GUIDE TO DEVELOPING AN EFFECTIVE SECURITY PLAN FOR THE HIGHWAY TRANSPORTATION OF HAZARDOUS MATERIALS

Table of Contents

October 9, 2003

Executive Summary

This Guide is a tool that motor carriers transporting hazardous materials can use in developing a security plan as required by the U.S. Department of Transportation in their HM-232 rulemaking [1]. It is designed to provide motor carriers with (a) sufficient background to understand the nature of the threats against hazardous materials transportation; (b) the means to identify the vulnerabilities to those threats; and (c) an approach to address the vulnerabilities.

The first step in developing a security plan is conducting a security assessment. The Guide establishes a framework for reviewing a company's hazardous materials operations and identifying relevant threats and vulnerabilities. The focus is on making the assessment specific with respect to an individual company facility or each type of hazardous material. The Guide also offers an approach for prioritizing each of the threats and vulnerabilities that are identified.

The discussion of the security plan introduces a recommended approach for determining appropriate security measures for addressing identified threats and vulnerabilities that help to eliminate unnecessary security-related expenses. Consideration of varying threat levels (such as those indicated by the Homeland Security Advisory System) and a method for prioritizing potential security measures is also discussed.

The Guide covers the required security training (awareness and in-depth) and security plan administration. Administration includes the distribution, maintenance, verification, and validation of the full security plan as well as how to best incorporate the insights and support that are available from industry partners, local community organizations, and law enforcement agencies.

Introduction

Hazardous materials in transportation are vulnerable to sabotage or misuse and in the wrong hands pose a significant security threat. The security of hazardous materials in transportation poses unique challenges as compared to security at fixed facilities because of the changing environment surrounding a moving vehicle. Since hazardous materials are frequently transported in large quantities, once mobile they are particularly vulnerable to theft, interception, detonation, or release. When transported in proximity to large population centers, accidental or intentional acts could have serious consequences.

Due to the terrorist attacks committed on September 11, 2001, and subsequent threats to the transportation system, the Federal Motor Carrier Safety Administration (FMCSA) conducted over 30,000 Security Sensitivity Visits (SSVs) between October 2001 and April 2002. The SSVs consisted of face-to-face meetings between FMCSA or state investigators and top carrier officials to assess security vulnerabilities and identify countermeasures that can improve security. FMCSA then began including SSVs as part of all compliance reviews on hazardous materials (HM) carriers to encourage a high level of vigilance within the industry.

Also prompted by the September 11, 2001 terrorist attacks and subsequent threats related to biological and other types of hazardous materials, the Department of Transportation's Research and Special Programs Administration (RSPA) issued new regulations under Docket No. HM-232 intended to enhance the security of hazardous materials transportation [1]. As discussed in more detail below, the new regulations impose security plan and security training requirements on certain hazardous materials shippers and carriers.

The Research and Special Programs Administration, which has regulatory authority over hazardous materials transportation across all modes, published the HM-232 final rule on March 25, 2003. The HM-232 regulations require persons who offer certain types and quantities of hazardous materials (hazmat) for transportation or transport in commerce to develop and implement security plans by September 25, 2003. In addition, all hazmat employees, as defined in the Hazardous Materials Regulations (HMR, 49 CFR Parts 171-180), must receive training that provides an awareness of security risks associated with hazmat transportation and methods designed to enhance hazmat transportation security.

Persons who offer for transportation or transport the following hazardous materials must develop and implement security plans that conform to the HM-232 requirements:

HAZARDOUS MATERIALS SHIPMENTS SUBJECT TO HM-232	
Material	**Threshold (if specified)**
Class 7 - Radioactive	Highway route controlled quantity (HRCQ)
Division 1.1, 1.2, or 1.3 - Explosive	More than 25 kg (55 pounds)
PIH in Hazard Zone A	More than 1 liter (1.06 quarts)
HM in a bulk packaging (container)	Capacity of packaging equal to or greater than: Liquid or gas: 13,248 liters (3,500 gallons) Solid: 13.24 cubic meters (468 cubic feet)
HM in a non-bulk packaging	Total gross weight equal to or greater than 2,268 kg (5,000 pounds)
Select agent or toxin regulated by the Centers for Disease Control and Prevention (CDC)	
Any HM shipment requiring placarding according to subpart F of the HMR	

Many motor carriers include security measures in their standard operating policies and procedures. The HM-232 final rule requires a more systematic approach to transportation security and a specific focus on potential terrorist or criminal threats. While any plan that meets the specific provisions of the rule will be acceptable, many organizations will have to make adjustments to existing plans to cover all required areas. Other organizations will develop their security plans for the first time in response to this new regulation. The information in this Guide should serve as a tool in developing a security plan required by the U.S. Department of Transportation.

You should also be aware that the U.S. Patriot Act, passed in October 2001, included a provision for requiring background checks for individuals operating motor vehicles transporting hazardous materials [2]. The Transportation Security Administration (TSA) enacted regulations on May 5, 2003 implementing this provision. TSA's rule requires routine background checks for drivers with a hazmat endorsement on their Commercial Drivers License (CDL). The required background checks must include a review of criminal, immigration, and FBI records [3].

How to Use This Document

Although this Guide is directed at motor carriers that transport hazardous materials, hazmat shippers may also find this publication a useful tool. The information herein is a tool that you may apply in developing a security plan required by the U.S. Department of Transportation. While the main chapters guide you through the steps a motor carrier needs to take and the issues they need to consider, the appendices provide more in-depth information that will be helpful in the development of an effective security plan. Following is a review of the chapters and appendices:

- The Introduction provides a review of the security planning process and of the background for this Guide. If you would like more information about terrorists and their operations, refer to Appendix A.
- Chapter One guides you through your security assessment to identify the threats and vulnerabilities to your operations. A security assessment is a necessary first step in preparing your security plan. If you would like more detailed information on issues to consider, refer to Appendix B.
- Chapter Two addresses the detailed components that need to be included in your security plan and provides examples on how to construct the plan. Personnel security, unauthorized access, and en route security are specifically addressed. Additional guidance for companies with operations at many locations is also included. This chapter does NOT provide a comprehensive list of security measures for you to implement; rather, it guides you in

determining which ones are right for you. Some examples are included in this chapter to get you started and more are included in Appendix C.

- Chapter Three discusses the required components of a training program and how to develop one.
- Chapter Four covers the administration of your security plan including how it is provided to your employees and maintained. This section also covers establishing relationships with other entities, such as local law enforcement, to augment and enhance your security.
- Appendix D outlines the approach that the Federal Motor Carrier Safety Administration (FMCSA) is taking to ensure that the highway transportation of hazardous materials is secure and that motor carriers are in regulatory compliance.
- Appendix E at the end of this Guide contains a list of references and citations.

Acronyms

CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CDL	Commercial Drivers License
DOT	U.S. Department of Transportation
DHS	U.S. Department of Homeland Security
FMCSA	Federal Motor Carrier Safety Administration (in DOT)
FBI	Federal Bureau of Investigation
HM-232	Security Requirements for Offerors and Transporters of Hazardous Materials, a rulemaking issued by RSPA
HM, hazmat	Hazardous Materials
HMR	Hazardous Materials Regulations
HRCQ	Highway Route-Controlled Quantity (of RAM)
HSAS	Homeland Security Advisory System (with five color-coded levels)
PIH	Poisonous by Inhalation (synonymous with Toxic by Inhalation)
PSO	Primary Security Objective
RAM	Radioactive Material
RSPA	Research and Special Programs Administration (in DOT)
SSV	Security Sensitivity Visit
TSA	Transportation Security Administration (in DHS)
WMD	Weapons of Mass Destruction

Glossary

carrier	The company transporting a shipment from the shipper to the consignee
consignee	The company (or person) to which a shipment is destined (the receiver)
likelihood	The probability of something happening; for HM security, the attractiveness of something to a terrorist is used in place of likelihood
may	Indicates an option for consideration only.
must	Indicates something which is required for you to do by regulation
non-specific but credible	Refers to a threat that is general in nature but is still believed to be realistic
primary security objective	Term used to represent a main goal in addressing security vulnerabilities; security measures are chosen to meet the primary objective
risk	Represents the exposure to a hazard; for HM security, risk is the likelihood of a terrorist act combined with its probable consequences
specific and	Refers to a threat that is focused (perhaps to a city, bridge, or industry) and

credible	believed to be realistic
specific security measure	A policy, procedure, device, etc. that is put in place to reduce one or more vulnerabilities that an organization may face
shipper	The offeror of the shipment for transportation (the origin)
should	Implies a recommendation only - it is not required
threat	A source of danger; for HM security, this includes terrorists and criminals and the types of attacks they might initiate to achieve their objectives
vulnerability	A weakness; susceptibility to attack or injury.

Chapter One: Security Assessment

One of the most critical components of HM-232 is the assessment of possible transportation security risks for covered shipments of hazardous materials. Many companies have implemented numerous security measures without examining the threats against their operations and their vulnerabilities to those threats. Threats are sources of danger and can include both criminals and terrorists and the attacks that they might initiate to achieve their objectives. Vulnerabilities are weaknesses that make you more susceptible to attack or injury.

HM-232 requires companies to complete a written security assessment and to develop a security plan that is based on the assessment. This Guide will assist motor carriers in conducting their security assessments and in developing their security plans.

Part A. Reviewing Your Hazmat Operations

When conducting a proper assessment of the threats to and vulnerabilities of your operation to a terrorist attack or terrorist activity, the types of information to consider include: (a) the type of hazardous material you transport, (b) the frequency and quantity of shipments, (c) the packaging type, and (d) the amount stored on-site. You will also need to identify and address your business practices (including relationships with external partners), such as the emergency response information that is available on site, and physical assets that are a part of your hazmat transportation activities.

A.1 Business Practices

You should analyze your company's business practices that affect the transportation of the hazardous materials included in HM-232 to identify potential security vulnerabilities. Such business practices may include:

- Taking and processing orders, including dispatching;
- Hiring and human resources-related activities (which relate to ensuring the trustworthiness of employees);
- Job descriptions, organization charts, and reporting structures for responsible management and decision making, security policies, and reporting (which all relate to who has access to information and who makes key decisions);
- Facility and building access policies and procedures;
- Qualification and selection of outside service providers (contractors) with access to hazmat handling areas; and
- Policies and procedures on distributing information related to hazmat shipments, including to business partners.

A.2 Physical Assets

You should analyze each physical asset (facility, terminal, etc.) used in the transportation of hazmat to identify potential security vulnerabilities. This analysis should consider, at a minimum, the following:

- Exterior surveillance and line-of-sight attack potential;
- Areas of concealment;
- Normal and potential vehicle and pedestrian paths;
- How congestion, choke points (where vehicles or pedestrians may get delayed during an evacuation), and other circumstances might reduce the effectiveness of your security measures;
- Your immediate surroundings - assess the potential for layered protection or and the nature of potential nearby threats;
- Storage facilities, transfer, loading, and unloading areas;
- Business offices, storage of empty hazmat packagings; and
- Visitor, vendor, and employee parking.

In addition, you should examine each configuration of transport vehicles for vulnerabilities based on use and the likely routes. Unlike many facilities, where the areas that are most in need of protection (such as critical operation centers) are separated from an outer fence by a considerable distance, there is no protective buffer surrounding vehicles on the road. Vehicles, therefore, can be more vulnerable. You should also identify and assess facilities that are owned and/or operated by others, such as truck stops, and rest/parking areas.

Part B. Identifying Relevant Threats and Vulnerabilities

It is important to remember that in the case of hazardous materials, the assumed agenda of terrorists is to convert the material, package, or vehicle into a weapon; in other words, controlling the material is an operational act in support of a larger attack plan. This can occur in several ways. The three principal methods are:

- The material can be purchased and delivered to the target location or an intermediate site to be transported later.
- The material can be acquired by theft either in transit or at a storage site. This part of the operation can take the forms of fraud, stealth, or violence.
- The material can be converted to weapons use directly while under legitimate control. This could be a violent event that takes the form of a catastrophic release, typically by explosive or mechanical attack.

Taking the case of the legitimate purchase, there is nothing in the HM-232 security requirements that calls for validation of the consignee. However, it would be prudent business practice (but not required) to verify that an order of unusual character, such as a large shipment of toxic-by-inhalation gas to a stadium, is in fact expected and required. When it comes to determining which security measures are appropriate for your company, such as checking with consignees, only you can be the judge.

Material acquired by theft is not unlike criminal activity associated with high value shipments. Unlike typical criminal profiles, however, the terrorist's readiness to employ extreme violence is much greater. Where the criminal may be reluctant to employ deadly force because of the repercussions if captured, the terrorist may not expect to survive the operation and so eventual capture is meaningless as a deterrent. Without considering the tactics used, a terrorist's objective

is to take control of the material and transport it to a target location for use as a weapon. Maintaining control of the cargo, not the vehicle, is the primary concern here.

In the third case, the material is converted to a weapon on the spot. This means that the material must be located at or near the final target. Storage areas and transport routing that are near desirable targets should be areas of concern. The 'Trojan Horse' scenario, where a device is attached to a shipment and detonated at the desired moment and location, and the 'Intercept' where a device is located in anticipation of the material's passage, are the two most likely options.

What you can derive from all of the preceding discussion is that each method requires specific knowledge in order to be successful. There are basically three ways in which a terrorist can obtain this information:

- Conduct research of public records and reference materials, including company websites, annual reports, and marketing information;
- Observe operations; and
- Acquire knowledge from participants in the company's operations or by actually taking part themselves (as an "insider").

Public information may be of limited value beyond learning the characteristics of the material being pursued. Observation is an operational act that involves exposure and risk of discovery. Direct knowledge through participation or trust of those in a position to know provides both detail and a high level of confidence in the information. This is the reason why business processes are of a security concern to HM-232. For additional insight into terrorists and their operations, see Appendix A.

Part C. Addressing the Transportation of Specific Hazardous Materials

Although a major portion of the security plan may be uniform across a company's entire operation, planning must recognize that different classes of material may require different strategies. This is due to the nature of the material and the character of the transportation processes involved. The following is a discussion of several materials:

- Radioactive materials (RAM) are not likely to be used in creating a fission or fusion bomb, but as a persistent contaminant, that represents both a real health hazard and an emotional trigger for widespread panic. The most publicly discussed tactic is the 'Dirty Bomb', more appropriately referred to as a 'Radiological Dispersion Device' or RDD. This device uses conventional explosives to disperse the contamination, potentially creating an acute situation for large numbers of people. Because certain types of RAM are effectively invisible and easily spread through contact, less spectacular methods of dispersal must also be considered.
- Explosives require proximity to the target and sufficient quantity to be effective. By controlling either of these two parameters, the potential consequences can be reduced.
- Poisons are similar to RAM in that they represent a dispersal attack in order to be effective. Unlike RAM, dispersal of poisons must maintain an effective level of concentration to be successful. This tends to limit use of these materials to situations where the dispersal can occur within a defined volume.
- Flammables represent the most common category of hazardous material shipped and transported. The sheer number of opportunities and the diversity of locations and circumstances involved make flammable materials cause for concern.
- Biological materials represent means for dispersal attack, similar to RAM. CDC-regulated materials represent a potential for the introduction of infectious disease into the population.

Another category of hazardous materials of interest to HM-232 includes all other placarded materials. Although these may not present the level of weapons potential as those discussed above, some of them are capable of significant economic and social disruption when intentionally released with malicious intent, while others do not require any additional security measures to be implemented.

Part D. Addressing Your Specific Operations

Companies have different and distinct types of operations. For example, some companies act as both shipper and carrier. In addition, some carriers maintain their over-the-road operations entirely separate (and differently) from their local pickup and delivery operations. It is appropriate to consider the distinct character of each of your operations in your security assessment.

HM-232 addresses the transportation of hazardous materials. It does not cover fixed facility operations unless those operations are incidental to transportation, such as loading, unloading, and certain temporary storage. At a shipper facility, the elements that you should examine include the preparation of hazmat for transportation, selection and use of appropriate packaging, preparation of shipping documentation, loading operations, and so on. To the extent that this information can be hidden, the vulnerability can be reduced. You may want to include issues related to long-term storage of hazmat at your facilities in your security assessment, but are not required to do so by HM-232.

Both shipper and carrier operations involve the processing of orders. The 'business side of the house' is important because of the storage and shipping information. There are two groups of people of concern: those that must process or act on the order information and those who may have access to the information but do not typically process or act on it. Although each person who processes an order should be considered a potential threat, they also represent an opportunity for threat recognition.

Carrier operations present several difficult security issues. Effective status and tracking of the cargo may be impractical, forcing strategies that involve the personnel and transportation equipment as surrogate indicators to potential problems. The variety of situations typically encountered while en route present many vulnerabilities that a terrorist can exploit.

Part E. Prioritizing Threats and Vulnerabilities

Companies have limited security dollars, making it necessary to prioritize the vulnerabilities to be addressed and the primary security objectives (PSOs).

There are many ways to do a prioritization, but most rely on some form of subjective ranking system. For example, you may prioritize the threats you face as highly likely, somewhat likely, possible, unlikely, or improbable (of course, you could use a greater or fewer number of categories). You may then rate your vulnerabilities (perhaps on a scale from very low to high), considering how easy you believe it would be to exploit that vulnerability given your current operations. Combining these categories can help you focus your energies and limited resources on those vulnerabilities most easily exploited that correspond to the highest threats. You can treat this combination of threats and vulnerabilities as the relative likelihood of a terrorist act. However, this is not likelihood in the traditional sense of the word, since there are not sufficient historical data to know the probabilities of any future terrorist acts; it is simply a good substitute. This analysis will help you see what terrorists find attractive. The table below shows one example-assigning a value from 1 to 4 to each combination of threat and vulnerability, with a value of 4 having the highest likelihood. Let's say you have identified three threats to which you have some vulnerability. For one of these threats you have a single vulnerability that could be exploited; however, for the other two, you have two vulnerabilities each. This makes a total of five threat-

vulnerability combinations. To prioritize these, you would place each of the five combinations in the appropriate cell in the table below.

"LIKELIHOOD"				
VULNERABILITIES				
THREATS	Very Low	Low	Medium	High
Specific and Credible	2	3	4	4
Non-specific but Credible	2	3	3	4
Possible	1	2	3	3
Unlikely	1	2	2	2
Improbable	1	1	2	2

You may also wish to consider the potential consequences of a terrorist act in each case. For example, you may identify similar threats and vulnerabilities for operations involving different materials, but the consequences of one material may be worse than for the others. You could use a ranking scheme similar to the one used above in which you assign potential consequences to severe, high, medium, or low categories. Combining consequences with their "likelihoods" provides you with a measure of risk. Since our "likelihoods" are only approximations of the true probability of a terrorist event, the risk would also be a crude approximation of the actual risk. One way of combining likelihood and consequence to determine risk follows the same approach used above. Take each of the threat-vulnerability combinations (which represent the "likelihood") and place them in the appropriate cell in the following table, depending on how severe the consequences would be if the threat were able to exploit that particular vulnerability.

"RISK"				
CONSEQUENCES				
LIKELIHOOD	Low	Medium	High	Severe
4	2	3	4	4
3	2	3	3	4
2	1	2	3	3
1	1	1	2	2

Of course, you may chose to assign different values to the cells in these tables, but you should focus first on the elements in the top right of the "Risk" table. Anything you place in a cell with a value of 3 or 4, for example, might warrant further attention. Ultimately, you have to decide which vulnerabilities you need to address, but this approach provides you with a method for prioritizing them.

Chapter Two: Security Plan

Your Security Plan should be a complete document and should include: (a) information on your security assessment; (b) how you address any vulnerabilities identified in the assessment; (c) what security measures you have adopted; (d) how, when, and by whom they will be implemented; (e) your organizational structure; and (f) the responsibilities of the various employee positions. In essence, your security plan is the detailed map of how you address the security assessment.

Each motor carrier should evaluate the threats it faces and its vulnerabilities based on its unique operations and facilities and should recognize that a cookie-cutter approach is not appropriate. The measures adopted by your company to address your vulnerabilities do not need to be complex or expensive to be effective, but the justification and rationale to support them needs to be sound and documented. The key to developing adequate security measures is to think

"prevention." Understand that the threat is very real and try to think like a terrorist when assessing your security weaknesses.

A security plan can be formatted using any structure that makes sense for your company. An example of a good model would be to structure or organize it into the following components or sections: Personnel Security, Unauthorized Access, and En Route Security. These areas are specifically required to be addressed by RSPA's HM-232 rule and must be included in the plan in some form.

For each component, it is strongly recommended that you provide a complete description of the relevant specific security measures you will use to reduce your vulnerabilities. You should also discuss personnel roles and responsibilities for implementing each measure. Remember, the most effective security measures do not necessarily involve high-tech or high-cost implementations. Sometimes very simple changes in procedures can achieve the same result as a much more costly equipment-based solution.

Model security plans are available from some vendors and representatives of the hazmat transportation industry that may provide guidance for development of your plan. However, it should be noted that some plans will be more stringent than required by HM-232 and others may not adequately cover all areas addressed by HM-232. Model plans may not address the unique circumstances at each facility or for different types of trucking operations (e.g. truckload versus pickup and delivery). You are responsible for ensuring that any model plan you use has been specifically adapted to your operations. This is particularly true for organizations that have many sites, facilities, or terminals. A corporate-wide plan (and the accompanying security assessment) may not be specific enough to each location to be adopted outright. Additional consideration and modification will probably be necessary for each location.

Part A. Primary Security Objectives

While many security plans are developed by matching specific security measures to the vulnerabilities identified in a security assessment, we recommend taking a step back to think about what you want each security measure to accomplish. Your security plan should include specific objectives/goals and measures for your company and its employees. These are your primary objectives.

For example, you determine that your facility is vulnerable to a terrorist bringing a weapon into your facility. You already have a fenced facility and have located visitor parking outside the front gate. Your main goal is to prevent an armed terrorist from entering through the front gate. Your first thought may be to set up airport-type screening that includes a metal detector and an X-ray machine at the front gate. Such devices are very expensive and require a staff that is well-trained in screening procedures. There are other things you can do to achieve the same goal at a lesser expense. You could use guards with magnetic wands to detect weapons that people are carrying and they could manually inspect bags and briefcases. You may even forgo the wands and rely only on visual weapons checks. All these approaches can be equally effective with properly trained employees, yet each is progressively cheaper to implement.

A real-world example proves the value of this approach. A transit agency on the West Coast recently completed an extensive security review. It was recommended that they implement a very costly (millions of dollars) group of measures to protect their buses while they were in the yard. These included additional fencing and lighting, intrusion detection systems, extra guards and patrols, guard dogs, and more. A second review determined that all they wanted to do (their primary objective) was to prevent a terrorist from planting a bomb on a bus left overnight in their yard, so that it could be detonated later when the bus was in service and carrying passengers. They determined that adding a couple of new items to their existing pre-trip inspection checklist

(looking in the few spaces where a bomb could be hidden that they were not already checking) would meet that objective. The cost for this procedure was minimal, saving millions of dollars.

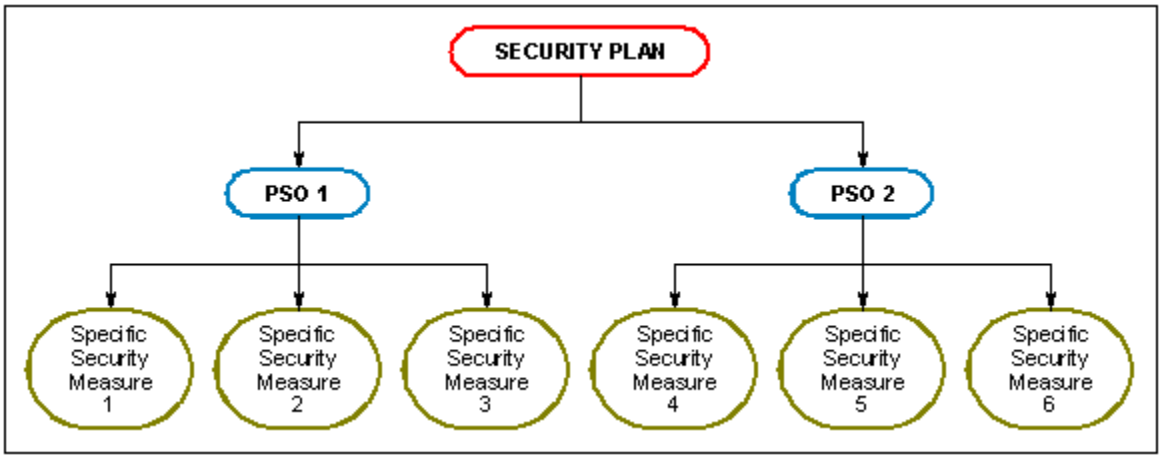
As long as your measures meet the primary objective, you have done your job. Choosing the specific measure(s) for each primary objective can be based on any number of factors, including cost and other benefits. In the example above, there may be other tradeoffs to consider, such as the throughput that each method will allow. Many more people per hour can be screened through airport-type security devices than with manual inspection so the former may make sense for a high-volume facility.

Part B. Specific Security Measures

After you identify the primary security objectives (PSOs) for each component of your security plan, you need to identify the specific security measures (or steps) you will implement to achieve each objective. A security measure is a policy, procedure, device, or system that is put in place to reduce one or more vulnerabilities that you may face. If one of your PSOs is to prevent access to hazmat vehicles by non-employees, an appropriate specific security measure might be to require employee identification cards and have a security officer check cards in the area where the hazmat vehicles are parked. Another option might be to park all hazmat vehicles in a secured area and only allow access by employees with identification cards and a signed dispatch order listing a specific vehicle.

It is important to remember that specific security measures can be hardware-based (fences), technology-based (motion detection), policies and procedures oriented (always ask to see the visitor badge of anyone you do not recognize), or training-based (to reinforce policies that may not be followed properly).

The following graphic illustrates how specific security measures are related to the PSOs within a security plan. A security measure that is used to satisfy more than one PSO should be listed (by reference) in each instance and cross-referenced in the event of future changes.



As you identify PSOs and specific security measures (SMs) that are appropriate for your organization, you can use an approach similar to the one used to identify "risk" in Chapter One, Part E to select appropriate SMs. You can determine whether each PSO and the related specific SM you implement will have a high, medium, low, or very low impact (or another, similar ranking) on reducing or eliminating specific vulnerabilities. The reduction or elimination of vulnerabilities is the security benefit of that PSO and its related specific SM. Those PSOs and specific SMs that allow you to significantly reduce your vulnerabilities to the highest level of risks are those that have the greatest benefit. For example, if you are considering one SM that is extremely effective

in addressing a vulnerability to a threat that, when combined with your vulnerabilities and potential consequences, you have placed at the bottom of your risk ranking, you would place that SM in the bottom right cell in the table below (risk=1 and reduction in vulnerabilities=high).

BENEFIT of Security Measures				
REDUCTION IN VULNERABILITIES				
RISK	**Very Low**	**Low**	**Medium**	**High**
4	2	3	4	4
3	2	3	3	4
2	1	2	3	3
1	1	1	2	2

Ultimately, you need to select those PSOs and specific security measures that provide the greatest benefit for the least cost. The "Prioritizing PSOs and Specific SMs" table below can provide you a way to examine the tradeoffs between cost and benefit for each PSO and its related specific SMs. You would most likely want to implement the objectives and associated measures with a value of 4 in this table (high benefit and low cost) before you would implement those with lower numbers. Your assessment of which measures are appropriate for your organization needs to consider all your vulnerabilities and that more than one measure that you are considering may address the same primary objective. In that case, you may only want to implement one of the measures and then focus on finding the best measure for another vulnerability. Of course, you may choose to assign different values to the cells in the table, but the general concept is to focus first on the measures you place in the top right-those with higher benefit and lower cost.

PRIORITIZING PSOs and SPECIFIC SMs				
IMPLEMENTATION COST				
BENEFIT	**Very High**	**High**	**Medium**	**Low**
4	2	3	4	4
3	2	3	3	4
2	1	2	3	3
1	1	1	1	1

Part C. Addressing Varying Threat Levels

The U.S. Department of Homeland Security determines the national threat level based on information it receives from the various security organizations. The five levels of the Homeland Security Advisory System (HSAS) are color-coded based on the assessed threat condition. A low condition (green) indicates a low risk of terrorist attack; a guarded condition (blue) indicates a general risk; an elevated condition (yellow) indicates a significant risk of terrorist attack; a high condition (orange) elevates the level to a high risk; and a severe condition (red) is the highest level, indicating a severe risk of attack and requires the highest level of security.

The national threat level may be increased by one or more levels depending on the nature of any pending threats. For example, if an attack occurred under a guarded threat level (blue), the level would be immediately raised to severe (red). While it is not required that your plan address varying threat levels, it is highly recommended. Some organizations adopt a system with less than five threat levels (for example, often green, blue, and yellow are lumped into a single category, resulting in three threat levels).

Your security plan should address the specific measures or actions to be implemented for each of the threat levels. Again, some of these measures may require only a policy change, while others

may require a company to incur up-front costs at the lowest threat level to prepare for the highest threat level. You must already have the measures identified and ready to be implemented if a "red" threat condition is declared. Here is an example of why you need to think through your measures to see if there may be a problem with implementation. If your plan includes the use of off-duty police officers for security to satisfy a primary objective at orange or red threat levels, you may have a problem. When you need them most (at the red level), they are unavailable - having been assigned to perform other duties. Increased staffing needs for the police at the orange threat level may make them unavailable. Therefore, an alternative strategy or contingency plan would need to be included to address this deficiency.

When considering how to respond to varying threat levels, you should remember that the threat to your operation may be elevated for various reasons, including type of hazmat hauled or location of your facility, even if the national threat level is not raised. For example, there was a recent alert to possible terrorist threats in a state located in the Midwest, but HSAS remained at yellow. Motor carriers operating in that state, however, might have implemented their plans for the orange level. Future threats and alerts could be specific to your location, as in this example, or to your industry.

Some examples of general measures to address the varying threat conditions are provided in the table below [4]. A more specific example is provided at the end of this chapter.

Threat Condition		Measures
LOW	A low risk of terrorist attacks.	General measures include ensuring personnel receive proper training on the HSAS; regularly assess vulnerabilities of all facilities and regulated sectors.
GUARDED	A general risk of terrorist attacks.	In addition to protective measures for low condition, review and update emergency procedures; check communications with drivers and employees.
ELEVATED	A significant risk of terrorist attacks.	In addition to protective measures taken in guarded condition, increase surveillance of critical locations; implement contingency and emergency plans, as appropriate.
HIGH	A high risk of terrorist attacks.	In addition to protective measures for elevated condition, driver should take additional precautions when stopping en route; restrict facility access to essential personnel.
SEVERE	A severe risk of terrorist attacks.	In addition to protective measures for high condition, monitor or constrain driver travel or locations for stopping.

As the table shows, with each increase in threat, additional measures are implemented. Note that while you may implement additional measures as the threat level is raised, you must be prepared for such implementation well in advance of actual implementation. When the threat is elevated, it will be too late to shop for equipment or to train employees.

Part D. Security Plan Components

As discussed above, there are three major components that must be included in your security plan in some form: personnel security, unauthorized access, and en route security. The number and extent of the measures that you choose to implement for each component is solely dependent on your analysis of your threats and vulnerabilities and your determination of the cost-effectiveness of each measure for your organization. A brief description of each component and security general objectives is provided below. More detailed examples of primary objectives and security measures for each component are included in Appendix C.

D.1 Personnel Security Component

Personnel security includes confirmation of identity and credentials. Identification of personnel is the foundation for access control, based on trust. This means a degree of confidence that an individual is who he represents himself to be and has the skills and experience claimed. Higher levels of trust relate to whether the individual can meet various operational safety and security requirements and even whether they are allowed access to secured areas or information systems. For example, to confirm the identity and credentials of job applicants, one security measure that can be used is to check the applicant's motor-vehicle record-a regulatory requirement for commercial drivers.

Personal security and safety of your personnel is an essential element of this component. This begins with the ability of the individual to recognize threatening situations, but must also be supported by systems and infrastructure that provide the capability for a proper response. For example, identifying critical personnel and establishing procedures to protect them are two security measures that you should consider adopting.

D.2 Unauthorized Access Component

How you control access to your site and to important information needs to be addressed in your plan. An example of controlling access to your site might be to install an early-warning system, such as closed-circuit television, to observe your facility externally and to actively monitor critical spaces. Another example might be installing physical barriers. Examples of controlling access to information include requiring passwords, installing a computer-intrusion-detection system, and monitoring Internet activity in your organization.

D.3 En Route Security Component

A vehicle in transit represents not just a moving target, but a critical space under constant exposure to an uncontrolled environment harboring a diversity of threats. A critical space is an area that is essential to your operations, such as a dispatch center, hazmat storage area, or an individual vehicle. When defining primary objectives, it is important to remember that the cargo is the prime source of consequential damage. Security measures that do not link directly to the regulated materials in some way, but just the vehicle, may be of limited value. An example of a security measure for en route security is regular contact with drivers, whether by telephone or by satellite tracking systems. Other security measures might be installation of bypass and shut-down mechanisms or theft-protection devices.

Part E. Example

The following example for a motor carrier with only one small facility will help illustrate the concepts presented in this chapter. We will provide some sample security measures, organized by HSAS threat level, for a primary objective related to personnel security.

Primary Objective: Prevent unauthorized people from entering facility

Sample Security Measures to Implement at Condition Green or Blue

- Implement photo employee ID badge system;
- Establish control and custody process for badges;
- Enforce display of badges for employees and visitors;
- Rely on employees to challenge unbadged individuals;
- Install a fence around facility;
- Install security guard station(s) at gate(s), but leave them unstaffed; and
- Install perimeter lighting.

Additional Sample Security Measures to Implement at Condition Yellow

- Periodically patrol the site and fence line to spot individuals not displaying their badges; and
- Occasionally test employee response to unbadged individuals.

Additional Sample Security Measures to Implement at Condition Orange

- Limit site access to one entrance and exit;
- All visitors must be escorted at all times; and
- Post a security guard at the gate.

Additional Sample Security Measures to Implement at Condition Red

- Deny visitors and vendors access to the site.

Notice that a guard gate is used at a higher threat level (orange), but needs to be installed initially, when the threat is low. Otherwise, it is too late to start constructing one in the hectic situation that will undoubtedly accompany an elevated threat. All physical or hardware-based security measures should be ready to deploy when they are needed.

If you would like to review additional examples of security measures, refer to Appendix C.

Part F. Corporate vs. Terminal Level Planning

A security plan is not a "one-size-fits-all" plan. Each plan for a site or terminal will vary based on the facility layout, design, location, highway access, and operations. In the event your company has more than one terminal, each terminal would need to have a site-specific security assessment, considering its unique characteristics. Each terminal would also need a site-specific security plan developed for and maintained at that facility. Policies or procedures may be set at the corporate level in some cases, but when implemented, may need some modification at the terminal level.

Some companies, such as chemical manufacturers, group their facilities according to the nature of their operations and the types and quantities of materials that they handle. Security planning may be done at different levels of detail for each type of facility, with the more critical facilities getting a very in-depth treatment. Some companies may wish to implement a corporate-wide security plan for each type of facility since those grouped together are very similar. This may not be appropriate! Facilities of similar size and material handling may not have similar threats and vulnerabilities. One may be in a very rural location and another may be very close to a major urban population, critical bridge, or other potential terrorist target. Local law enforcement in one area may be very proactive and effective in deterring terrorist activity and may be understaffed in another area. Also, consider the routes that hazmat vehicles take when leaving your terminals. Your facility may not be in a target-rich environment, but the routes you use may be. Site- and operation-specific analysis and treatment are always required; however, the plan you implement may still be the same.

Chapter Three: Security Training

Security training is important to assuring the integrity of the plan, employee understanding and cooperation, and reducing the company's vulnerabilities. Security training may be categorized based on the type of information provided, level of detail, duration of the training, and level of responsibility of the employee. In addition to hazmat safety training, all hazmat employees must

receive security awareness training and many of them will also require in-depth security training. Training records for each employee must be maintained with the security plan and updated as training is completed. The records must include the employee's name, the most recent training completion date, a description or copy of training materials, the name and address of the person providing the training, and certification that the employee has been trained and tested.

Part A. Security Awareness Training

There is no prescribed format for security awareness training, but it can be delivered in many forms, including classroom, CD, and over the Internet. RSPA provides an awareness training module that can be downloaded at no cost from http://hazmat.dot.gov/hmt_security.htm, or is available on CD at no charge by calling 1 800 467 4922, ext. 3.

Security awareness training is the most basic form of training and must be administered to all hazmat employees no later than the date of the first scheduled recurrent training after March 25, 2003, or by March 24, 2006. Any hazmat employee hired after March 25, 2003 must receive their security awareness training within 90 days. The awareness training must address the security risks involved with hazmat transportation, methods designed to enhance transportation security, and how to recognize and respond to possible security threats.

Part B. In-Depth Security Training

In-depth security training must be provided to each hazmat employee that is responsible for implementing or being aware of any part of the security plan by December 22, 2003. New employees hired after this date must be trained within 90 days. The training should only cover the part of the plan for which the employee is responsible. It would be poor security practice to train employees in areas for which they do not have a need to know. Training could be administered by an instructor in a classroom setting, through the use of computer modules on a CD with quizzes, or with a training video. Hazmat classification-specific training with a security component is available through various organizations or Web sites. Consult with your state or national industry association to identify resources to assist you in developing or delivering your in-depth security training.

The training material and content must include instruction or information on company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure. Use of third-party instruction materials may only augment material that is specific to your security plan. If your security plan accommodates varying threat levels, your in-depth training should inform employees of the policies, procedures, and actions expected of them at each threat level.

Part C. Recurrent Training and Recordkeeping

Currently, the hazardous materials regulations require that all hazmat employees be given recurrent training every three years on the safe handling, packaging, and transport of hazmat covered by the regulations. This training must now include security training. Additionally, the records related to employees' security training must be kept for the previous three years and for 90 days after termination of employment, as is required for other training.

Chapter Four: Security Plan Administration

Administration of the security plan requires a commitment from management to document its operating policies and procedures, complete a threat and vulnerability assessment, and dedicate time and resources to develop the security plan and prepare for implementation, if necessary.

Part A. Distribution and Availability

The security plan should be a written document that is secured in a location accessible to employees with the appropriate company security clearance (managers, supervisors, security officers) during the normal operating hours of the facility. The plan should not be openly distributed, but components of the plan must be available to those employees who are responsible for implementing it. Due to its sensitive nature, the plan is not a public document and should never be released to any outside party without a verified and appropriate need to know.

As with any sensitive information, it is important to develop and rigorously follow a system of logging and tracking access to the security plan. It is important to know the name of every individual who has a copy of the entire security plan and know where it is kept. It may be useful to label each page of the plan with a "plan clearance level" or similar concept that would indicate the employee type or company clearance level to which that page applies. This would help ensure that portions of the plan were not inappropriately distributed to the wrong employees.

The security plan must be made available to FMCSA investigators conducting official business as part of security contact reviews or compliance reviews.

Part B. Updates and Maintenance

Administration also includes monitoring the security plan implementation, including all components, primary objectives, and specific measures to identify appropriate changes that should be considered. This activity could involve employee, vendor, and customer feedback on security measures, review of the reported security breaches, and periodic testing of security measures for weaknesses. In addition, communication to and from employees and continuous improvement to the plan, where warranted, are key elements of plan administration.

It is very important to review both the security assessment and the security plan periodically to ensure that both reflect current conditions. For large, complex companies or operations, it may be appropriate to review the assessment and the plan every year, while a review every three years may suffice for more simple operations. The assessment and the plan should be examined when the threat level changes, particularly if accompanied by specific information on the nature of the threat.

Any regulatory changes affecting any component of the plan will need to be considered and incorporated into the plan, if necessary. Of course, any revisions to the plan must be communicated to affected employees, and all written copies must be updated simultaneously and consistently. This requires careful implementation to ensure that no old versions of the plan remain in use. One possible solution is to require the return of all old copies to a central location where they are checked off of a master list. It is good practice to include a version number and date on all pages of the plan.

Part C. Verification and Evaluation

Once you have developed and implemented your security plan, it is crucial that it is followed completely and consistently. You should establish procedures for verifying that your employees, contractors, and others are performing their responsibilities as outlined in your plan. As discussed in Part D below, you may employ outside parties, such as local law enforcement or industry partners, to assess your plan and how it is being implemented. You may also wish to test your plan with mock surveillance, phony job applicants, or other staged events to see how your plan works under actual conditions.

You should also develop performance measures for your plan to see if it is making a difference in your vulnerabilities. For example, did the new measures that you implement reduce theft or property damage? You should develop a schedule for examining the performance measures you select and assessing your plan's performance.

These steps will help you identify changes that can make your plan more effective.

Part D. Coordination, Cooperation, and Liaisons

There can be great benefit from expanding your efforts to include other partners in your security planning process. Contract carriers may wish to discuss the security of the hazmat that they transport with their shippers and consignees, particularly because they will operate within their facilities. It is important to understand how the security measures that each party implements will work with, or against, each other.

Your own industry groups are also a good source for new ideas on approaches to specific security problems and information on best practices. As discussed earlier, your industry may have developed its own guidance for you to follow. Just be sure that you are addressing the regulatory requirements as they relate to your specific operations.

An excellent source for security advice is your local law-enforcement community, including the local and state police, the FBI, and your state Bureau of Investigation. These individuals, or consultants with experience in these organizations, can be a great help in exploring your vulnerabilities as part of the security assessment. They can be used as third-party auditors to provide an independent, unbiased review of your final security plan.

Appendix A: Understanding the Security Threat

In the months following September 11, 2001, the media reported several incidents that provide real-life examples of why carriers and drivers of hazardous materials must plan and adopt security measures to prevent terrorists from commandeering their vehicles and loads. A summary of some of the incidents is provided below to assist you in understanding potential vulnerabilities and how a terrorist could acquire and use hazmat to inflict casualties or induce fear and panic. None of the domestic incidents listed have been proven to be terrorist-related, but they remain suspicious. Hijacking a tractor-trailer loaded with hazmat that could be used as a weapon of mass destruction (WMD) can no longer be dismissed. Knowing more about terrorists and their tactics can help us achieve our goal of preventing terrorist acts from occurring or succeeding.

- In Mexico, a tractor-trailer loaded with 76 drums of cyanide was hijacked on May 10, 2002. Six days later, it was recovered along with all but six drums of the cyanide. The perpetrators were only interested in the truck and not the hazmat [5].
- Two incidents in March 2003 in the U.S., within two days of each other, in the same Midwest state illustrate the potential threat posed for drivers of hazmat CMVs. First, a late-model white GMC Yukon pulled up alongside a fuel tanker truck and tried to force, at gunpoint, the truck driver to pull over. The Yukon flashed blue and red lights in its grill and had no license plates. Two days later a late-model blue Volvo with temporary Delaware tags passed a tractor-trailer on I-70. The suspicious activity of the car driver and occupant alerted the truck driver that he might be a potential target for a hijacking. A few minutes later, another car with temporary Delaware tags and two similar individuals came alongside and did the same thing. The truck driver slowed down as he neared his exit and called the state police. The car passed him and took off.
- On April 14, 2003, the FBI issued an alert in California and Oklahoma following the theft of a truck transporting 280 propane bottles. There were other reports of small propane bottles being stolen and one 500 gallon propane bottle.

- In June 2003, an Ohio truck driver pleaded guilty to two felony charges: conspiring with al Qaeda to blow up the Brooklyn Bridge and conspiring to derail a freight train.
- On May 23, 2002, a diesel fuel tanker truck departed Israel's largest fuel terminal in Haifa, Israel, for a delivery run. Terrorists planted explosives on the truck while en route, undetected by the driver. When the truck had returned to the depot and was being reloaded, a remote-controlled detonation caused an explosion and fire. The fire was barely contained before the ignition of nearby LNG tanks.

Part A. Terrorist Profiles

In a 1999 retrospective report on terrorism, the FBI classified terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorists [6]. There are many types of terrorists. Domestic terrorists may be delusional individuals (the Unabomber and Timothy McVeigh), extreme fringe groups (some animal rights and environmental groups), religious cults, or political resistance fighters (including some so-called "militias"). International terrorists may also include some of these groups, such as the religious cult Aum Shinrikyo, in addition to groups like al Qaeda [7].

To begin to think like a terrorist and, thus, identify vulnerabilities and weaknesses in your hazmat operations, you should begin with an understanding of what motivates an individual or a group to commit a terrorist act. For instance, al Qaeda is considered a special threat to United States citizens and is a group that is difficult to fight. It has the resources of a government without any of the responsibility. It is an umbrella organization with a single point of contact for multiple militant groups. It has about 700 core members from many countries and thousands of supporters all over the world. It chooses targets that are symbolic of its declared enemy, the United States. Its members are devout followers of Osama bin Laden, not just willing but eager to become the instrument of delivery in a terrorist act, such as September 11, 2001 demonstrated [7].

Part B. Terrorist Operations

B.1 Operational Acts Needed to Carry Out an Attack

Terrorist organizations, such as al Qaeda, are characterized by meticulous planning, a focus on inflicting mass casualties, and multiple and simultaneous suicide attacks. The operatives are highly trained in basic and sophisticated surveillance techniques. In fact, surveillance is only one step in a sequence of operational acts that a terrorist must complete to pull off a successful attack. These steps are the following:

- Targeting-terrorists first must identify a target based on their primary objectives or motivations. This could include actions designed to inflict huge casualties or significant economic disruption, attacks on facilities or buildings with significant iconic value, such as monuments, and/or actions that will result in high media exposure. Your operation may provide terrorists the equipment or materials needed to attack their target. If so, then you are a target, too!
- Casing-this is the careful examination of the terrorists' plan of attack. They will think through all the steps and what might stop them. They may try to get copies of your security procedures or plan.
- Surveillance-a close observation of the elements of their plan. They may watch a facility to determine how many visitors, deliveries, and employees come and go and how often. Is there a regular pattern, such as during shift changes?
- Rehearsal-rarely do terrorists carry out an attack without first testing out their plan. They may stop in front of a truck to see what the driver does. They may set off your perimeter motion-detection system to test your response time.

- Attack-looks just like a rehearsal, except it doesn't end the same way. The goal of a security plan is to develop sufficient security measures to prevent them from getting to this stage at all!

The following is a list of possible indicators of terrorist casing or surveillance. The list is not exhaustive, but provides examples of suspicious activity for which hazmat carriers and their employees should be alert:

- Unusual or prolonged interest in security measures or personnel, entry points and access controls, or perimeter barriers, such as fences or walls;
- Unusual behavior, such as staring or quickly looking away from personnel or vehicles entering or leaving designated facilities or parking areas;
- Increase in anonymous telephone or e-mail threats to facilities in conjunction with suspected surveillance incidents-indicating possible surveillance of threat reaction procedures;
- Foot surveillance involving two or three individuals working together;
- Mobile surveillance using bicycles, scooters, motorcycles, cars, trucks, or small aircraft;
- Prolonged static surveillance using operatives disguised as panhandlers, demonstrators, shoe shiners, food or flower vendors, news agents, or street sweepers not previously seen in the area;
- Discreet use of still cameras, video recorders or note taking at non-tourist type locations;
- Use of multiple sets of clothing, identifications, or the use of sketching materials (paper, pencils, etc.); and
- Questioning of security or facility personnel [8].

B.2 How Terrorists Pick Their Targets

The Department of Homeland Security (DHS) issued an information bulletin following the terrorist attacks in Riyadh, Saudi Arabia. The May 15, 2003, information bulletin provides potential indicators of threats involving Vehicle-Borne Improvised Explosive Devices (VBIEDs) to alert the public of possible terrorist planning and encourage the reporting of suspicious activity. The characteristic tactics used in the Riyadh attack were multiple targets, simultaneous attacks, multiple vehicles per target, and an "assault/breaching cadre" armed with small arms/weaponry accompanying the VBIED to clear security personnel and gain access for the suicide bombers.

While most non-bulk hazmat is not easily weaponized, the following classes of hazmat, when transported in sufficient quantities, are likely to be particularly attractive to terrorists because of their potential to inflict mass casualties or significant psychological trauma: explosives (Class 1); radioactive materials (Class 7); gases or liquids that are poisonous by inhalation (Division 2.3 or Division 6.1); flammable gases or liquids (Division 2.1 or Class 3); certain organic peroxides (Division 5.2); certain biological materials (Division 6.2); and certain flammable solids (Class 4). However, other types of hazmat may also be terrorist targets because they can be used to manufacture or construct bombs or other weapons.

The most likely terrorist attack profiles for hazmat transported by commercial motor vehicle are theft, interception and diversion, and legal exploitation. For simplicity, diversion is considered a special case of interception. Theft is the taking of hazmat by means of stealth, deception, or force. Interception is the instantaneous theft with the cargo released and/or detonated or ignited while still in the control of the carrier. Diversion is a special case of interception in which the carrier is directed off its intended route and to a predetermined target. Legal exploitation would be acquiring hazmat by commercial transaction or diversion using insiders.

The attack profile used by terrorists will vary depending on such factors as the type of hazmat transported, type of transportation used, and quantity of hazmat (truckload, less-than-truckload). The target and attack profile chosen are based on the attractiveness of a specific profile relative

to others, and a specific material to produce an aggregate impact outcome that maximizes the following:

- Mass casualties;
- Significant economic damage;
- Extensive psychological trauma; and
- High symbolic value.

The final determination of the attack profile a terrorist would use considers the following criteria:

- Minimal illegal activity, particularly in the early stages;
- Fewest operational acts;
- Maximizing consequences; and
- High probability of success.

Appendix B: Issues to Consider in Your Security Assessment

This appendix provides additional information that you may consider during your security assessment process. Not all of the issues, operations, or assets discussed will apply to your organization, but they may help you ensure that you have covered all relevant aspects of your operations. It may be beneficial to conduct your analysis without considering the protective measures that you already have in place. This will allow you to determine the vulnerabilities you have that need to be addressed. You can then examine whether your existing measures are appropriate for eliminating or reducing that vulnerability or whether less costly alternatives would do the job.

Part A. Facilities

Each physical facility used in the storage, handling, or transportation of hazmat should be analyzed for potential exploitation by terrorists. As already mentioned in this Guide, only the activities related to hazmat transportation should be considered under the requirements of HM-232. The analysis should consider the following types of facilities.

- Operations large enough to have separate headquarters are likely to use this office facility as a location for consolidation of order information. This concentration of data, including security plans, represents an attractive information-gathering target for a terrorist that is conducting casing operations (casing is discussed in Appendix A, section B.1).
- Carrier terminals are locations from where trucks are dispatched, fueled, loaded, or unloaded. Hazmat at less-than-truckload carrier terminals would be in small quantities and would not stay on site for very long. Dispatch operations are a potential source of information and can be commandeered in an effort to redirect shipments along routes to target locations as part of an attack strategy.
- Some bulk facilities are attended but unsupervised, allowing the driver to load/unload without further assistance and potentially cursory monitoring. Some non-bulk operations may present a sufficient level of activity and potential confusion to cover the diversion of material. Although the presence of hazmat at bulk carrier terminals may be rare because they often leave the terminal empty, obtain loads elsewhere, and proceed directly to the consignee, the equipment used in transport is often stored there. This would not be the case for private carriers that move their own products.
- Intermodal container shipping represents a set of vulnerabilities and security opportunities that are unique. The operational goals of speed and efficiency run counter to awareness and security, placing the security plan at risk to economic pressure. Although this

will be true in all operations, it is most acutely felt at these intermodal facilities, and you might want to pay special attention to them.

Part B. Transportation Assets

Each configuration of rolling stock must be examined for vulnerabilities in light of its intended use and probable routing. Keep in mind that most vehicles represent a critical space adjacent to an uncontrolled space while they are in use. In other words, there is no moderately secure buffer zone that surrounds a truck while en route. This is the most challenging security setting.

For tractors, the issues are relatively straightforward: Who is driving? Is the person authorized to do so? Are they acting appropriately? Also, sabotaging the power units may be a concern you must address.

While the hazmat cargo is the primary concern it is usually not possible to know its status and location directly as this information is most often tied to the vehicle. You may also want to know whether a cargo tank or trailer has been separated from the power unit. You should also be concerned about devices and other contraband placed in or on the equipment to support an attack profile.

Part C. Uncontrolled Support Assets

Transportation beyond local delivery may entail the utilization of facilities owned and/or operated by others. Those facilities or types of facilities most often utilized should be an integral part of the security analysis.

Truck stops are an example where the driver will be separated from the equipment for a significant period. This is mitigated slightly by the presence of other drivers, the awareness of the truck-stop personnel, and a level of activity and mutual vigilance that can occur. To the extent possible, route selection should favor stops that provide some supplemental security in addition to that provided by the individual carriers. Rest/parking areas cannot be relied upon to provide additional security or significant opportunities for mutual support that might be enjoyed at certain truck stops. They are also generally located in remote areas far from a location where suspicious activity or actual terrorist operations could be reported.

The use of safe stopping places provides what amounts to a temporary escape from en route threats and vulnerabilities, trading these in for more predictable threats and vulnerabilities applicable to any facility. The use of a safe stopping place must, therefore, result in a net reduction in vulnerability/consequence, or the en route situation should probably continue.

Hazardous waste is hazardous material without significant economic value. Certain wastes may still possess weapons potential and should be treated as appropriate for their classification. The EPA allows transporters of hazardous waste to store manifested shipments at a transfer facility for ten days or less without being subject to their storage regulations [40 CFR 263.12]. If you use these facilities incidental to transportation, you should consider them in your assessment process.

Part D. En Route Components

Routing may present a variety of security challenges, particularly where alternate approaches or passages are not feasible or available. To the extent that routes can be identified, they should be analyzed for threats, vulnerabilities, and potential consequences (target value). You should also consider the existing FMCSA regulations on the routing of hazardous materials in your assessment of en route vulnerabilities [49 CFR 397]. These requirements include the following:

- Following state and Indian tribe routing requirements;
- Providing drivers of certain explosives with written route plans;
- Ising preferred routes for highway-route controlled radioactive materials;
- Expeditiously delivering hazmat shipments; and
- Other requirements on parking and leaving vehicles unattended.

Where no other specific routing requirements apply to a shipment, FMCSA requires motor carriers to use routes that do not go through or near heavily populated areas, places where crowds are assembled, tunnels, narrow streets, or alleys, with some limited exceptions [49 CFR 397.67(b)].

Explosives, poisons, and flammables all represent significant potential consequences for weapons conversion in a tunnel scenario. Besides their target value, tunnels may also be used to facilitate a theft in a controlled environment.

Long-span bridges, such as suspension bridges, are targets for both their iconic and economic value. The investment in their construction is justified by the commercial and social benefits they provide and are often sources of great pride to the communities that surround and use them. Explosives and incendiaries would be the most likely tools of attack.

Vehicle ferries may present themselves as a target where a large number of passengers are involved, and they can be considered an opportunity to commandeer the vehicle in a controlled situation.

Gaining control of a vehicle against the will of the driver must be accomplished while the vehicle is either stopped or moving slowly. This is cause for including steep grades or switchbacks as a consideration. Downhill grades may also present a vehicle sabotage opportunity where a potential target lies below the route.

Referencing the discussion in Appendix A, part B.2, sporting and convention venues, which present opportunities as densely populated targets; government offices; and many other features near potential routes need to be considered in your assessment. From a route-selection standpoint, alternatives avoiding these potential targets should be developed to accommodate the potential for an attack occurring where the preferred route is unavailable.

Despite the best route planning, not all contingencies can be foreseen. These can be as ordinary as changes in dispatch orders due to customer direction, police and/or emergency activity necessitating route closure and detour, or unannounced construction. How the response to these situations is analyzed is important because the detour offered may be a diversion operation to place the cargo near a target or an opportunity to commandeer the vehicle. You must also consider the routing requirements of 49 CFR 397 and any pertinent routing requirements of the states or Indian tribes' jurisdictions through which you travel. These requirements prohibit travel through or near heavily populated areas, places where crowds are assembled, tunnels, narrow streets, or alleys. Class 7 radioactive materials have even more stringent routing requirements.

Part E. Personnel

Personnel can be exploited for their information and for their responsibilities. They can provide unwitting support or be active participants in an attack operation. They can be developed as assets over months or years or become victims of sudden violence. Personnel are also the single most valuable asset in securing the operation. Technology cannot substitute for continued awareness, informed rational judgment, and responsible actions. You should address employees, contractors, vendors, and customers in your security assessment.

Businesses often underestimate the amount of information that employees possess about day-to-day operations and even strategic decision-making. Casual conversations eliciting anecdotal situations, particularly with those who have long histories with the company, can often reveal information vital to operation planning. Employees should be aware that keeping business confidence is a matter of security with consequences beyond those of a competitive nature.

Employees in otherwise good standing can also undergo life-changing events that can manifest themselves in destructive and violent behavior. Coworkers should be sensitized to indicators that someone may be vulnerable to being influenced or prone to taking violent action. Employee status changes may be used as an opportunity and cause for examining factors and researching information that can reveal potential problems.

Contractors are controlled by the language of the contract. There is a direct relationship between this language and the cost incurred; the more extensive the requirements of the contract, the greater the cost. The economic pressure must be balanced against the need to maintain your planned level of security. From a security perspective, contractors placed in positions where they can directly influence operations, or be exposed to security sensitive information, should have at least the same verifiable character as an employee placed in the same position and preferably more. In addition, contractors and subcontractors who handle hazmat that is subject to security plan requirements should be trained as to their responsibilities under the plan. For example, if a motor carrier contracts with owner-operators to perform hazmat transportation, the carrier is responsible for ensuring that each owner-operator complies with the security plan requirements applicable to their transportation of the hazmat and that the owner-operator is trained. Owner-operators, which are contract operators, provide their own transportation equipment, but the carrier that retains them maintains certain responsibilities. Similarly, contract drivers who use company equipment also need to be trained to adhere to a carrier's security plan.

Vendors should be provided with the information needed to obtain the best price and service and nothing more. It is in the vendor's interest to obtain information about the business for marketing and strategic pricing purposes, but this does not necessarily provide the shipper/carrier with any benefit. Security sensitive information should be closely held and shared with vendors only when sufficient guarantees of confidence have been obtained and there is a strong business need, such as in the formation of a long-term partnership between shippers and carriers.

Customers can be unwitting accomplices to an attack operation. Although good customer service is usually not associated with suspicion, it is appropriate to share your security concerns with your customers. Where customers refuse to act in support of security needs, or create situations of increased vulnerability, a cost/benefit analysis of the relationship may be in order.

Part F. Information Systems

Electronic data is a great benefit as it allows the rapid transfer of important information to decision-makers. This efficiency can also be exploited. Information security must include voice and print as well as electronic data. Security planning and policy may include the following classifications for information:

- Security sensitive-such as security plans and hazardous materials orders;
- Personnel private-such as health and financial information;
- Business confidential-need-to-know business statistics and strategies;
- Commercial transaction-business-to-business that is not security sensitive;
- Workgroup shared-internally shared information; and
- Public-freely available to all.

Some organizations contract out their business systems operations, and if you do, you should consider how this affects your vulnerabilities. Does the outside firm provide sufficient security measures to prevent your information from being inadvertently released to others? What employee screening do they have in place?

Documenting order-processing procedures, including dispatch and other communication, will define the personnel who are covered by security requirements due to business processes. This will also reveal those who have access to information without any responsibility for it. Creating or modifying processes that minimize information exposure may be indicated-remember, this includes voice and print as well as electronic information.

There are two elements of internal computer information security, which would cover your personal computers, servers, local area networks, and intranets. The first is having physical access to the system; the second is having the ability to access the system to retrieve or view the information. Telephone modems are inexpensive, easily attached to a computer, and rarely accompanied by protective firewall software. These present a potential avenue for putting malicious software into the system. E-mail and chat programs are a primary source of business communications and the most likely path that security sensitive information would take to exit the company electronically.

Many operations maintain public and private access to information over the Internet. This provides a low-cost and immediate source of information for customers and employees. The security policy should determine what content is made available. If an outside service is used to host the Web site(s), the opportunity for gaining access to unauthorized information via this offering is nearly eliminated.

Appendix C: Sample Security Plan Measures

Chapter two discusses the recommended use of primary objectives to organize and select the appropriate security measures for your organization, how to vary their implementation as the security threat changes, and how to apply them to varying organizational structures. This section offers more examples on how to structure the primary objectives and select specific security measures that meet them. Again, these are offered only as limited examples and may not be appropriate or sufficient for your organization. You should develop the details of your security plan to address the vulnerabilities that you have identified in your security assessment.

Part A. Personnel Security

Personnel security includes confirmation of identity and credentials. Identification of personnel is the foundation for trust-based access control. This means a degree of confidence that an individual is who he represents himself to be and has the skills and experience claimed. This trust progresses through the ability to confirm compliance with various operational safety and security requirements to sophisticated permission systems in support of information and physical access control. Please review the graduated example below.

Primary Objective: Confirm the identity and credentials of applicants and employees

Sample Security Measures to Implement at Condition Green

- Check motor-vehicle records;
- Have a criminal background check;
- Confirm past employment;
- Confirm Social Security number; and

- Subject to drug and alcohol testing-drug or excessive alcohol use may make the individual more susceptible to blackmail or coercion.

the applicant is applying for a driver position and will be transporting hazardous materials, additional measures should be considered that are more stringent. These measures include the requirements above and also include the following:

- Have a CDL with a current hazmat endorsement; and
- Verify citizenship.

Additional Sample Security Measures to Implement at Condition Blue

- All Hazmat employees are subject to a random check of their background and updating of their personnel files.

Additional Sample Security Measures to Implement at Condition Yellow

- All employees are subject to background checks and confirmation of the information in their personnel file; and
- Applicants are asked to provide two additional references: one personal reference and an additional reference for a former employer.

Additional Sample Security Measures to Implement at Condition Orange

- Review the personnel files of employees who were recently terminated by your company to determine if they may pose a current security threat;
- All employees must use a current credential to access workplaces (no piggybacking through access-controlled areas); and
- Interview applicants only at certain times and dates.

PERSONNEL PROTECTION

Personal physical security as well as safety is an essential component of this planning (although not covered by HM-232). This begins with the ability of the individual to recognize threatening situations. This must also be supported by systems and infrastructure that provide the capability for a proper response. Robust communications, particularly the ability to communicate as well as function under duress, are an essential consideration. Review the graduated example below. Are there other security measures you would add under a particular condition?

Primary Objective: Protect personnel deemed as critical

Sample Security Measures to Implement at Condition Green

- Determine if the organization has personnel deemed as critical;
- Establish procedures for the protection of personnel deemed critical;
- Identify and assess potential safe havens within buildings to use in emergencies (safe havens are areas that are more survivable than other areas in buildings-basements, hallways, inner rooms, or stairwells-and that generally offer a significant barrier to an intruder);
- Inform employees about buildings that contain safe havens;
- Have an emergency evacuation plan;
- Ensure the emergency evacuation plan has escape routes, emergency lighting, and exits; and

- Establish emergency lockdown/shelter-in-place procedures.

Additional Sample Security Measures to Implement at Condition Blue

- Rehearse procedures for the protection of personnel deemed critical;
- Conduct drills moving employees to designated safe havens; and
- Periodically run drills to test the emergency evacuation plan.

Additional Sample Security Measures to Implement at Condition Yellow

- Ensure that personnel are alerted and familiar with the emergency evacuation plan, and
- Ensure that personnel are familiar with emergency lockdown/shelter-in-place procedures.

Additional Sample Security Measures to Implement at Condition Orange

- Be prepared and implement the emergency evacuation plan or lockdown/shelter-in-place plans, if required.

Additional Sample Security Measures to Implement at Condition Red

- Implement protection procedures for critical personnel; and
- Implement the safe-haven plan.

Part B. Unauthorized Access

Access control is usually associated with either information or an enclosed space. In either case, the basic organization and approach to defining the control strategy should be as follows:

EXTERNAL SURVEILLANCE

Primary Objective: Provide awareness of the area outside the protected space, so that early warning of possible unauthorized access is provided

Review the security measures below. What others can you think of?

- Install closed-circuit television (CCTV) to observe your facility externally and actively monitor its view of critical spaces;
- Increase perimeter lighting;
- Have security/law enforcement periodically check identified covered observation posts that can observe the site;
- Have security/law enforcement periodically check identified cover/concealment opportunities for criminals or terrorists around the site; and
- Have security/law enforcement periodically check located infiltration/egress routes for criminal or terrorist use around the site.

OBSTACLES AND BARRIERS

Obstacles and barriers provide the ability to prevent, discourage, or delay entry into the protected space at its outer boundaries. Another graduated example is provided below. Is this approach starting to make sense?

Primary Objective: Maintain a physical safety system

Sample Security Measures to Implement at Condition Green

- Install a fence around the site;
- Fenced sites should have a "clear zone" inside and outside the fence for unobstructed observation;
- Fenced-in sites should have the capability to have locked, secure gates;
- Install a security alarm system;
- Have sufficient lighting in and around the site; and
- Purchase all necessary equipment for implementation at higher threat levels. A determination will have to be made as to when to install any equipment or devices, even if not used until later. If installation is time consuming, waiting until condition orange or red may be too late.

Additional Sample Security Measures to Implement at Condition Blue

- Periodically check lighting in and around the site;
- Test the security alarm systems;
- Test the site alarm system with local law enforcement; and
- Locking hardware for gates should be case-hardened chain and high-security padlocks.

Additional Sample Security Measures to Implement at Condition Yellow

- Routinely check lighting in and around the site; and
- Rehearse actions required if the security alarm system is activated.

Additional Sample Security Measures to Implement at Condition Orange

- Activate previously installed lighting in areas not routinely covered;
- Activate the emergency law enforcement notification system; and
- Back-up automated access systems with employees.

Additional Sample Security Measures to Implement at Condition Red

- Employ additional portable lighting in and around the site for critical assets, and
- Employ obstacles or barriers in addition to standard fencing. Examples would be using concertina or razor wire to provide a double fence, or placing Jersey barriers to restrict vehicular traffic. While the concertina wire or Jersey barriers would have to already be on site, they can be put in place very quickly.

ACCESS CONTROL

Portals should allow authorized personnel, equipment and material to pass through, and exclude the passage of all else. To accomplish this filtration, it is necessary to identify those who have entrance permission. Possession, such as the use of a key, is the most passive form of confirmation, progressing to biometric and confirmation of access systems that can be real-time updated.

Primary Objective: Maintain control of everyone entering the facility

Sample Security Measures

What other measures would be appropriate for your operations?

- Determine if employee identification badges are required;
- Establish a control and custody process for the identification badge program;
- Enforce display of badge for employees while at work;
- Require photo identification badges;
- Limit site access to one entrance and exit;
- Post security guard at gate(s) if not routinely done; and
- Deny visitors, vendors, and job applicants access to the site.

INTRUSION DETECTION

The protected space should not rely totally on boundaries and access controls. Confidence in the protected space can be maintained by an awareness of activities, comparing this awareness with established norms to recognize aberrant conditions.

Primary Objective: Detect unauthorized entry into the facility

Sample Security Measures

Once again, can you come up with other measures?

- Train employees to recognize unauthorized people inside the facility;
- Institute periodic roving patrols of the facility perimeter;
- Install a property alarm system;
- Integrate alarm systems with security force and regularly exercise and check for reliability;
- Tie site alarm system into local law-enforcement department;
- Have a video camera monitor areas not under direct observation;
- Employ explosive detection devices; and
- Use metal detectors/x-ray machines to screen personnel, visitors, and bags.

COMMUNICATION AND REPORTING

Fire alarms, intercoms, dedicated communication stations, and similar assets can be employed in support of detection and response protocols. These capabilities can be employed in non-traditional ways to augment security requirements. Graduated examples are listed below. Review these and, as before, see if you can develop other primary objectives and security measures that would apply.

Primary Objective: Maintain positive communication with driver

Sample Security Measures to Implement at Condition Green

- Implement a predetermined communication plan with drivers and dispatch;
- Driver and dispatcher communicate as needed via cell phone or radio; and
- Purchase equipment and plan for primary, secondary, or tertiary means of communication. As mentioned previously, a determination will have to be made as to when to install any equipment or devices, even if not used until later.

Additional Sample Security Measures to Implement at Condition Blue

- Driver and dispatch maintain regular daily communication via cell phone or radio; and
- Train with new equipment and test your plan for primary, secondary, or tertiary means of communication.

Additional Sample Security Measures to Implement at Condition Yellow

- Implement plan for primary and secondary means of communications,
- Driver and dispatch maintain communication every eight hours via cell phone or radio;
- Ensure dispatchers are familiar with drivers and their voices, and vice versa; and
- Employ radio and Internet deceptive measures for routes, times, and deliveries.

Additional Sample Security Measures to Implement at Condition Orange

- Employ tertiary means of communications to augment primary and secondary means; and
- Driver and dispatch maintain communication every four hours via cell phone or radio.

Additional Sample Security Measures to Implement at Condition Red

- Driver and dispatch maintain communication every two hours via cell phone or radio; and
- Increase frequency of GPS satellite location messages, if used, for certain high-hazard materials.

DISPATCH AND RESPONSE

The response capability should be described in terms of timing, capability, and quantity. Any response that can disrupt or otherwise degrade a potential attack scenario, without placing additional people at risk or otherwise raising the potential target value, may be considered as a security measure. Can you think of other security measures besides those listed below? What could be some primary objectives that the security measures would address?

Sample Security Measures

- Establish procedures for retaining essential employees on site;
- Have an emergency notification plan for employees (e.g., calling tree);
- Plan for emergency closure, including procedures;
- When a shipment is delayed, late, or does not arrive as scheduled, have an emergency procedure in place for notification;
- Conduct drills and rehearsals with the security response force; and
- Implement predetermined alternate routes and safe stopping places as necessary.

INFORMATION SYSTEMS

The use of systems can enhance security and allows for the rapid dissemination of information. However, these systems must be secure or protected to prevent intrusion. Once again, some security measures are listed below. Develop one or more primary objectives and then use the measures below, or others you think of, to satisfy each primary objective.

Sample Security Measures

- Initiate a mass notification system for emergencies (public-address system, intercom, alarm);

- Install a computer-intrusion-detection system;
- Monitor Internet activity in your organization;
- Periodically test back-up power for communication systems; and
- Do not pass hazmat shipment data over an unsecured Internet connection.

Part C. En Route Security

A vehicle in transit represents not just a moving target, but a critical space in constant exposure to an uncontrolled environment harboring a diversity of threats. When defining primary objectives, it is important to remember that the cargo is the prime source of consequential damage. Security measures that do not, in some way, link directly to the covered materials, but just the vehicle, may be of limited value.

TRACKING SYSTEMS

Satellite systems and other technologies are excellent examples of graduated security capabilities. The frequency of location and status checks can be varied with HSAS alert levels and tailored to specific materials, reflecting the threat environment and potential consequences. A graduated example of measures is listed below. As you review it, think of what other technology is available to enhance security.

Primary Objective: Employ technology to enhance en route security

Sample Security Measures to Implement at Condition Green

- Plan for primary (phone/cell phone), secondary (radio), and tertiary (satellite tracking) means of communications;
- Install by-pass and shutdown mechanisms;
- Install panic-button option in vehicles;
- Install theft-protection devices to disable fuel, hydraulics, and/or electrical systems;
- Seal tank trailers;
- Driver should always have a communication device readily available to him, and
- Purchase all other necessary technology devices to be installed.

Additional Sample Security Measures to Implement at Condition Blue

- Train with new equipment and test plan for primary, secondary, and tertiary means of communications;
- Routinely use primary means of communications; and
- Use high-quality hitch and trailer pin locks.

Additional Sample Security Measures to Implement at Condition Yellow

- Periodically use secondary means of communication.

Additional Sample Security Measures to Implement at Condition Orange

- Periodically use tertiary means of communication.

CARGO STATUS AND SEALS

A security plan should include measures to minimize the possibility of theft of material from a transport vehicle. Cargo seals, tamper-proof locks, and other technology may be utilized. Some cargo seals are designed to show signs of physical tampering, while others are electronic and can provide wireless notification if breached by an unauthorized individual. Note, however, that a simple locking system may be all that is necessary to deter theft. Of course, seals are not appropriate in all circumstances. For example, it would be counterproductive to use seals for bulk petroleum shipments with multiple drops (unloading).

Sample Security Measures (Can you provide more examples?)

- Check paperwork to ensure it is complete and accurate;
- Inspect cargo manifest and match with cargo;
- See that all tractor/trailer access panels/doors are locked and seals remain intact/undamaged;
- Implement a search plan for tractors and trailers on the site;
- Routinely check truck transits to ensure routing plan is on file prior to departure; and
- Arrange with consignee to notify shipper and carrier if the cargo does not reach its destination.

Appendix D: FMCSA Security Contact Reviews

Due to the terrorist attacks committed on September 11, 2001, and subsequent threats to the transportation system, FMCSA conducted more than 30,000 security sensitivity visits (SSVs) between October 2001 and April 2002. SSVs are face-to-face meetings between FMCSA or state investigators and top carrier officials to assess security vulnerabilities and countermeasures that can improve security. FMCSA then began including SSVs as part of all compliance reviews of hazardous-materials (HM) carriers to maintain a high level of vigilance within the industry. To complement these efforts, FMCSA has initiated a new security program called a security contact review (SCR).

A security contact review is a stand-alone visit to a transportation entity that will evaluate that company's security posture. The goal is to provide assistance and recommendations for security improvements. Security contact reviews will initially be conducted at motor carriers that transport the following high-risk hazardous materials:

- Division 1.1, 1.2, 1.3, in quantities over 55 lbs. and 1.5 explosives in quantities over 1,000 lbs.;
- Division 2.3 poisonous gases in bulk packages as defined in 49 CFR 171.8;
- Class 7 highway route-controlled quantities of radioactive materials; or
- Division 6.1, packing group I materials and Division 2.1 materials in cargo tanks with a capacity exceeding 3,500 gallons.

SCRs will be ranked to focus on those carriers that transport these high-risk materials frequently and in large quantities, or who do not already have advanced security programs. For example, due to the security programs of the Department of Defense and the Department of Energy, an SCR is not necessary for carriers transporting one or more of the above materials under contract to one of these agencies. Also, a carrier that is listed as transporting Division 1.1 explosives may not transport them in quantities exceeding 55 lbs. Therefore this carrier would not warrant a SCR.

If a compliance review or safety audit is conducted on an HM carrier transporting materials warranting an SCR, an SCR should be conducted in conjunction with the review or audit.

The FMCSA investigators conducting the SCRs will complete a security contact review checklist, included at the end of this chapter. The investigator will note any regulatory violations and recommendations for enhancing security and provide them to the motor carrier.

Please note that the SCR checklist is marked as security sensitive information (SSI). This refers to a completed SCR and not the blank form. A completed SCR left with you by an investigator should be treated as you would your security plan. It should not be seen or distributed to people outside your company, or to your employees, without a valid need to know and the appropriate company security clearance.

Security Contact Review

Conducted by: _____

Instructions:

- Treat this document as Sensitive Security Information (SSI) [Need to know basis]. For SSI guidelines, see Volume II, Chapter 4, paragraph 1, subparagraph d of the FOTM for compliance procedures for handling security information.
- All No responses require explanation in the comment section.
- If a question involves several parts, only check "Yes" if ALL conditions are met otherwise, check "No" and discuss in the comment section.
- Use the company's USDOT number as the filename for this document (example: "OOOOOOO.xls");
- Append additional characters if necessary to avoid overwriting older SCRs for the same company.

Applicability

1. Does the organization fall under the provisions of 49 CFR 172.800 requiring the development and implementation of security plans? No Yes

Comments:

2. Security Assessment

3. Has a specific assessment of possible transportation security risks for HM shipments been performed IAW 49 CFR 172.802(a)? No Yes

Comments:

4. Does this Security Assessment adequately capture the specific threats and vulnerabilities faced by this organization IAW 49 CFR 172.802(a)? No Yes

Comments:

5. Does the Security Assessment adequately capture the specific threats and vulnerabilities of personnel security IAW 49 CFR 172.802(a)(1)? No Yes
Comments:

6. Does the Security Assessment adequately capture the specific threats and vulnerabilities of unauthorized access IAW 49 CFR 172.802(a)(2)? No Yes
Comments:

7. Does the Security Assessment adequately capture the specific threats and vulnerabilities of en route security IAW 49 CFR 172.802(a)(3)? No Yes
Comments:

8. Does the organization periodically assess its security posture IAW 49 CFR 172.802?
Comments:

9. **Security Plan**

10. Does the Security Plan correlate to the Security Assessment in question 2 above IAW 49 CFR 172.802(a)? No Yes
Comments:

11. Is the Security Plan "specific" to the organization IAW 49 CFR 172.802>
Comments:

12. Is there a written procedure on actions to take in the event of a security breach(see 49 CFR 172.704(a)(5))? No Yes
Comments:

13. Does the organization have an Oil Spill Prevention and Response Plan IAW 49 CFR Part 130? No Yes
Comments:

14. **Personnel Security**

15. Does the Security Plan contain a section addressing personnel security IAW No□ Yes □49 CFR 172.802(a)(1)?
Comments:

16. Is the Security Plan's approach to personnel security operation specific IAW No□ Yes □49 CFR 172.802(a)?
Comments:

17. Are the Security Plan's personnel security measures appropriate for the No□ Yes □security assessment as written IAW 49 CFR 172.802(a)?
Comments:

18. Are the Security Plan's personnel security measures adequate IAW 49 CFR □ Yes □172.802(a) even if the security assessment did not identify all risks? No
Comments:

19. Are the Security Plan's personnel security measures security assessment did No□ Yes □not identify all risks?
Comments:

20. Do all drivers required by 49 CFR 383.23(a) to have valid CDLs with required No□ Yes □endorsements have them?
Comments:

21. Does the organization conduct required background checks on drivers IAW 49 No□ Yes □CFR 391.23?
Comments:

22. Does the organiation tke measures to confirm information provided by job applicants hired for positions that involve access to and handling of the HM No□ Yes □covered by the Security Plan IAW 49 CFR 172.802(a)(1)?
Comments:

23. **Unauthorized Access**

24. Does the Security Plan contain a section addressing unauthorized access IAW No□ Yes □49 CFR 172.802(a)(2)?
Comments:

25. Is the Security Plan's approach to unauthorized access operation specific No□ Yes □IAW 49 CFR 172.802(a)?
Comments:

26. Are the Security Plan's unauthorized access measures appropriate for the No□ Yes □security assessment as written IAW 49 CFR 172.802(a)?
Comments:

27. Are the Security Plan's unauthorized access measures adequate IAW 49 CFR □ Yes □172.802(a) even if the security assessment did not identify all risks? No
Comments:

28. Are the Security Plan's unauthorized access measures being followed IAW 49 No□ Yes □CFR 172.800(b)?
Comments:

29. **En Route Security**

30. Does the Security Plan contain a section addressing en route security IAW 49 No□ Yes □CFR 172.802(a)(3)?
Comments:

31. Is the Security Plan's approach to en route security operation specific IAW No□ Yes □49 CFR 172.802(a)?
Comments:

32. Are the Security Plan's en route security measures appropriate for the No□ Yes □security assessment as written IAW 49 CFR 172.802(a)?
Comments:

33. Are the Security Plan's en route security measures adequate IAW 49 CFR □ Yes □172.802(a) even if the security assessment did not identify all risks? No
Comments:

34. Are the Security Plan's en route security measures being followed IAW 49 CFR No□ Yes □172.800(b)?
Comments:

35. **Security Plan Administration**

36. No□ Yes □Is the Security Plan written IAW 49 CFR 172.802(b)?
Comments:

37. Is the Security Plan r No□ Yes □etained IAW 49 CFR 172.802(b)?
Comments:

38. Are copies of the Security Plan(or relevant portions of it) available to □ Yes □employees who are responsible for implementing it IAW 49 CFR 172.802(b)? No
Comments:

39. Are all copies of the Security Plan updated and revised as necessary to No□ Yes □reflect changing circumstances IAW 49 CFR 172.802(b)?
Comments:

40. **Security Training**

41. Does the training program contain Security Awareness Training IAW 49 CFR No□ Yes □172.704(a)(4)?
Comments:

42. Has Security Awareness training been provided to all hazmat employees no later than the date of the first schedule training after March 25, 2003 or by No□ Yes □March 24, 2006 IAW 49 CFR 172.704(a)(4)?
Comments:

43. Does the Training material contain In-Depth Security Training IAW 49 CFR No□ Yes □172.704(a)(5)?
Comments:

44. Has In-Depth Security Training been provided to all hazmat employees with responsibility for implementing the Security Plan by December 22, 2003 IAW 49 No□ Yes □CFR 172.704(a)(5)?
45. Does the In-Depth Security Training Material contain company security objectives IAW 49 CFR 172.704(a)(5)?
Comments:

46. Does the In-Depth Security Training material contain organization-specific No□ Yes □security Plan for personnel security IAW 49 CFR 172.704(a)(5)?
Comments:

47. Does the In-Depth Security Training Material contain organization-specific security procedures derived from the Security plan for unauthorized access IAW No□ Yes □49 CFR 172.704(a)(5)?
Comments:

48. Does the In-Depth Security Training Material contain organization-specific security procedures derived from the Security Plan for en route security IAW 49 No□ Yes □CFR 172.704(a)(5)?
Comments:

49. Does the In-Depth Security Training Material contain employee responsibilities IAW 49 CFR 172.704(a)(5)? No Yes

Comments:

50. Does the In-Depth Security Training Material contain actions to take in the event of a security breach IAW 49 CFR 172.704(a)(5)? No Yes

Comments:

51. Does the In-Depth Security Training Material contain the organizational security structure IAW 49 CFR 172.704(a)(5)? No Yes

Comments:

52. Is the Security Training Program correctly administered IAW 49 CFR 172.704(c) and (d)? No Yes

Comments: