter provides guidelines for the following site and shipping security assurance elements in the following sections:

- ◆ Controlling Access
- ◆ Protecting the Perimeter
- ◆ Providing Security Officers
- ◆ Controlling Packages

### **Controlling Access**

Access controls are physical measures for managing the passage of personnel and vehicles into, out of, and within a facility. The level of access control varies from facility to facility. Control measures depend on the following variables:

- ◆ Number of employees
- ◆ Hazards of materials present
- ◆ Level of pedestrian and vehicular traffic into and out of the facility
- ◆ Degree to which facility operations are controversial



- ◆ Attractiveness of the facility as a target of various threats
- ◆ Proximity to populated areas
- ◆ Facility security history
- ◆ Law enforcement concerns

Although many access controls require employee involvement, managers should not inform employees of all of the security measures it uses. Some employees require a greater knowledge of security measures than other employees do. Include the following access controls in a carrier security program.

- ◆ Appropriate locks on interior and exterior doors, fences, and other passageways.
- ◆ Adequately lighted facility areas. Arrange access points, office areas, and storage areas so that unescorted visitors can be easily identified. Keep closets locked. Equip windows with appropriate locks and window bars.
- ◆ Require employees, contractors including owner-operators, and vendors to carry photo identification badges. If identification badges are not provided, treat these personnel as visitors who are required to check-in, show identification, carry visitor badges, and use an on-site escort. Obtain a list from contractors and vendors of approved personnel who are authorized to service the facility.

- ◆ Require all visitors to show identification, sign log-in sheets, carry visitor badges, and be escorted while within the facility.
- ◆ Install electronic access control systems that require the use of key cards at main entrances and on other appropriate doors that provides an audit trail of entrance and exit to various areas.
- ◆ Provide surveillance for loading and unloading areas for additional access controls. Install closed circuit television to monitor key areas of the facility. Use motion sensors to trigger video recording and alert security staff when someone enters a restricted area.
- ◆ Establish standard procedures to determine which cars, trucks, or other vehicles may enter the site, through which gates, docks or other entrances and for what purpose.

## Protecting the Perimeter



*Perimeter protection includes secure fences and gates.*

Perimeter protection measures include:

- ◆ Fences or buildings to secure hazardous materials storage areas.
- ◆ Bollards, trenches and "K-Rail" to prevent vehicles from driving into the facility at points others than official entrances.
- ◆ Vehicle gates equipped with retractable barriers.

- ◆ Setbacks from fence lines and clear zones established to eliminate hiding places near the site perimeter. Clear away bushes and weeds from both the inside and outside of the fence line to give a clear line of sight.
- ◆ Perimeter lighting so that employees and passersby can observe potential intruders.

## **Providing Security Officers**

Security officers provide a range of useful security services, such as touring a site to look for intruders or irregularities, staffing site entrances to check identification, maintain entry and exit logs, training employees and contractors on security policies, and assisting with emergencies. If security officers are deemed appropriate, consider the following questions to establish their responsibilities.

- ◆ Should the security staff tour the facility or remain at fixed posts, or both?
- ◆ Should the security staff be contract or in-house personnel?
- ◆ What level of training should the security officer be required to attain (i.e. first aid, cardio pulmonary resuscitation, emergency response, etc.)?
- ◆ What level of pro-active interaction should the security officer have with local police and fire departments?

### **How A Site Review Improved Access Control and Perimeter Protection**

XYZ Trucking, a hazardous materials trucking company, reviewed its facilities for security improvements following an alert issued by DOT and found the following deficiencies.

- The entrance gates to the material storage and truck parking areas were left open and unguarded during business hours,
- Weeds had grown up along the fence line
- The fence line had several openings where damage to fence and soil erosion occurred.
- Unidentified personnel were found in material storage areas filling vending machines

As a result of the review, the carrier made the following improvements.

- Gates were locked and a vehicle check-in system was instituted.
- The fence was repaired and weeds were pulled to provide a clear view of the site perimeter.
- Employees were provided identification cards to be worn at all times when on-duty and/or on the facility grounds. All visitors were required to sign-in, show identification, and restricted to noncritical areas. The vending machines were moved to the sign-in area that was visible to office personnel.

### **Controlling Packages**

Package control guidelines include the following.

- ◆ Implement standard procedures for control of packages and/or shipments. Educate all employees on package control procedures. Post package control procedures in prominent locations. Maintain records for the acceptance and removal of all hazardous materials to or from the facility.



*Drivers must attend loading and unloading.*

- ◆ Compare all shipping papers to the actual shipment being hauled by the carrier to ensure they match.
- ◆ Determine the authenticity of shippers by performing credit checks.
- ◆ Do not accept any hazardous material shipments from unfamiliar shippers.
- ◆ Conduct parcel inspections using magnetometers, X-ray screening, or explosives detectors where appropriate.
- ◆ Do not leave vehicles unattended during loading or unloading. Require drivers to verify observing the loading and unloading process and verify that the shipment matches the shipping papers or manifest.
- ◆ Equip containers with tamper-proof seals that are numbered. Compare seal numbers against documentation provided by the shipper. Immediately report any seals that have been removed or tampered with and inspect the shipment.

## CHAPTER 4. ASSURING EN ROUTE SECURITY

En route security assurance for all shipments, includes the following elements described in this chapter:

- ◆ Planning Transportation Operations
- ◆ Ensuring Vehicle Security
- ◆ Communicating
- ◆ Complying with DOT Regulations

### Planning Transportation Operations

When planning transportation operations, consider the following guidelines.

- ◆ Instruct drivers to use interstate highways and by-passes whenever feasible. Avoid travel in tunnels and on bridges. Regular shipments should have designated routes that avoid population centers where possible.
- ◆ Transport the shipment only in the trailer (or container) scheduled for the shipment. The manager in charge of the shipment must approve any changes in the vehicle to be used.
- ◆ Prohibit drivers from making unscheduled trips or performing any work not authorized by proper documentation such as a work order.

- ◆ Occasionally switch drivers on routes where practicable to reduce the potential for collusion with would-be hijackers.
- ◆ Require drivers to supply a deadhead ticket. Do not permit a "last load ticket" when a trucker deadheads back to the terminal.

## **Ensuring Vehicle Security**

To ensure vehicle security, consider the following guidelines.

- ◆ Consider guards for very high hazard shipments such as Department of Defense or radioactive shipments.
- ◆ Permit driver layovers only in well lit truck stops and require drivers to remain with units and have meals in open truck stops where they can observe the vehicle. Lock windows and doors whenever the vehicle is parked or when operating in potentially unsafe areas. Prohibit unauthorized personnel access to the vehicle. Inspect vehicles after each stop to ensure good mechanical condition and to identify suspicious objects that may have been attached to the vehicle.
- ◆ Enforce parking and attendance rules in the Federal Regulations 49 Code of Federal Regulations (CFR) Part 397.5.

## How A Security Review Improved En Route Security

XYZ Trucking reviewed their en-route security procedures following a DOT security alert and found the following deficiencies.

- On long-haul shipments, drivers were using interstate highway routes through several downtown areas because the highway connections were more direct and the mileage was shorter.
- Drivers contacted the dispatcher only after the shipment had been delivered.
- Drivers used public phones to contact the dispatcher.
- Drivers picked up extra shipments from customers without advance paperwork and notified the dispatcher after the pick-up

As a result of the review, this carrier made the following improvements:

- Long-haul shipments were routed around urban areas on belt highways. The carrier found that these alternative routes were faster than downtown route.
- Drivers were equipped with cell phones and were required to report to the dispatcher after every pick-up and delivery. The drivers could call customers before arrival and reduce the time needed to receive the shipment and prepare receiving papers.
- Drivers were required to call in to the dispatcher to obtain approval for handling extra shipments.
- Using the cell phones reduced delays in obtaining approvals. Obtaining this information in advance virtually eliminated errors in processing the carrier's shipment paperwork.

- ◆ Do not drop or interchange shipments except at terminals and/or other approved shipper/consignee sites.
- ◆ Require seals and/or locks on all valves and/or containers whenever the vehicle is involved in overnight transportation, or when the shipment is interchanged between carriers.



## Communicating

This section provides guidelines for communications for en route operations.

- ◆ Protect shipment information systems against access by unauthorized individuals.
- ◆ Equip drivers with cell phones or require them to check-in with dispatchers at pre-specified intervals.
- ◆ Notify shippers and consignees of when shipments are expected. If a shipment does not arrive within a timely fashion, the consignee or interchange carrier should immediately notify the delivering carrier.
- ◆ Prohibit drivers from discussing the nature of their shipment, the route or timing of transportation, or other aspects of the shipment with strangers or over the CB or other radio.

## Complying with DOT Regulations

Federal Requirements Pertaining to Attendance, Surveillance, Parking, and Fueling of Motor Vehicles involved in the Transportation of Hazardous Materials (CFR 49 Part 397) are significant to carrier security. An excerpt from CFR 49 Part 397 is provided in Figure 4-1.

## Figure 4-1. Excerpt from CFR 49 Part 397.

### §397.5 Attendance and surveillance of motor vehicles.

(a) Except as provided in paragraph (b) of this section, a motor vehicle which contains a Division 1.1, 1.2, or 1.3 (explosive) material must be attended at all times by its driver or a qualified representative of the motor carrier that operates it.

(b) The rules in paragraph (a) of this section do not apply to a motor vehicle which contains Division 1.1, 1.2, or 1.3 material if all the following conditions exist --

(b)(1) The vehicle is located on the property of a motor carrier, on the property of a shipper or consignee of the explosives, in a safe haven, or, in the case of a vehicle containing 50 pounds or less of a Division 1.1, 1.2, or 1.3 material, on a construction or survey site; and

(b)(2) The lawful bailee of the explosives is aware of the nature of the explosives the vehicle contains and has been instructed in the procedures which must be followed in emergencies; and

(b)(3) The vehicle is within the bailee's unobstructed field of view or is located in a safe haven.

(c) A motor vehicle which contains hazardous materials other than Division 1.1, 1.2, or 1.3, materials, and which is located on a public street or highway, or the shoulder of a public highway, must be attended by its driver. However, the vehicle need not be attended while its driver is performing duties which are incident and necessary to the driver's duties as the operator of the vehicle.

(d) For purposes of this section --

(d)(1) A motor vehicle is attended when the person in charge of the vehicle is on the vehicle, awake, and not in a sleeper berth, or is within 100 feet of the vehicle and has it within his/her unobstructed field of view.

(d)(2) A qualified representative of a motor carrier is a person who --

(d)(2)(i) Has been designated by the carrier to attend the vehicle;

(d)(2)(ii) Is aware of the nature of the hazardous materials contained in the vehicle he/she attends;

(d)(2)(iii) Has been instructed in the procedures he/she must follow in emergencies; and

(d)(2)(iv) Is authorized to move the vehicle and has the means and ability to do so.

(d)(3) A safe haven in an area specifically approved in writing by local, State, or Federal governmental authorities for the parking of unattended vehicles containing Division 1.1, 1.2, or 1.3 materials.

(e) The rules in this section do not relieve the driver from any obligation imposed by law relating to the placing of warning devices when a motor vehicle is stopped on a public street or highway. [59 FR 63925, Dec. 12, 1994].\

### Sec. 397.7 Parking.

(a) A motor vehicle which contains Division 1.1, 1.2, or 1.3 materials must not be parked under any of the following circumstances--

(1) On or within 5 feet of the traveled portion of a public street or highway;

(2) On private property (including premises of fueling or eating facility) without the knowledge and consent of the person who is in charge of the property and who is aware of the nature of the hazardous materials the vehicle contains; or

(3) Within 300 feet of a bridge, tunnel, dwelling, or place where people work, congregate, or assemble, except for brief periods when the necessities of operation require the vehicle to be parked and make it impracticable to park the vehicle in any other place.

(b) A motor vehicle which contains hazardous materials other than Division 1.1, 1.2, or 1.3 materials must not be parked on or within five feet of the traveled portion of public street or highway except for brief periods when the necessities of operation require the vehicle to be parked and make it impracticable to park the vehicle in any other place. [59 FR 63925, Dec. 12, 1994]

### §397.15 Fueling.

When a motor vehicle which contains hazardous materials is being fueled --

(a) Its engine must not be operating; and

(b) A person must be in control of the fueling process at the point where the fuel tank is filled.

## **CHAPTER 5. ESTABLISHING A CARRIER SECURITY PROGRAM**

Assign a primary manager responsible for security management. When a carrier has multiple facilities, designate an employee responsible for security at each facility. Senior management is responsible for security and has the following security-related roles described in this chapter:

- ◆ Developing and maintaining a security policy
- ◆ Communicating and collaborating
- ◆ Providing employee security training programs
- ◆ Reporting and analyzing incidents
- ◆ Using technical innovations
- ◆ Investigating security breaches and enforcing policy
- ◆ Managing incidents
- ◆ Reassessing the security program

### **Developing and Maintaining a Security Policy**

Employees are more likely to understand and support the carrier's security effort if they see it as a carrier priority that is supported by senior management. One of the best ways to communicate the security effort and demonstrate management support is to develop and

communicate official carrier policies regarding security.

Develop security policies on a carrier-wide basis because of the nature of the transportation network. Drivers and shipments may interact with more than one facility and a comprehensive carrier-wide policy reduces potential confusion associated with differing policies at different locations. Security is often called a function of the weakest link, and a comprehensive security system minimizes the number of "weak links." Appendix B contains sample policies related to a security program.

## Communicating and Collaborating



*Include security issues in every meeting where safety is discussed.*

Establish relationships with local, state, and federal law enforcement and other public safety agencies such as Local Emergency Planning Committees. Network with other hazardous material carriers to discuss potential security threats and rational methods of response. Become acquainted with the security officer or a manager with similar responsibilities for major shippers and consignees.

Provide shippers and consignees with updated lists of employees authorized to pick-up and deliver hazardous material shipments.

Communicate security risks and concerns

identified by employees to management and among employees.

## **Providing Employee Security Training Programs**

Employees serve as the first line of communication and response in a carrier security program. Employees can be trained to provide a natural security surveillance system. Include the following topics in a security-training program:

- ◆ A discussion of the types of hazards, exposures, and security risks related to carrier operations
- ◆ Review of security existing policies and those being considered by the carrier
- ◆ Procedures/instructions to identify a potential security threat or incident
- ◆ How to identify a suspicious shipment or package
- ◆ Actions in response to potential and actual security threats:
  - Reporting incidents, incident reporting requirements and contact numbers
  - Procedures to address people not wearing proper identification
  - Alternatives available for drivers operating en route when suspicious activities occur
  - Personal protective measures

Maintain attendance logs of meetings where security topics and policies are discussed. Forgetfulness or "I didn't know" responses do not excuse violations of security policy.

## **Reporting and Analyzing Incidents**

Keep records of security incidents. The security manager may be able to identify trends and needed corrective actions through use of these records. Incident data can then be available for analysis in a consistent and timely manner. Reportable incident information is listed in Table 5-1.

## **Using Technical Innovations**

Consider the following technical innovations to support a carrier security program:

- ◆ Satellite tracking systems that send periodic signals or emails to dispatcher computers that includes the location of the vehicle such as a system manufactured by QualCom
- ◆ Tamper proof locking mechanisms for 5<sup>th</sup> wheels if the tractor and trailer are not regularly separated
- ◆ Blanket alarms for shipment is not otherwise transported in a secure and locked container
- ◆ Electronic engine controls that require a code to start a vehicle in addition to a key

**Table 5-1. Incident Reporting Information.**

<b>Type of Information</b>	<b>Description</b>
Identification of the responder	Name Association (facility name, truck identification, supervisor) Means of contact (telephone number, radio frequency, etc.)
Types of Security Incident	Immediate threat to personnel, facility, vehicle, etc. Unauthorized personnel in secure areas Lost or stolen cargo Perimeter activity Access breach (fence break-in, lock removal, etc.) Cargo tampering (seal removal, tampering, etc.) Suspicious cargo notification Information theft Shipper or carrier notification
Location of Security Violation	Name of facility, truck number, street address, city, highway milepost, etc.
Date and Time	Include when discovered if actual time is unknown.
Affect on operations	Impact on facility operation, truck operation, shipper or consignee facility
Shipments involved	Shipper name, chemical involved, manifest number
Resources required to respond	Fire, ambulance, law enforcement
Initial actions taken	Agencies responding, replacement of locks or fencing, trespassers secured, etc.
Initial notifications made	Police/Fire, Shipper/Consignee, etc.
Other Information	Map of incident site, corrective action taken, follow-up investigation personnel and findings.

### **Investigating Security Breaches and Enforcing Discipline**

Investigate breaches of company security policy and suspicious incidents. Some incidents may warrant only a cursory investigation by the facility security manager. Refer potentially serious incidents/breaches to law enforcement.

Investigate the following security incidents:

- ◆ Trespassing or otherwise unauthorized entrance by personnel in restricted areas
- ◆ Package or shipment loss or theft
- ◆ Breach of access control systems (locks, gates, fences, etc.)
- ◆ Cargo tampering
- ◆ Information theft

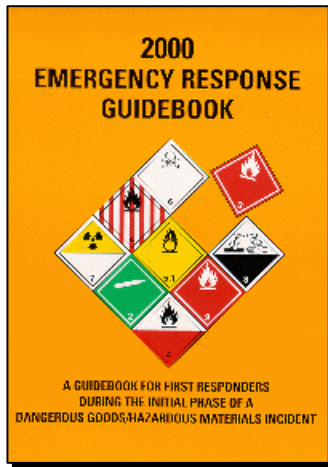
Enforcement of discipline guidelines and policy is essential to general employee morale and compliance with all carrier policies. Enforce discipline for all incidents involving a proven breach of security policy by an employee, vendor, and contractor including an owner/operator.

Contact contractor and/or vendor management if their employees violate carriers' security policies. Ban the offending employee from the carrier's facilities. If their employee commits a second violation, consider terminating the contract or business arrangement.

## **Managing Incidents**

Proper incident management may prevent an intrusion or attack from becoming a major incident. Consider the following incident management measures.





*DOT provides emergency response guidelines for hazardous commodities.*

- ◆ Identify high hazard shipments that should be reported immediately to law enforcement agencies in the event of loss, theft, or other loss of control.
- ◆ Develop an emergency response plan that fits the carrier's needs and resources.
- ◆ Develop a system to account for employees and visitors during emergencies.
- ◆ Attempt to control the incident so that evidence will be preserved for later investigations.
- ◆ Develop an incident communications system.

## **Reassessing the Security Programs**

Security programs are dynamic to identify and respond to changing risk conditions. Personnel come and go, facility layouts are modified, customers and shipments change, routes change, and various threats come and go. Review the following elements of the carrier security program on a regular basis and when significant changes occur involving threats, shipments, or facilities:

- ◆ Security risk assessment for commodities
- ◆ Site security surveys including layout, access controls, perimeter controls
- ◆ Communication plan
- ◆ Compliance with security procedures
- ◆ Evaluation of procedure effectiveness

## **CHAPTER 6. ASSESSING SECURITY RISK FOR COMMODITIES**

Security risk assessment is important in developing a security program for hazardous material carriers. Risk assessment consists of the following tasks described in this chapter:

- ◆ Making a List of Commodity Chemicals
- ◆ Ranking Chemical Hazard
- ◆ Ranking Exposure Risk
- ◆ Prioritizing Transportation Security Risk
- ◆ Reviewing Transportation Security Risk

### **Making a List of Commodity Chemicals**

Make a list of the chemicals handled and transported. Include the type of container and vehicle used to transport the chemicals, the location characteristics of the shipments (metropolitan areas, type of roads used, geography, etc.). Include the DOT classification system for the chemical. DOT created a hazard classification system that includes placards. These DOT classifications and placard information are presented in Appendix C.

### **Ranking Chemical Hazard**

Chemical hazard is ranked by the inherent chemical nature of the commodity. Chemicals hazard ranking can be as fundamental as the

U.S. DOT system (see Title 49 Code of Federal Regulations, Part 173.2(a), in particular, Table 1 in 49 CFR 172.504). Other ranking systems can be developed upon multiple factors such as the following factors:

- ◆ Flammability
- ◆ Explosivity
- ◆ Toxicity
- ◆ Vapor Pressure
- ◆ Reactivity
- ◆ Corrosivity

### **How To Rank Chemical Hazard Risk**

XYZ Trucking decided it should rank the chemical hazards of the commodities carried by developing a security risk exposure rank for each of their following commodities.

- The gasoline, diesel fuel, and waste oil were transported between bulk storage facilities located in an industrial area to various urban delivery points. The gasoline and diesel fuels were transported on frequent and regular schedules.
- Liquid Petroleum Gas (LPG) originated at the same bulk storage facility but was delivered to several outlying points at rural locations on an "as-needed" basis.
- Chlorine originated at a chemical plant located in an industrial area and was normally delivered to several urban water treatment facilities on a scheduled basis.
- Industrial cleaning products were boxed and palletized and transported between chemical plants and warehouses, all located in industrial areas.

The carrier decided to rank the relative chemical hazards using three categories: High, Medium, and Low.

- Waste oil was classified as a low hazard because of very low flammability rating and no other significant chemical hazard factors.
- LPG was classified as a high chemical hazard because of high flammability and its potential to generate a major explosion.

- Gasoline was classified as a medium chemical hazard because it is not considered as dangerous as LPG but is still a highly flammable liquid.
- Diesel fuel was classified as a low chemical hazard because of its relatively low flammability rating.
- Chlorine was classified as a high chemical hazard because it is a highly toxic material with a low exposure limit.
- Industrial cleaning products were classified as a medium chemical hazard because of high flammability and high corrosivity.

In summary, the carrier classified the chemical hazard risk for each of its commodities as follows:

- Low Chemical Hazard - Waste Oil, Diesel Fuel
- Medium Chemical Hazard - Gasoline, Industrial Cleaning Products
- High Chemical Hazard - LPG, Chlorine

## Ranking Exposure

After commodity chemicals are listed and their hazard ranked, develop an exposure ranking system that will evaluate the potential exposure to the public and the environment. Exposure risk is the potential of a given chemical hazard to actually harm the public or the environment if it is released in an uncontrolled manner.

Consider the following factors in ranking exposure risk:

- ◆ Predictability of shipment timing that might permit a hijacker to know when and where to intercept a shipment
- ◆ Number of shipments
- ◆ Shipment distance
- ◆ Chemical volume per shipment
- ◆ Bulk versus nonbulk shipments

- ◆ Proximity to population centers
- ◆ Proximity to public events
- ◆ Proximity to significant landmarks
- ◆ Proximity to sensitive environmental areas

When ranking exposure risk, focus on shipments that may be prone to deliberate acts of sabotage or terrorism, for example explosives and other highly hazardous chemicals.

### **Ranking Commodity Exposure Risk**

After ranking the chemical hazard risks of its shipments, XYZ Trucking then decided to rank the exposure risks using the simple High-Medium-Low method in the following manner:

- The waste oil was classified as a medium exposure risk because it was transported in urban areas on an intermittent basis.
- The diesel fuel and gasoline were classified as a high exposure risk because they are transported in urban areas on a regularly scheduled (and therefore predictable) basis.
- LPG was classified as a medium exposure risk because it is transported in industrial and rural areas on an intermittent basis.
- Chlorine was classified as a high exposure risk because it is transported in urban areas on a predictable basis.
- Industrial cleaning products were classified as a low exposure risk because they are transported in industrial areas in small volume non-bulk packages.

In summary the carrier classified the exposure risk for each of its commodities as follows:

- Low Exposure Risk - Waste Oil, Industrial Cleaning Products
- Medium Exposure Risk - LPG
- High Exposure Risk - Gasoline, Diesel Fuel, Chlorine

## Prioritizing Transportation Security Risk

After chemical hazard risk and exposure risk are ranked for each commodity, combine them into a single table to determine each commodity's relative overall transportation security risk. Use the High-Medium-Low method to prioritize both chemical hazards and exposure risks, to develop the overall transportation security shown in Table 6-1.

**Table 6-1. Transportation Security Risk Ranking.**

<b>Chemical Hazard Ranking</b>	High	<b>3</b>	<b>4</b>	<b>5</b>
	Medium	<b>2</b>	<b>3</b>	<b>4</b>
	Low	<b>1</b>	<b>2</b>	<b>3</b>
	Low	Medium	High	
	<b>Exposure Ranking</b>			

Shipments that are classified as high for both chemical hazard and exposure risk receive the highest risk ranking of 5.

Shipments that have a medium exposure risk and a high chemical hazard risk receive the next highest risk ranking of 4. This prioritization continues on until shipments with a low exposure risk and a low chemical hazard risk receive the lowest overall security risk ranking of 1.

## Ranking Commodity Security Risks

To rank its commodity security risk, XYZ Trucking, combined the chemical hazard ranking and exposure rankings. The chemical hazard and exposure rankings were then combined in Table 6-2.

**Table 6-2. How To Rank Transportation Security Risk.**

<b>Chemical Hazard Ranking</b>	High	<b>3</b>	<b>4 LPG</b>	<b>5 Chlorine</b>
	Medium	<b>2 ICP</b>	<b>3</b>	<b>4 Gasoline</b>
	Low	<b>1 Waste Oil</b>	<b>2</b>	<b>3 Diesel Fuel</b>
		Low	Medium	High
		<b>Exposure Ranking</b>		

This process then allowed XYZ Trucking to rank its overall transportation security risks as follows:

- 5 - Highest - Chlorine
- 4 - Medium High - Gasoline, LPG
- 3 - Medium - Diesel Fuel
- 2 - Medium Low - Industrial cleaning products
- 1 - Low - Waste Oil

## Reviewing Transportation Security Risk

Once transportation security risks are prioritized, security risk reviews should review those shipments with the highest risk rank. Once the highest shipment risks have been reviewed, then lower ranked shipment risks can be reviewed.

Involve a team of personnel responsible for different aspects of the shipment and with

different expertise with the security risk review. Include threat assessment and vulnerability assessment in the security risk review.

Threat assessment may include events such as:

- ◆ Attack on the physical property such as vehicles and fixed facilities
- ◆ Theft of property
- ◆ Product contamination or tampering
- ◆ Container tampering

Vulnerability assessment considers aspects of shipments that cause them to be more or less vulnerable to identified threats. Consider the following characteristics of shipments to assess vulnerability:

- ◆ Type of equipment and equipment design
- ◆ Route(s) of shipment through areas of concern
- ◆ Communication systems between driver
- ◆ Driver attendance in transit
- ◆ Driver procedures in transit (i.e., inspection of equipment)
- ◆ Security of temporary storage areas
- ◆ Special equipment (i.e., theft protection devices, 5<sup>th</sup> wheel locking systems, tamper proof seals and fittings)
- ◆ Communication of shipment routes, timing, and contents between carrier, shipper, and consignee



### **Reducing Commodity Security Risk**

After conducting the transportation security risk ranking for each type of shipment, XYZ Trucking conducted a security risk review of its chlorine shipments that resulted in the following actions:

- Working with customers to reduce the shipment predictability
- Providing drivers with cell phones and security training
- Coordinating with local law enforcement agencies to identify transportation routes with lower exposure to the public

RECOGNIZING AND MANAGING  
CARRIER SECURITY:  
A HANDBOOK FOR HAZARDOUS  
MATERIAL TRANSPORTERS

---

---

*APPENDIX A*

---

---

PERSONNEL SECURITY SAMPLE  
DOCUMENTS

## **APPENDIX A**

### **Personnel Security Sample Documents**

This appendix contains the following documents related to personnel security:

- ◆ Sample Driver's Application for Employment
- ◆ Sample Request for Information from Previous Employer
- ◆ Sample Employee Disclosure Form
- ◆ Summary of Your Rights Under the Fair Credit Reporting Act
- ◆ Sample Pre-employment Screening Policy\*
- ◆ Workplace Violence Policy\*\*
- ◆ Sample Employee Misconduct Policy\*

\* Adapted from, "Site Security Guidelines for the U.S. Chemical Industry" by the American Chemistry Council.

\*\* Adapted from, "Combating Workplace Violence" by the Defense Personnel Security Research Center for the International Association of Chiefs of Police."

## SAMPLE DRIVER'S APPLICATION FOR EMPLOYMENT

(COMPANY'S NAME, ADDRESS, CITY, STATE, ZIP, PHONE)

In compliance with Federal and State equal employment opportunity laws, qualified applicants are considered for all positions without regard to race, color, religion, sex, national origin, age, marital status, or non-job related disability.

Date: \_\_\_\_\_

### PERSONAL INFORMATION

Name: \_\_\_\_\_ Social Security Number: \_\_\_\_\_

Aliases or AKA: \_\_\_\_\_

Address: \_\_\_\_\_

Street \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Date of Birth: \_\_\_\_\_ Home Phone Number: \_\_\_\_\_

Can you provide proof of age? \_\_\_\_\_ Cell Phone Number: \_\_\_\_\_

In case of emergency Notify: \_\_\_\_\_

Name \_\_\_\_\_ Phone Number (Area Code) \_\_\_\_\_

Addresses for the last TEN YEARS:

Street \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Street \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Street \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Street \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Do you have a legal right to work in the US?: \_\_\_\_\_

Status of Immigration Papers? (if applicable): \_\_\_\_\_

Current Drivers License Number: \_\_\_\_\_ State of Issuance: \_\_\_\_\_

Issued on: \_\_\_\_\_ Expires on: \_\_\_\_\_

License Type: \_\_\_\_\_ List CDL Endorsements: \_\_\_\_\_

Last state licensed in: \_\_\_\_\_ Reason for new license: \_\_\_\_\_

Have you ever been denied a permit, license, or privilege to operate a commercial vehicle?: \_\_\_\_\_

If yes, explain: \_\_\_\_\_

Has your license ever been revoked or suspended?: \_\_\_\_\_  
If yes, explain: \_\_\_\_\_

Have you worked for this company before?: \_\_\_\_\_ If yes, position & location?: \_\_\_\_\_

Dates: \_\_\_\_\_ Reason for Leaving?: \_\_\_\_\_

Are you currently employed?: \_\_\_\_\_ If yes, when will you be available?: \_\_\_\_\_  
If no, how long since leaving last employment?: \_\_\_\_\_

Who referred you?: \_\_\_\_\_ Rate of pay expected?: \_\_\_\_\_

**DRIVING INFORMATION (if none, write in "None")**

<u>Power Equipment</u>	<u>(mark yes)</u>	<u>Type of Trailers</u>	<u>Years of Experience</u>	<u>States Driven In</u>
Tractor _____		Van _____		
Straight Truck _____		Tanker _____		
School Bus _____		Flatbed _____		
Coach Bus _____		Hopper _____		
Other (specify): _____				
_____				

Do you have full knowledge of the Federal Motor Carrier Safety Regulations? \_\_\_\_\_

When was your last training class?: \_\_\_\_\_

List courses, certificates, training, etc. (applicable to job): \_\_\_\_\_  
\_\_\_\_\_

Which safe driving awards do you hold and from whom? : \_\_\_\_\_

List any special equipment or technical materials you know or have worked with (other than those already listed): \_\_\_\_\_

**ACCIDENTS IN LAST THREE YEARS**

(Attach a sheet if more space is needed) If none, write in "None."

Date	Nature of Accident	# Fatalities	# Injuries	Commercial Unit	Personal Unit
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____



**Employer:** \_\_\_\_\_ Dates: From: \_\_\_\_\_ To: \_\_\_\_\_  
Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_  
Address: \_\_\_\_\_ Position: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_  
Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**Employer:** \_\_\_\_\_ Dates: From: \_\_\_\_\_ To: \_\_\_\_\_  
Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_  
Address: \_\_\_\_\_ Position: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_  
Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**Employer:** \_\_\_\_\_ Dates: From: \_\_\_\_\_ To: \_\_\_\_\_  
Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_  
Address: \_\_\_\_\_ Position: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_  
Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**Employer:** \_\_\_\_\_ Dates: From: \_\_\_\_\_ To: \_\_\_\_\_  
Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_  
Address: \_\_\_\_\_ Position: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_  
Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**Employer:** \_\_\_\_\_ Dates: From: \_\_\_\_\_ To: \_\_\_\_\_  
Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_  
Address: \_\_\_\_\_ Position: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_  
Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**Employer:**

Dates: From: \_\_\_\_\_ To: \_\_\_\_\_

Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_

Address: \_\_\_\_\_ Position: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_

Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**Employer:**

Dates: From: \_\_\_\_\_ To: \_\_\_\_\_

Name: \_\_\_\_\_ Mo. \_\_\_\_ Yr. \_\_\_\_ / Mo. \_\_\_\_ Yr. \_\_\_\_

Address: \_\_\_\_\_ Position: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_ Wage/Salary: \_\_\_\_\_

Contact Person: \_\_\_\_\_ Phone Number: \_\_\_\_\_  
(Area Code)

Reason for Leaving: \_\_\_\_\_

**NOTICE TO APPLICANT**

Applicant - If employer has not explained or given a job description, make sure one is given to you and that you fully understand what is expected of you prior to answering the following two questions:

Is there any reason you might be unable to perform the functions of the job for which you have applied?

If yes, explain: \_\_\_\_\_  
\_\_\_\_\_

**TO BE READ AND SIGNED BY APPLICANT**

This certifies that this application was completed by me, and that all entries on it and information in it are true and complete. I understand that any blanks left on this application can disqualify my candidacy for employment. I agree and understand that any misrepresentations of information given above shall be considered an act of falsification. I authorize you to make such investigations and inquiries regarding my background, and ascertain any and all information concerning my employment is factual. I agree and understand that in the event of employment, I will be on a probationary period during which time I may be discharged without recourse. I understand, also, that I am required to abide by all rules and regulations of the Company.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Applicant's Signature



**OFFICE USE ONLY - PROCESS RECORD**

Applicant Hired: \_\_\_\_\_ Rejected: \_\_\_\_\_

Date Employed: \_\_\_\_\_ Location Employed: \_\_\_\_\_

Department: \_\_\_\_\_ Classification: \_\_\_\_\_

(If rejected, summary report of reasons should be placed in file.)

1. Application Complete? \_\_\_\_\_

2. Interview (comments): \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

3. Criminal background, accidents, violations acceptable? \_\_\_\_\_  
\_\_\_\_\_

4. Previous Employers Contacted?

Date	Person Contacted	Results
_____	_____	_____
_____	_____	_____
_____	_____	_____

5. Written Exam? \_\_\_\_\_

Date	Given By	Results/Score
_____	_____	_____

6. Road Test? \_\_\_\_\_

Date	Given By	Results/Score
_____	_____	_____

Signature of Interviewing Officer: \_\_\_\_\_

\_\_\_\_\_ Date

**TERMINATION OF EMPLOYMENT**

Date Terminated: \_\_\_\_\_ Department Released From: \_\_\_\_\_

Dismissed: \_\_\_\_\_ Voluntarily Quit: \_\_\_\_\_ Other: \_\_\_\_\_

Termination Report in File: \_\_\_\_\_ Date: \_\_\_\_\_ Signature of Officer: \_\_\_\_\_

## SAMPLE REQUEST FOR INFORMATION FROM PREVIOUS EMPLOYER

I hereby authorize you to release the following information to:

(COMPANY NAME)

For the purposes of investigation as required by Section 391.23 of the *Federal Motor Carrier Safety Regulations*, you are released from any and all liability which may result from furnishing such information.

Date: \_\_\_\_\_ Applicant's Signature: \_\_\_\_\_  
\_\_\_\_\_

Mail To: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Dear Sir/Madam:

The below named individual has made an application to this company for a position as a driver. He states that he worked for you from \_\_\_\_\_ to \_\_\_\_\_.

We appreciate your time in completing, in confidence, the information requested below. Enclosed is a business reply envelope for your convenience. Thank you for your courtesy.

Sincerely,

(NAME OF INDIVIDUAL)  
Director of Safety

Applicant: \_\_\_\_\_ Social Security Number \_\_\_\_\_

Employed From: \_\_\_\_\_ to \_\_\_\_\_

What kind of vehicle did he drive for you? \_\_\_\_\_

Any accidents, preventable or not? \_\_\_\_\_

Reason he left your employ? \_\_\_\_\_ Resigned \_\_\_\_\_ Discharged \_\_\_\_\_ Lay Off

Any other remarks: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**SAMPLE EMPLOYEE DISCLOSURE FORM**  
*(Including summary of rights under Fair Credit Reporting Act)*

-

In connection with my application for employment (including contract for services) with you, I understand that consumer reports which may contain public record information may be requested from a consumer reporting agency (CRA). These reports may include the following types of information: names of previous employers, dates of employment, reason for termination of employment, work experience, accidents, etc. I further understand that such reports may contain public record information concerning my driving record, worker's compensation claims, credit, bankruptcy proceedings, criminal records, etc. from federal, state, and other agencies which maintain such records; as well as information from the CRA concerning previous driving record requests made by others from such state agencies, and state provided driving records.

I understand that I have the right to make a request to any CRA, upon proper identification, requesting the nature and substance of all information in its files on me at the time of my request, including the source of information, and the recipients of any reports on me which the CRA has previously furnished within the five year period preceding my request. In the event that the information from examination of these records is utilized in making an adverse decision with regard to my potential employment, before making the adverse decision, (COMPANY NAME) will provide you with a copy of the report and description, in writing, of my rights under the Federal Fair Credit Reporting Act. I hereby consent to (COMPANY NAME) in obtaining the above information from any CRA, and I agree that such information which any CRA has or obtains, and my employment history with you if I am hired, may be supplied by the CRA to other companies which subscribe to the CRA's services.

**EMPLOYEE AUTHORIZATION**

I AUTHORIZE, WITHOUT PRESERVATION, ANY PARTY OR AGENCY CONTACT BY (COMPANY'S NAME HERE), OR AN AGENT OF (COMPANY'S NAME HERE) TO FURNISH THE ABOVE-MENTIONED INFORMATION.

I hereby authorize procurement of consumer report(s), if hired (or contracted), this authorization shall remain on file and shall serve as ongoing authorization for you to secure consumer reports at any time during my employment (or contract) period. Any reproduction of this document shall be as valid as the original.

\_\_\_\_\_  
Print Your Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date of Birth

\_\_\_\_\_  
Social Security Number

\_\_\_\_\_  
CDL # and State Issued In

\_\_\_\_\_  
Today's Date

## SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) is designed to promote accuracy, fairness, and privacy of information in the files of every Consumer Reporting Agency (CRA). Most CRA's are credit bureaus that gather and sell information about you - such as where you work and live, if you pay your bills on time, and whether you have been sued, arrested, or filed for bankruptcy - to creditors, employers, and other businesses. Other CRA's gather information about employment related matters including acts of theft or dishonesty, and sell that information to prospective employers. The FCRA gives you specific rights in dealing with CRA's, and requires CRA's to provide you with a summary of these rights as listed below. You can find a complete text of the FCRA, 15 U.S.C. 1681 et seq., at the Federal Trade Commission's web site (<http://www.ftc.gov>).

- You must be told if information in your file has been used against you. Anyone who uses the information from a CRA to take action against you - such as denying an application for credit, insurance, or employment - must give you the name, address and phone number of the CRA that provided the report.
- You can find out what is in your file. A CRA must give you all the information in your file, and a list of everyone who has requested it recently. There is no charge for the report if your application was denied because of information supplied by the CRA, and if you request the report within 60 days of receiving the denial notice. You are also entitled to one free report per year if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you a fee of up to eight dollars.
- You can dispute inaccurate information with the CRA. If you tell a CRA that your file information contains inaccurate information, the CRA must reinvestigate the items (usually within 30 days) unless your dispute is frivolous. The CRA must pass along to its source all relevant information you provided. The CRA also must supply you with written results of the investigation and a copy of your report, if it has changed. If an item is altered or deleted because you dispute it, the CRA cannot place it back in your file unless the source of the information verifies its accuracy and completeness, and the CRA provides you a written notice that includes the name, address, and phone number of the source.
- Inaccurate information must be deleted. A CRA must remove inaccurate information from its files, usually within 30 days after you dispute its accuracy. The largest credit bureaus must notify other national CRA's if items are altered or deleted. However, the CRA is not required to remove data that is accurate unless it is outdated or cannot be verified.
- You can dispute inaccurate items with the source of information. If you tell anyone - such as a creditor who reports to a CRA - that you dispute an item, they may not then report the information to a CRA without including a notice of your dispute. In addition, once you have notified the source of the error in writing, they may not continue to report it if it is in fact an error.
- Outdated information may not be reported. In most cases, a CRA may not report negative information that is more than seven years old.
- Access to your file is limited. A CRA may provide information about you only to those who have a need recognized by the FCRA - usually to consider an application you have submitted to a creditor, insurer, employer, landlord, or other business.
- Your consent is required for all reports that are provided to employers. A CRA may not report to your employer, or prospective employer, about you without your written consent.
- You may seek damages from violators. You may sue a CRA or other party in state or federal court for violations of the FCRA. If you win, the defendant may have to pay damages and reimburse you for attorney fees. If you lose and the court specifically finds you sued in bad faith, you and your attorney may have to pay the defendant's fees.

You may have additional rights under state law. You may wish to contact a state or local consumer protection agency or a state attorney general to learn those rights. Please be sure to include the report date, your name, social security number, and your signature. Request for corrections submitted by persons purporting to act on your behalf can only be accepted if they contain your written authorization.

The FCRA gives several different federal agencies authority to enforce the FCRA. For additional questions or concerns regarding CRAs and/or the FCRA, you may contact the Federal Trade Commission, Bureau of Consumer Protection - FCRA Washington, DC 20580 - (202) 326-3430.

## SAMPLE PRE-EMPLOYMENT SCREENING POLICY

It is standard [Company Name] practice to require pre-employment background screening, as specified below, as a means of verifying applicant data prior to hire. This standard applies to regular and non-regular employments, including rehires where the separation period is more than 30 days. Pre-employment background screening is required for all rehires into designated positions regardless of the duration of the separation period.

It is intended that background checks will be made after reaching a decision to offer employment following the usual candidate review process.

Failures to disclose and discrepancies between the employment application and a background report will be reviewed and evaluated by HR. HR will consult with Security and Labor/Employment Law as appropriate. Any additional investigation will be conducted by [Company Name] Security or the company's designated third-party background screening agency. Criteria for evaluating background reports are set out below, following the background screening matrix. Copies of all investigative reports should be retained in the candidate's file.

Any decision on employment, or on discipline or termination of a current employee, as a result of information generated by the background checks should be reviewed for consistency and endorsed by [Company Name] Recruiting & Employment, Security, and Labor/Employment Law.

### **Waiver Provision**

Hiring an individual prior to completion of pre-employment background screening is discouraged. However, where it is deemed necessary due to business necessity, approval may be authorized by the hiring organization's senior management following endorsement by Security and HR. In such cases, the individual's employment will be conditioned on completion of the pre-employment background screening and evaluation process. No exceptions to pre-employment background screening involving designated positions are permitted.

In considering conditional employment arrangements due to business necessity (typically restricted to executives), organizations should balance operational needs against other considerations/exposures to the company. Because candidate disqualification due to background problems occur regularly, at least the following issues should be considered before early hire is approved:

1. In almost all cases, if there is a problem, it will be impractical to attempt to recover relocation costs, e.g., home search, new hire loan, home sale/purchase, home finding/interim living lump sum, moving expenses, relocation allowance/miscellaneous expense payment, etc., as well as salary advances and training costs.
2. Individuals may quit their current job, remove children from established schools, etc. to accept [Company Name] employment, increasing the possibility the individual will challenge a decision to revoke the offer.
3. The above factors put pressure on the objectivity of the decision-making process when there is an issue with the background report.

4. The removal of the employee from the workplace may disrupt the workplace and harm the morale of other employees.

<b>EMPLOYMENT BACKGROUND SCREENING MATRIX</b>										
	<b>Identification</b>	<b>Employment History</b>	<b>Education</b>	<b>Criminal Record</b>	<b>Motor Vehicle Record</b>	<b>Credit History</b>	<b>Military</b>	<b>Prof. Accredited</b>	<b>Pre-Placement Medical Assessment</b>	<b>INS Form 109</b>
Current Employees not previously screened				X	X					X
New Regular Hires	X	X	X	X	X	X	X	X	X	X
Contractors and Vendors	X			X	X	X				X

#### **Employment Application and Background Report Principles**

*Any intentional misrepresentation or failure to disclose information on the employment application should result in immediate revocation of the employment offer, or termination of employment if the applicant has been employed.*

*Any felony, misdemeanor, or other offense (including attempt or conspiracy) that is relevant to the work to be performed by an applicant or to the presence of the individual on company premises, that is either disclosed by an applicant or discovered in a background check should result in immediate revocation of the employment offer, or termination of employment if the applicant has been employed. Factors such as commission of the offense when a youth and very old convictions may, in some circumstances, work against relevance and a decision to revoke or terminate. Even if an applicant has not been formally convicted of a crime or offense (for example, in the case of a "deferred adjudication" [except where consideration is prohibited by law] or an unresolved charge or indictment), if investigation determines that the applicant engaged in conduct of the type prohibited, the offer should be revoked or employment terminated, as set out above. The types of crimes and offenses that are usually found to be relevant include, but are not limited to, the following:*

- ◆ Theft (e.g., robbery, theft, burglary, hot checks, etc.)
- ◆ Fraud or embezzlement
- ◆ Industrial espionage or trade secret theft
- ◆ Physical violence, such as assault, battery, or homicide
- ◆ Sexual crimes
- ◆ Sale, distribution, or possession of illegal substances
- ◆ Weapons or contraband-related offenses

DWI, DUI, public intoxication, or other alcohol or drug offenses (always relevant for designated positions and security drivers)

## SAMPLE WORKPLACE VIOLENCE POLICY

Nothing is more important to (Company Name) than the safety and security of its employees. Threats, threatening behavior, or acts of violence against employees, visitors, guests, or other individuals by anyone on (Company Name) property will not be tolerated. Violations of this policy will lead to disciplinary action, which may include dismissal, arrest, and prosecution.

Any person who makes substantial threats, exhibits threatening behavior, or engages in violent acts on (Company Name) property shall be removed from the premises as quickly as safety permits, and shall remain off (Company Name) premises pending the outcome of an investigation. (Company Name) will initiate an appropriate response. This response may include, but is not limited to, suspension or termination of any business relationship, reassignment of job duties, suspension or termination of employment, or criminal prosecution of the person or persons involved.

No existing (Company Name) policy, practice, or procedure should be interpreted to prohibit decisions designed to prevent a threat from being carried out, a violent act from occurring, or a life-threatening situation from developing.

All (Company Name) personnel are responsible for notifying the management representative designated below of any threats they have witnessed or received and any threats that they have been told another person has witnessed or received. Even without an actual threat, personnel should report any behavior they have witnessed which they regard as threatening or violent when that behavior is job-related, might be carried out on a company-controlled site, or is connected to company employment. Employees are responsible for making this report regardless of the relationship between the individual who initiated the threat or threatening behavior and the person or persons who were threatened or were the focus of the threatening behavior. If the designated management representative is not available, personnel should report the threat to their supervisor or another member of the management team.

All individuals who apply for or obtain a protective or restraining order that lists company locations as protected areas must provide to the designated management representative a copy of the petition and declarations used to seek the order, a copy of any temporary protective or restraining order granted, and a copy of any protective or restraining order that is made permanent.

(Company Name) understands the sensitivity of the information requested and has developed confidentiality procedures that recognize and respect the privacy of reporting employees.

## SAMPLE EMPLOYEE MISCONDUCT POLICY

These rules address serious acts of misconduct obviously contrary to the ability to maintain a safe, respectful, orderly, and productive workplace. The actions and behaviors listed below will not be tolerated. This means all such acts will be treated as extremely serious violations of the rules of conduct for which discharge will be the first consideration. The list of items below is not intended to represent a complete list of unacceptable conduct. There may be other acts of misconduct that result in the same consequences.

1. Violations of safety rules, practices or policies
2. Dishonesty
3. Engaging in hostile, abusive, threatening, or disrespectful behavior while engaged in activities on behalf of the company, including physical or mental intimidation, threats, or sexual or other forms of harassment
4. Use of abusive, threatening, provocative, or inflammatory language or gestures
5. Receiving or attempting to receive pay under fraudulent circumstances or any other attempts to defraud the company
6. Falsification of records, data documents, or other information including giving false or incomplete information during employment or when applying for employment, or in connection with management investigations
7. Engaging in a fight in the workplace or on site property or in activity that could provoke fighting
8. Use or possession of weapons, ammunition, explosives, or fireworks on site property or in the workplace
9. Use, sale, distribution, manufacture, dispensing, or possession of drugs or alcohol in the workplace
10. While in the workplace, "presence in the body" of alcohol or drugs taken for non-medical reasons
11. Insubordination, including deliberate refusal to comply with reasonable requests or instructions
12. Absence from work without notice or authorization from supervision, unless the cause of absence prevents giving notice
13. Conduct which violates common decency or morality
14. Use of company electronic communications resources for non-business purposes, including unauthorized access to the Internet or access to websites that are inconsistent with company policies, ethics, values, and business practices
15. Horseplay or malicious mischief
16. Using or divulging, without permission, confidential information such as trade secrets, process know-how, personnel data, salary information, business data, etc., regardless of whether the information is taken wrongfully by the employee or merely passed on by the employee
17. Theft, unauthorized possession, removal, or attempted removal of company property or property belonging to employees, contractors, vendors, or visitors
18. Sleeping on the job
19. Intentional damage to company, employee, contractor, or vendor property
20. Bringing "strike anywhere" matches on-site, or having any type of match, cigarette lighter, or flame-producing device in restricted areas
21. Smoking except in designated smoking areas



RECOGNIZING AND MANAGING  
CARRIER SECURITY:  
A HANDBOOK FOR HAZARDOUS  
MATERIAL TRANSPORTERS

---

---

*APPENDIX B*

---

---

CARRIER SECURITY PROGRAM  
DOCUMENTS

## **APPENDIX B**

### **Carrier Security Program Documents**

This appendix contains the following documents related to carrier's security program:

- ◆ Sample Guidance on Suspicious Letters and Packages
- ◆ Sample General Weapons Policy
- ◆ Sample Bomb Threat Procedures
- ◆ Compact, Unified Security Policy and Procedures: Sample 1
- ◆ Compact, Unified Security Policy and Procedures: Sample 2

Adapted from, "Site Security Guidelines for the U.S. Chemical Industry" by the American Chemistry Council.

## SAMPLE GUIDANCE ON SUSPICIOUS LETTERS AND PACKAGES

*The considerations below apply to letters and packages that might contain bombs or hazardous chemical or biological materials.*

Workplaces tend to receive a great number of letters and packages every day. However, not even one piece in a million contains a bomb or chemical or biological material designed to harm the recipient, and closely analyzing each piece would drastically slow down delivery. Furthermore, there is no way to prevent dangerous letters and packages from being sent. Detection and interception are the only responses possible.

A prudent, risk-based approach to detecting dangerous letters and packages is likely to involve general, initial screening by the mail clerk. Possible indicators of suspicious mail include the following:

- ◆ Lumps, bulges, protrusions, or lopsidedness
- ◆ Unusual rigidity or bulk (in an envelope)
- ◆ Handwritten or poorly typed addresses or labels
- ◆ Use of string to bind a package
- ◆ Excess postage (suggests the object was not weighed by the Post Office or a company mailroom)
- ◆ Lack of postage or uncanceled postage
- ◆ Mismatching postmark and return address
- ◆ Any foreign writing, address, or postage
- ◆ Handwritten notes, such as: "To Be Opened in the Privacy of...", "PERSONAL," "CONFIDENTIAL," or "Prize Enclosed"
- ◆ Incorrect spelling of common names, places, or titles
- ◆ Generic or incorrect titles
- ◆ Leaks, stains, strange odor, or protruding wires, string, or tape
- ◆ No return address or nonsensical return address
- ◆ Arrival before or after a phone call from an unknown person asking if the item was received

Mail that does not pass the simple, initial test should be subjected to interception (removal from the mail flow) and follow-up screening. To conduct follow-up screening, the screener could ask the recipient whether he or she was expecting the package, call the apparent sender, or use screening technology. If the screener is still concerned after taking those steps, he or she should report those concerns as directed by the company. The screener also should not open, shake, sniff, or taste the package or its contents.

## **SAMPLE GENERAL WEAPONS POLICY**

In keeping with [Company Name]'s intent to provide a safe and secure work environment for its employees, a "no weapons" policy has been instituted. No weapons of any sort (knife with blade over 2½ inches long, handgun, rifle, shotgun, or other weapons originally designed, made, or intended to fire a projectile by means of an explosion from one or more barrels) are permitted on [Company Name]'s premises. This includes parking lots, leased buildings, leased vehicles, and recreation areas before, during, and after normal business hours. This policy also applies when associates are conducting company business, whether or not on company premises. The sole exceptions apply to military or law enforcement personnel in the performance of their duties and armored car escorts making pickups and deliveries (but side arms are to be holstered inside a facility).

## SAMPLE BOMB THREAT PROCEDURES

The most popular method of making bomb threats is by telephone. It is important that as much information as possible be received from the caller. All bomb threats should be taken seriously. However, experience has shown that most anonymous threat calls are a hoax, intended to create an atmosphere of anxiety and panic in order to interrupt normal activities. Therefore, absent positive target identification (PTI) indicators or other credible information, an evacuation may not be considered appropriate.

### Threats by Phone

All persons who could receive a telephone bomb threat should be taught how to handle the situation effectively. In the event a call is received, the following procedure should be followed:

- Stay calm, be courteous, and do not display fear.
- Activate telephone recording unit, if available.
- Listen carefully. During or immediately after the conversation, take notes of the exact time the call was received, the exact words of the caller, and all details such as sex of caller, accent, attitude, background noises, and motive. Use a bomb threat checklist to record the details of the call.
- Advise the caller that the building, plant, or facility may be occupied and the explosion could result in death or serious injury to many innocent people.
- Keep the caller talking; the more he or she says, the more helpful the information. If the caller does not indicate the location of the bomb or the time of detonation, ask him or her what time it is to go off and where it is located.
- After the phone call, notify the appropriate facility staff.
- Do not discuss the call with anyone else unless authorized to do so or required by law.

### Threats by Mail

Following are the instructions on how to handle bomb threats received by mail. The most likely recipients are mail room personnel and secretaries.

- Place all papers and envelopes associated with the threat in a bag or large envelope (clear plastic bag if possible). Pick up any bomb threat note **ONLY** by the edge.
- Do not handle the written threat any more than absolutely necessary.
- Do not allow anyone else to touch the note unless specifically authorized by a security representative or senior management.

### Manager's Responsibility

In all cases of bomb threat, the facilities or security manager should assess the seriousness of the threat using the following bomb threat assessment and bomb threat response guidelines. He or she should also, if appropriate, notify law enforcement authorities.

### Bomb Threat Assessment

#### ***Is the threat credible?***

Consider:

- Time of day and day of week

- Mode—telephone or mail
- Identity of caller—child, female/male, young/old, drunk, foul language
- Specificity of the threat—time, location, type of explosive device
- Possibility of access to allow placing of the device

***Does the threat contain Positive Target Identifications (PTIs)?***

Did caller identify:

- Time the bomb is to detonate?
- Target to be destroyed?
- Bomb's construction, shape, or description?
- Bomb's location?

Bomb Threat Response

***What is the proper response?***

Do not evacuate?	This may be an appropriate response if there have been a number of recent, publicized hoax bomb threats in the area; if the caller seemed to be drunk; if the caller was a young child, or if it is a beautiful Friday afternoon about an hour or so before quitting time. This is especially true when no PTIs were provided in the bomb threat call.
Conduct a limited or general search of the facility?	Searches are usually the most appropriate choice and should generally be the chosen response, especially if no PTIs or only one PTI was given in the threat.
Order limited evacuation, general evacuation, or move to a safe haven?	Evacuations are usually ordered only when the call is judged to be serious, the threat credible, there is insufficient time to conduct a thorough search, and the judgment is made that employees will be at less risk evacuating or moving to a safe haven than remaining in place and seeking cover. <b>If two or more PTIs are given in the bomb threat call, an evacuation may be in order.</b>

***How should the chosen response be executed?***

- Use a PA announcement, telephone cascade, messenger, or other local notification plan.
- Determine who is to search and in what area. In general, employees should search their own area to determine if there are any suspicious objects. Common areas should be searched by those most familiar with the areas.
- Notify public law enforcement and emergency services as appropriate; notify immediately if a suspicious object is found.
- If appropriate, determine who is to be evacuated and to what location.
- If evacuation is ordered before a search is done, determine for how long. Consider options if weather is inclement. Consider possible effect on operations if evacuation occurs at or near shift change.

- Ensure that procedures are in place to account for all persons ordered to evacuate and determine that they have in fact evacuated and there is an orderly shutdown of operations, if required.
- Coordinate with local authorities to determine if the area needs to be searched and who will determine that operations can resume and people can return to their work stations.

#### Search Plans

A predetermined search should be organized. It is not effective to delegate the search to the police alone because they are unfamiliar with the area and do not know which objects in the facility would look unusual or out of place. The most effective search is possible when all employees are calmly told about the bomb threat and the reason for the search and are then asked to check their familiar areas for suspicious objects. Teams should be organized to search common areas. A search team leader should be designated and a notification protocol developed to report search results to the facilities manager. A plan should be developed to designate who is responsible for searching a specific area—for example, security will search restrooms and outside areas, while facilities staff will search LAN and electrical rooms.

The objective of the search activity is to search for and report suspicious objects. There are several points to be stressed within search plans:

- The search should be systematic (divide the facility into search areas), it should be thorough, and it should be done calmly. It should be done by company personnel. Identify the areas that are most accessible to outsiders and the areas that are most vulnerable; search them first.
- When searching a room, the room should first be searched from floor to waist height, then from waist height to eye level, and finally from eye level to ceiling. If the room has a false ceiling, the false ceiling should also be inspected and searched.
- **Nobody should move, touch, or jar any suspicious object or anything attached to it. The removal or disarming of a bomb must be left to law enforcement professionals.**

#### No Bomb Found

If no bomb (or suspicious object) is found, the facilities manager should advise employees, the police, and local management and return the operation to normal activity.

#### Suspicious Object Found

If a suspicious object is found, the search team coordinator and the facilities manager should do the following:

- Stress again to personnel not to touch or move the object.
- Evacuate personnel from the surrounding area.
- Prevent re-entering of the evacuated area.
- Inform the police who will take charge of getting the object deactivated and removed.
- After the object has been removed, finish searching to ensure that no other bombs have been placed.

#### Bomb Explosion

If there is a bomb explosion, the facilities or security manager should take these steps:

- Determine if there are any injuries and attend to them immediately.
- Evacuate the surrounding area.

- Ensure no one goes near the scene of the explosion except to remove the injured.
- Control access to the area as other bombs may have been set to detonate at intervals.
- Advise police who will take charge of the situation.
- Initiate the on-site emergency plan if fire fighting or other medical response becomes necessary.

#### After-Action Plan

An after-action report, including incorporation of lessons learned, should be prepared immediately after resolution of the event.



## **COMPACT, UNIFIED SECURITY POLICY AND PROCEDURES: SAMPLE 1**

It is important that management state the security behavior expected while persons are on company property or performing duties directly related to work requirements. This may best be done by the issuance of a written policy, which articulates expectations and compliance criteria. Procedures to comply with the policy should also be provided.

### **Access Control:**

**Policy:** It is the policy of [Company Name] that access to the facility be limited to those who have been granted authorization for access.

**Procedures:** The property boundary will be clearly defined. Signage will be used to direct entrants to the appropriate entry point for processing onto the facility. Management will define the process for granting authorization for access to an individual. This may include verification of safety briefings and utilization of personal protection equipment. Employees, visitors, and contractors will log into and out of the facility, when entering or exiting the facility after being granted access authorization.

### **Pre-employment Screening**

**Policy:** It is the policy of [Company Name] that pre-employment screening will be conducted on candidates for employment.

**Procedures:** Human Resources will contract with a third-party provider approved by Corporate Human Resources to conduct such screens.

### **Workplace Violence**

**Policy:** [Company Name] has “zero tolerance” for any incident of violence in the workplace, whether it be physical violence, verbal abuse, willful destruction of company property, or any form of intimidation that affects the morale of the workforce. Such acts may be cause for counseling, reprimand, or even termination of employment. Alleged incidents will be investigated and sanctions exercised when warranted.

**Procedures:** Incidents of violence shall be reported to management immediately. Management will take appropriate action to defuse an ongoing confrontation and to gather evidence for investigation. Those involved in the incident shall be suspended from work, pending conclusion of the investigation. After consideration of the facts, management will adjudicate the incident. Employees victimized by violence, who obtain court-issued restraining orders, shall notify management immediately and provide copies of documentation. Management will notify law enforcement of any violations.

### **Drug and Alcohol Abuse**

**Policy:** [Company Name] has a corporate policy on this subject.

**Procedures:** Local management should publicize the policy to all employees and, as necessary, supplement the policy to reflect local conditions and requirements. NOTE: Local management can only increase the severity of the policy, not reduce any conditions of the corporate policy.

### **Protection of Information**

**Policy:** It is the policy of [Company Name] that all company information—classified confidential, internal, or external—be secured from unauthorized disclosure or misuse.

**Procedures:** Management will define information to be safeguarded. Information will be disclosed on a limited basis and will be stored in a locked desk, file cabinet, or safe when not in use. Employees, visitors, vendors, and contractors will be required to sign statements of confidentiality before being granted access to the facility.

### **Weapons on Company Property**

**Policy:** [Company Name] has a corporate policy on this subject.

**Procedures:** Management should ensure that anyone entering a [Company Name] facility is made aware of the restriction of weapons on company property. Exceptions to the policy are available based on specific needs. The policy and procedures should be supplemented at the local level to ensure compliance and enforcement.

### **Incident Reporting**

**Policy:** It is the policy of [Company Name] that security incidents be reported immediately to Corporate Security.

**Procedures:** *Security incidents should be reported to Corporate Security by calling [phone number]. This will be followed by the submission of an incident reporting form. If security guards are employed, the security post orders should include a requirement that the officer call [phone number] about all emergency incidents.*

**COMPACT, UNIFIED SECURITY POLICY AND PROCEDURES:  
SAMPLE 2**

- 1.0 **APPLICABILITY:** This policy shall apply to all company facilities.
- 2.0 **PURPOSE:** To require that minimum site security provisions be implemented to prevent harm to individuals, to avoid business interruption, and to prevent loss of property and information, due to theft, vandalism, violence, illegal and disruptive activities by extremist groups, and other criminal acts against the company.
- 3.0 **POLICY:** Each company location shall implement a site security program. The program will be developed considering the following potential sources of loss or disruption:
- 3.1 Theft, vandalism, and break-ins, considering both internal and external threats
  - 3.2 Theft of confidential business information
  - 3.3 Sabotage of equipment, utilities, and records; product contamination and tampering
  - 3.4 Bomb threats
  - 3.5 Demonstrators disrupting plant access and operations
  - 3.6 Workplace violence and assaults
- 4.0 **POLICY:** Each company location shall designate an employee as the site security coordinator. This person shall be responsible for performing the following security management functions:
- 4.1 Preparing and implementing a site security plan consistent with the requirements contained herein
  - 4.2 Establishing relationships with law enforcement agencies
  - 4.3 Developing and managing incident reporting systems and conducting investigations of breaches of company security policy
  - 4.4 Developing methods to increase employees' security awareness
  - 4.5 Working with the site emergency coordinator to address security issues in emergency and crisis management planning and execution
  - 4.6 Periodically reassessing the site's security program
- 5.0 **POLICY:** The security measures at each site shall include the following provisions:
- 5.1 Access control for people and vehicles into production areas, warehouses, utility facilities, and offices that contain business information that needs to be protected ("controlled areas")
    - 5.1.1 Signs to direct all visitors and vehicles to the appropriate entry points
    - 5.1.2 A system to verify visitors (any non-employee) and vehicles prior to entering company premises, along with safety and security briefing for all visitors
    - 5.1.3 For non-employees, mandatory sign-in for access to controlled areas for at least the first visit (policy on escorting visitors during subsequent visits to be developed by the location)
    - 5.1.4 Identifying badge for all visitors, along with requirement to wear the badge so it is visible
    - 5.1.5 Controlled areas to be provided with physical barriers capable of keeping unauthorized people and vehicles out, except through designated entrance points (barriers shall not impede emergency egress from facilities)
    - 5.1.6 Access points to controlled areas placed so that receptionist has a clear and remote view of visitors and vehicles approaching the facility

- 5.2 Perimeter protection (such as fences, solid exterior walls, gates to block vehicle traffic, and perimeter lighting) around controlled areas
- 5.3 Off-hours protection for controlled areas, such as remotely supervised intrusion alarms or a contract security guard service touring the facility regularly
- 5.4 Back-up power systems for controlled areas where operations are critical and for intrusion alarm and safety systems

6.0 POLICY: For employee security issues, refer to existing HR policies on the following subjects:

- Pre-employment screening
- Employee termination
- HR services
- “Zero tolerance” for violence
- Prohibition of weapons on company facilities, including parking lots
- Confidential business information
- Internal incident reporting systems
- Referring illegal or criminal activities to law enforcement

RECOGNIZING AND MANAGING  
CARRIER SECURITY:  
A HANDBOOK FOR HAZARDOUS  
MATERIAL TRANSPORTERS

---

---

*APPENDIX C*

---

---

DEPARTMENT OF TRANSPORTATION  
HAZARD CLASSIFICATIONS

**APPENDIX C**  
**Department of Transportation Hazard Classifications**

This appendix presents DOT classifications for hazards and placards in Table C-1.

**Table C-1. DOT Hazard Classes.**

<b>Class Definition</b>	<b>Division</b>	<b>49 CFR Reference for Description</b>	<b>Placard Name</b>	<b>Short Description</b>	<b>Additional Description</b>
None	--	49 CFR 173.21	--	Forbidden Materials	
None	--	49 CFR 173.53	--	Forbidden Explosives	
Class 1 - Explosives	1.1	49 CFR 173.50	Explosive 1.1	Mass Explosion Hazard	May explode if fire reaches cargo area. Fire may produce irritating or poisonous gases.
	1.2		Explosive 1.2	Projection Hazard	
	1.3		Explosive 1.3	Fire Hazard and either Minor Blast or Minor Projection Hazard	
	1.4		Explosive 1.4	Minimal Hazard	
	1.5		Explosive 1.5	Blasting Agents	
	1.6		Explosive 1.6	Very Insensitive Detonating Devices	

**Table C-1. DOT Hazard Classes.**

<b>Class Definition</b>	<b>Division</b>	<b>49 CFR Reference for Description</b>	<b>Placard Name</b>	<b>Short Description</b>	<b>Additional Description</b>
Class 2 - Gases	2.1	49 CFR 173.115	Flammable Gas 2	Flammable Gas	Extremely flammable; may be ignited by heat, sparks or flames. Vapor extremely irritating. May cause tissue damage.
	2.2		Nonflammable Gas 2	Nonflammable Nonpoisonous Gas	Container may explode in a fire. Some materials may burn. Contact may cause tissue damage.
	2.3		Poison Gas 2	Poisonous Gas	Container may explode in a fire. Some materials may burn. Contact may cause tissue damage. Poisonous if inhaled or absorbed through the skin.
Class 3 - Flammable Liquids	--	49 CFR 173.120	Flammable 3	Flammable Liquid	Flash point below 141 degrees F
			Combustible 3	Combustible Liquid	Flash point between 141 degrees F and 200 degrees F

**Table C-1. DOT Hazard Classes.**

<b>Class Definition</b>	<b>Division</b>	<b>49 CFR Reference for Description</b>	<b>Placard Name</b>	<b>Short Description</b>	<b>Additional Description</b>
Class 4 - Combustible Solids	4.1	49 CFR 173.124	Flammable Solid 4	Flammable Solids	Will ignite if exposed to air. Fire may produce irritating or poisonous gases.
	4.2		Spontaneously Combustible 4	Spontaneously Combustible	May be ignited by heat, sparks, or flame. May be poisonous if inhaled or absorbed through skin.
	4.3		Dangerous When Wet 4	Dangerous When Wet	Flammable/combustible material. May ignite by heat, sparks, or flame.
Class 5	5.1	49 CFR 173.127	Oxidizing Agent 5.1	Oxidizing Agents	May ignite with other combustible materials (i.e., wood, paper, etc.). May be harmful if inhaled.
	5.2	49 CFR 173.128	Organic Peroxide 5.2	Organic Peroxide	May ignite if exposed to air, heat, sparks or flame. Contact may cause tissue damage.
Class 6 - Poisons	6.1	49 CFR 163.132	Poison Inhalation Hazard 6	Inhalation Hazard	Poisonous if inhaled
	6.2	49 CFR 173.134	Harmful Stow away from Foodstuffs 6	Will contaminate food	



**Table C-1. DOT Hazard Classes.**

<b>Class Definition</b>	<b>Division</b>	<b>49 CFR Reference for Description</b>	<b>Placard Name</b>	<b>Short Description</b>	<b>Additional Description</b>
Class 7 - Radioactive Materials	7	49 CFR 173.403	Radioactive 7	Material has a specific radioactive activity greater than 70 kBq/kg. External radiation hazard from unshielded radioactive material. Internal radiation hazard from inhalation, ingestion, or skin absorption. Some materials may burn. Degree of hazard varies greatly depending on type and quantity of material.	
Class 8 - Corrosives	8	49 CFR 173.136	Corrosive 8	May burn, but not easily. Contact may cause tissue damage. Poisonous if inhaled, swallowed or absorbed through skin.	
Class 9 - Miscellaneous Dangerous Substances and Articles	9	49 CFR 173.140	9 (Miscellaneous Dangerous)	Miscellaneous Dangerous Substances & Articles	Materials that present a hazard during transport, but which are not included in any other hazard class.
None		49 CFR 173.144		Other Regulated Material-Dangerous (ORM)	

# Index

## A

- About The Authors ..... vii
- Access Control ..... 3-5
- Assessing Security Risk For
  - Commodities..... 6-1
- Assuring En Route Security ..... 4-1
- Assuring Site And Package Security 3-1

## B

- Benefits Of Carrier Security ..... 1-2
- Bomb Threat Procedures
  - See Sample Bomb Threat Procedures .....B-4

## C

- Carrier Security Program ..... 5-1
- Chemical Hazard Ranking ..... 6-5
- Commodity Security Risks ..... 6-7
- Communicating ..... 4-4
- Communicating And Collaborating .. 5-2
- Compact, Unified Security Policy
  - And Procedures: Sample 1
    - See Sample Compact, Unified Security Policy And Procedures: Sample 1 .....B-8
- Compact, Unified Security Policy And Procedures: Sample 2
  - See Sample Compact, Unified Security Policy And Procedures: Sample 2 .....B-10
- Complying With DOT Regulations .. 4-4
- Controlling Access ..... 3-1
- Controlling Packages ..... 3-5
- Criminal History ..... 2-3

## D

- Developing And Maintaining A Security Policy .....5-2
- Driver's Application For Employment
  - See Sample Driver's Application For Employment .....A-2
- Driver's License Requirements .....2-4

## E

- Employee Disclosure Form
  - See Sample Employee Disclosure Form .....A-9
- Employee Misconduct Policy
  - See Sample Employee Misconduct Policy .....A-14
- Employee Security Training .....5-3
- Ensuring Personnel Security .....2-1
- Ensuring Vehicle Security .....4-2

## F

- Federal Motor Carrier Safety Administration..... 1-2
- Federal Requirements Pertaining To Attendance, Surveillance, Parking, And Fueling Of Motor Vehicles...4-4, 4-5
- Freberg Environmental, Inc. .... 1-1

## G

- General Weapons Policy
  - See Sample General Weapons Policy ..... B-3
- Guidance On Suspicious Letters And Packages
  - See Sample Guidance On Suspicious Letters And Packages .....B-2

## H

How The Handbook Is Organized .... 1-4

## I

Identifying On-Site And En Route

Employees ..... 2-5

Immigration And Naturalization

Service ..... 2-3

Implementing Personnel

Communications Policies ..... 2-6

Incident Analysis ..... 5-4

Incident Management..... 5-7

Incident Reporting ..... 5-4, 5-5

Investigating Security Breaches And

Enforcing Discipline..... 5-6

## L

Local Emergency Planning

Committees..... 5-3

## M

Making A List Of Commodity

Chemicals ..... 6-1

Managing Incidents..... 5-7

## P

Perimeter Protection..... 3-5

Pre-Employment Screening ..... 2-1

Pre-Employment Screening Policy

*See Sample Pre-Employment*

Screening Policy ..... A-11

Preface.....v

Preventing And Responding To

Workplace Violence ..... 2-7

Prioritizing Transportation Security

Risk..... 6-5

Protecting The Perimeter ..... 3-3

Providing Security Officers ..... 3-4

## R

Radioactive Shipments .....4-2

Ranking Chemical Hazard.....6-2

Ranking Exposure.....6-3

Reporting And Analyzing Incidents ..5-4

Request For Information From

Previous Employer

*See Sample Request For*

*Information From Previous*

*Employer* .....A-8

Resources For This Handbook.....1-2

Reviewing Transportation Security

Risk.....6-7

## S

Security Breaches .....5-6

Security Officers.....3-4

Security Policy .....5-2

Security Program .....5-1

Developing .....5-1

Establishing .....5-1

Reassessing.....5-8

Security Site Review.....3-5

Security Talking Points.....1-2

Security Violation.....5-5

Site Security Guidelines For The U.S.

Chemical Industry .....1-3

Summary Of Your Rights Under The

Fair Credit Reporting Act.....A-10

## T

Technical Innovations.....5-5

Terminating Employment.....2-6

Transportation Operations Planning ..4-1

Transportation Security Guidelines

For The U.S. Chemical Industry....1-3

*U*

Uniting And Strengthening America By  
Providing Appropriate Tools  
Required To Intercept And Obstruct  
Terrorism ..... 2-4

*V*

Vehicle Security ..... 4-2

*W*

Workplace Violence .....2-7  
Workplace Violence Policy  
    *See* Sample Workplace Violence  
    Policy.....A-13



# FREBERG ENVIRONMENTAL INSURANCE

INSURANCE PROGRAM MANAGERS

1675 Broadway, Suite #2210 • Denver, Colorado 80202  
800/377-4152 • 303/571-4235 • Fax: 303/623-8101  
info@feinsurance.com  
[www.feinsurance.com](http://www.feinsurance.com)