

# **SECURITY AND EMERGENCY PREPAREDNESS PLAN TEMPLATE**

Prepared By:

Daecher Consulting Group, Inc. for the American Bus Association and the United Motorcoach Association through a grant from the Department of Homeland Security, Office of State and Local Government Coordination and Preparedness Grant. The views and opinions of authors of reference materials expressed herein do not necessarily reflect those of the United States Government. Reference within this document to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The information and statements contained within this document shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the United States Government.

10/03/05

## Table of Contents

<i>How To Use This Document</i> .....	1
<i>Purpose and Background</i> .....	2
<i>Terrorist Profiles and Operations</i> .....	4
<i>Risk Assessment for Transportation Sector Service Providers</i> .....	7
<i>Glossary of Terms</i> .....	13
<i>Section 1: Motorcoach Operator Self-Assessment for Operations Security and Response</i> .....	16
Management Structure & Operating Process.....	18
Personnel: Information .....	20
Personnel: Training and Enroute Procedures .....	21
Facility/Terminal Security .....	22
Passenger & Baggage Screening .....	24
Cyber Security .....	25
General Emergency Response Capabilities.....	26
Business Continuity .....	26
<i>Section 2: Risk Assessment</i> .....	28
What Is a Risk Assessment? .....	29
Threat Identification and Assessment .....	29
Vulnerability Assessment.....	30
Consequence Assessment .....	31
Calculation of Risk .....	31
Prioritizing Needs .....	32
Threat Matrix .....	33
Vulnerability Matrix .....	34
Consequence Matrix.....	35
Risk Matrix .....	36
<i>Section 3: Security and Emergency Preparedness Plan Guidelines</i> .....	37
Title Page .....	38
Division of Responsibilities .....	40
All Personnel .....	40
Chief Executive Officer (CEO).....	41
SEPP Point of Contact (POC) .....	41

Security Committee (SC) .....	42
Supervisors .....	43
Drivers .....	44
Other Personnel .....	44
Other Critical Roles and Responsibilities.....	45
Security & Emergency Preparedness Practices & Actions.....	46
Training and Exercising.....	47
Coordination with Public Safety Agencies .....	47
Coordination with Other Companies.....	48
Evaluation .....	48
Internal.....	48
External .....	48
Modification and Update .....	48
<i>Section 4: Emergency Response Procedures Guidelines .....</i>	<i>49</i>
Sample Emergency Contact Directory .....	51
Emergency Response Procedures.....	52
Recommended Operational Procedures to Be Followed Throughout a Security Threat or Incident.....	62
<i>Appendices.....</i>	<i>65</i>
Appendix A: Addressing Varying Threat Levels .....	66
Appendix B: Security Plan Considerations .....	69
Corporate vs. Facility Level Planning .....	69
Security Plan Components.....	69
Unauthorized Access .....	71
Appendix C: Security Issues from the SEPP to be Integrated into Policies and Procedures Governing Fleet Operations .....	77
Appendix D: Considerations for Conducting Emergency/Crisis Response Exercises .....	81
Appendix E: Reference Documents and Helpful Industry Web Sites .....	83
Reference Documents .....	83
Helpful Industry Websites .....	85

# How To Use This Document

This document is a guideline and template that you may use in developing a SEPP. The steps involved in this process include an evaluation of current security procedures, an identification of threats and vulnerabilities to your operation, and the development of policies and procedures to effectively address deficiencies.

**The template is primarily designed to be an adaptable document; however, full customization can be substituted while following the flow of the template.** Following is a review of the sections and appendices:

- The purpose and background for developing a security and emergency preparedness plan as well as descriptions of terrorist profiles and operations and risk assessment protocols establishes the importance and justifications for your efforts in developing your plan.
- A Glossary of Terms, defining frequently used and/or important words found throughout the document, is located in front of the Table of Contents
- Section One is Self-Assessment Checklist. After completing this checklist, deficiencies in your operations relating to security will be identified for your consideration.
- Section Two guides you through the process of identifying and prioritizing the threats and vulnerabilities to your operations. It is intended to help you identify threats for each element of your operations (service, facilities, employees, etc.), and to define vulnerabilities through a numerical ranking.
- Section Three addresses the detailed components that need to be included in your security plan and provides a template to construct the plan. Components include: key personnel and their responsibilities for the use of the plan; specific procedures to be followed during an incident or crisis; training for employees; procedures for employee, facility and operational security; relationship with local, state and federal enforcement/emergency response agencies; and plan review and modification.
- Section Four provides a template for developing Emergency Response Procedures and sample procedures for a security threat or incident.
- The Appendices at the end of this document contain additional support materials. To enhance your use of this document. Each appendix is identified at the beginning of the sections for which they are most applicable.

**This document can be accessed and used to develop your Plan via the web at [www.operationsecuretransport.com](http://www.operationsecuretransport.com)**

## Purpose and Background

The terrible tragedy of September 11, combined with our nation's continuing war on terrorism, has created a heightened threat environment for passenger transportation. In this new environment, the vulnerabilities have become more apparent. Threat assessments issued by the Federal Bureau of Investigation, Department of Homeland Security, and state and local agencies have consistently placed passenger transportation at the top of the *critical infrastructure protection agenda*, along with airports, nuclear power plants, and major utility exchanges on the national power grid. The London bus bombing makes similar threats here more ominous.

To establish the importance of security and emergency preparedness in all aspects of your organization, you should develop a SEPP. The SEPP is the culmination of a process to be used by your company to make informed decisions that are appropriate for your operations, passengers, employees and communities regarding the development and implementation of a comprehensive security and emergency preparedness program.

As a result of this program, your company can achieve not only an effective physical security program, but also enhance your coordination with the local public safety agencies in your service area. Improved communication will increase their awareness of your resources and capabilities, and improve your readiness to support their efforts to manage community-wide emergencies.

The overall purpose of the SEPP is to optimize -- within the constraints of time, cost, and operational effectiveness -- the level of protection afforded to passengers, employees, volunteers and contractors, and any other individuals who come into contact with the company, both during normal operations and under emergency conditions.

The SEPP should provide your company with a security and emergency preparedness capability that will:

- Ensure that security and emergency preparedness are addressed during all phases of operation, including the hiring and training of personnel; the procurement and maintenance of equipment; the development of policies, rules, and procedures; and coordination with appropriate federal, state, and local public safety and community emergency planning agencies.
- Promote analysis tools and methodologies to encourage safe operation through the identification, evaluation and resolution of threats and vulnerabilities, and the on-going assessment of company capabilities and readiness.
- Create a culture that supports employee safety and security and safe operation (during normal and emergency conditions) through motivated compliance with company rules and procedures and the appropriate use and operation of equipment.
- Assist the company in adhering to governmental guidelines, rules and regulations that promote transportation security.

Every threat cannot be identified and resolved, but your company can take steps to be more aware, to better protect passengers, employees, the motoring public, facilities and equipment, and to stand ready to support community needs in response to a major event. To this end, your SEPP should have five objectives:

1. Achieve a level of security performance and emergency readiness that meets or exceeds the operating experience of similarly-sized operations around the nation
2. Increase and strengthen community involvement and participation in the safety and security of our operation
3. Develop and implement an assessment program, and based on the results of this program, establish a course of action for improving physical security measures and emergency response capabilities to manage the identified risks.
4. Expand our training program for employees, volunteers, first responders, and contractors to address security awareness and emergency management issues
5. Enhance our coordination with applicable local, state and federal agencies regarding security and emergency preparedness issues

# **Terrorist Profiles and Operations**

## **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. 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

To begin to think like a terrorist and thus identify security vulnerabilities and weaknesses in your 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 those carried out in New York and Washington on September 11, 2001.

## **Terrorist Operations**

### **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 in order to execute a successful attack. These steps are:

- **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.
- **Casing**—this is the careful development of the terrorists’ plan of attack. They will think through all the steps needed to carry out an attack and what countermeasures 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 passenger 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

## **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.

The most likely terrorist attack profiles for passenger transportation by commercial motor vehicle are bombing, hijacking, and diversion. Bombing is the placing and detonating of explosives on the vehicle. The placing of explosives is accomplished by personal, direct detonation (suicide bombing) or by discrete placement on the vehicle and remote or timed detonation. Hijacking is the control and forcible direction of drivers and passengers for some intended purpose. Theft is the taking of a vehicle owned by a company for some intended



purpose. Diversion is a special case of interception in which the carrier is directed off its intended route and to a predetermined target.

The target and attack profile chosen are based on the attractiveness of a specific profile relative to others 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.

# Risk Assessment for Transportation Sector Service Providers

## Background

The transportation sector, and especially the “open” motor coach element of it, must prepare for and protect its ridership and staff from acts of terrorism to the greatest extent possible.

Traditionally, the motor coach industry has developed internal security and emergency preparedness plans (SEPPs). Limited standards, guidelines and recommendations have been provided, but development of the documentation and approach has been specific to the individual service providers. This situation has been further complicated by inconsistent, state-by-state interpretation of security standards or requirements, resulting in a national patchwork of plans, procedures and guidelines attempting to serve this domain.

To establish a “best practices” planning model specific to the motor coach industry, a baseline of standard elements must be identified. Because this model should address common and unique issues in response to terrorism, a natural starting point for its design is **Homeland Security Presidential Directive (HSPD) 8 – The Interim National Preparedness Goal**. This directive:

"Establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a **National Domestic All-Hazards Preparedness Goal**, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities."

Though this directive was aimed at government entities, its critical elements are also appropriate for industry. Adherence to this directive will provide a uniform approach to SEPP development. This approach focuses on standardized scenarios, universal tasks and agency capabilities, and is designed to address roles and responsibilities pertaining to prevention, protection, response and recovery. This directive focuses on critical elements of capability with regard to: staffing and personnel; training; exercise, evaluation, and corrective actions; equipment and systems; planning; and organization and leadership. By assessing these critical elements, service providers can begin to identify gaps and deficiencies.

The following pages provide a primer on risk analysis for terrorism. The various elements of our nation's transportation system are all changing their business paradigms to account for risk, especially the risk of terrorism. Along with these alterations, a business model has evolved that is intended to balance mitigation and countermeasures, with the requirement not to impede throughput and client services. Consequently, the application of risk management has evolved into a cost-benefit approach to address the most challenging issues with the limited resources available.

## Assessing and Managing Risk: A Primer

The relative value of a potential target can have a major effect on the likelihood of attack. Terrorists will set goals for an attack, such as casualties and economic disruption, or they may choose a target for its symbolic importance. Obviously, a larger relative value for one potential target over another makes it more likely that the site will be attacked. Changes in the relative value of other sites could change the risk of terrorism at a particular site, even if no change has occurred at the site itself.

### Components of Terrorism Risk

- **General Definition of Risk** – Risk is simply the likelihood of an event occurring multiplied by the estimated consequence of that event.

$$\text{Risk} = (\text{Likelihood}) \times (\text{Consequence})$$

Based on this equation, a risk represents the expected outcome over a period of time of some uncertain event.

### Likelihood

In assessing the risk of terrorism, the likelihood of occurrence is the product of two components: the likelihood of an attack occurring (threat) and the likelihood of that attack being successful (vulnerability).

$$\text{Likelihood} = (\text{Threat}) \times (\text{Vulnerability})$$

- **Threat** – The likelihood of an attack occurring is referred to as the threat. If we were to measure this factor in absolute terms, the threat would be equal to the probability of an attack or the frequency of attack on an asset. However, because it is in many instances difficult—if not impossible—to estimate these factors for terrorist attacks, threat must be evaluated on a relative scale.

In this type of analysis, the likelihood of a particular type of attack occurring is driven by two factors: plausibility of attack (i.e., the overall likelihood of a certain type attack occurring, regardless of target) and target attractiveness (i.e., the likelihood that a certain asset would be targeted for that type of attack).

$$\text{Threat} = f(\text{plausibility}, \text{target attractiveness})$$

Plausibility could be driven by a number of factors, including:

- Difficulty in obtaining the type of weapon
- Difficulty in transporting and using the weapon
- Presence of potential threat elements (PTE) in the geographic area
- Past history of attacks

- Specific intelligence.

Target attractiveness measures the features of a particular asset that may make it more or less likely to be targeted by terrorists for a particular form of attack. Evaluation of target attractiveness should include an evaluation of two sets of features: target value and deterrence. Target value evaluates those features of an asset that make it more likely to be attacked or that make it attractive as a target. These may include potential for casualties, potential for economic disruption, and symbolic importance. Deterrence evaluates those features that make a target less likely to be attacked, including security and response capabilities.

- **Vulnerability** – The likelihood of an attack being executed successfully is referred to as the vulnerability. In determining the vulnerability of an attack, it is assumed that the asset has been targeted, the terrorists have the required weapon and equipment, and the attack will take place. Vulnerability measures the probability that the attack will achieve its desired result. The desired result in this case is successful completion of the attack, not the desired results in terms of damage or casualties.

## Consequence

The consequence of a terrorist attack is a function of the total value of the asset (the maximum potential consequence) and the impact that an attack would have on that value. The asset value is sometimes referred to as the criticality of the asset.

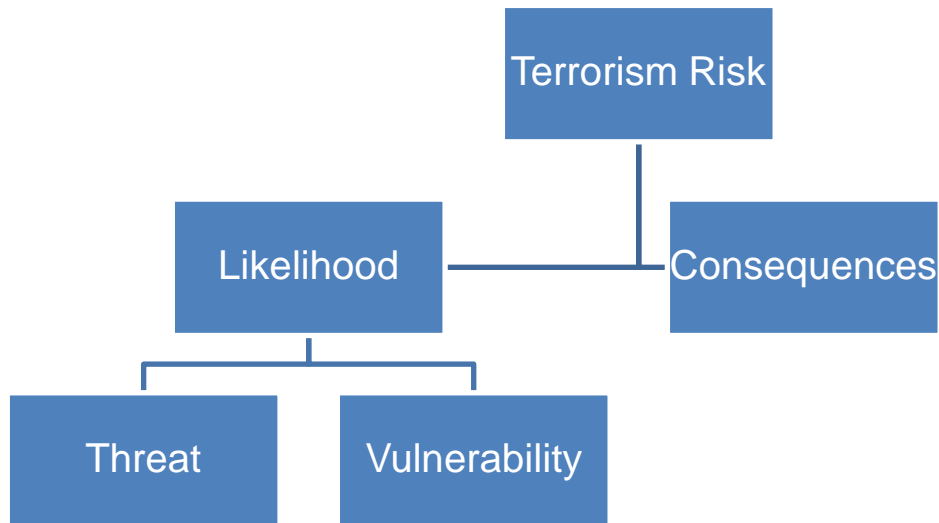
$$\text{Consequence} = f(\text{Criticality}, \text{Attack Impact})$$

- **Criticality** – Criticality is defined by the maximum potential consequence that an attack could have. This value represents the aspects or features of an asset that would make someone want to protect it. Generally, criticality is defined using a set of “Critical Asset Factors.” These factors define the features of an asset that could make it important to protect. Typical critical asset factors include:
  - Potential for casualties
  - Potential economic disruption
  - National strategic importance
  - Potential for environmental impact.
- **Attack Impact** – Criticality serves as the “yardstick” against which consequence can be measured. The evaluation of the criticality of an asset measures the greatest potential consequence of any attack on an asset from the perspective of the assessor. However, not all forms of attack would eliminate this importance. For example; a “backpack” type bomb may kill or injure a number of people at a train station but would not kill everyone in the station or destroy the station itself. For this reason, an evaluation of the expected impact of an attack scenario is completed to determine the portion of asset value that would likely be destroyed. The portion of the asset value is the consequence of the attack.

The evaluation of impact must be tied to the critical asset factors that are used to define criticality. For each asset and critical asset factor, the degree to which the contribution of that asset is destroyed is assessed.

### **Risk Assessment**

The basic equations presented above define the factors that must be included in an assessment of risk. **Figure 1.1** shows the relationship between these factors.



**Figure 1.1 Components of Terrorism Risk**

Three basic components of risk must be evaluated to calculate the level of terrorism risk associated with an attack on a particular asset:

- Threat
- Vulnerability
- Consequence

## Response Capabilities

It is now appropriate to review key components of planning for and responding to scenarios and/or a terrorism event. A key element of this is identifying local capacities for a response. Often this involves a meeting between agencies who, in the event of an incident, will have to work together to address the incident. Dedication and commitment are crucial to pre- and post-event planning. The following are key considerations for those professionals and the respective disciplines in which they serve:

- **Staffing and Personnel** – Field and supervisory staff must understand their responsibilities as non-traditional emergency first responders following a terrorist incident. This understanding includes the ability to: recognize that an emergency has occurred; initiate an emergency response either directly to 911 dispatch or through the agency control center; evacuate the service vehicle in an efficient manner; and secure the service vehicle, preventing bystanders from entering a potentially hazardous scene. Service providers should review staff responsibilities following emergency events and ensure a clear understanding of policies and procedures.
- **Training** – All staff with assignments and responsibilities in operations and/or communications should have appropriate weapons of mass destruction awareness training. This training should provide the necessary education and information to ensure the safety of staff and riders. Additionally, field supervisors are typically expected to provide critical technical representation in an incident command system situation. Incident command and management training is essential in establishing the required knowledge base to provide seamless technical support following an emergency, in addition to providing staff leadership and control. Senior safety and security managers may want to consider the online National Incident Management System (NIMS) training, which will help them gain a perspective on their roles and responsibilities during a response<sup>1</sup>.
- **Exercise, Evaluation, and Corrective Actions** – Motor coach service providers should participate in local, regional, state, and federally sponsored exercises in addition to company-specific events. This participation will provide an environment to initiate networking opportunities, as well as respond to emergency response agency assumptions and potential false premises. In addition, appropriate training in “real-life” situations will instill staff policies and procedures and validate operational plans, policies, and procedures. It is imperative that service providers view their system not only as a point of attack but also as a means for assisting in response to an attack. The use of various elements of the transportation sector for triage, evacuation, and all facets of emergency response is a key element of consequence management.
- **Equipment and Systems** – Motor coach services should coordinate active communication systems with area emergency response agencies in jurisdictions serviced by the provider. Communications systems include internal and external interoperability (the ability to exchange radio communication capabilities in a seamless manner), system

---

<sup>1</sup> The online course may be located at <http://www.nimsonline.com/>

redundancy, notification capacity (internal and external to the service provider), integrated communications plans with local emergency management, system linkage (ability to send and receive voice messaging or radio traffic to all service vehicles), and a panic priority system (designed to provide the service vehicle priority emergency communications with the appropriate control center).

- **Planning** – Service providers should review existing emergency operations plans, policies, and procedures. HSPD 8 identifies the inclusion of Terrorism Incident Annexes (designed to provide unique emergency response and operations roles, responsibilities, and tasks following a terrorist incident) as a priority. Additionally, emergency operations plans should be shared with local emergency management offices for technical data support and reference when needed. Planning and preparedness goes beyond documentation. Company officials responsible for supervisory or emergency management assignments must participate in local area emergency planning committees, providing the technical knowledge and support necessary in overall incident command and control. Service providers should provide field staff and vehicle operators with reference cards containing checklists to ensure that assignments and responsibilities are carried out during emergency incidents. All plans, policies, and procedures should be validated and tested through internal and community tabletop, functional, and full-scale exercises. In the event of an elevation of the Homeland Security Advisory System alert level, these plans and procedures should be made available to every employee that makes your company a success. From the safety and security personnel to the drivers and senior administrative personnel, knowledge of these guiding principles may save lives and time.
- **Organization and Leadership** – Motor coach service providers must identify management personnel who will be responsible for representing the company at command center facilities. Acts of terrorism will likely require representation at a variety of operations centers at the local, state, and/or federal levels, in addition to the service provider's own command and control center. Relying on a single employee to represent the company needs will result in a significant delay in relaying potentially critical information at the appropriate command level. Additionally, those tasked to represent the service provider should have the appropriate incident command and emergency management training. Service providers should implement an internal emergency command committee that reviews their policies and procedures in response to an emergency, in addition to providing appropriate incident command and emergency management training.

## Glossary of Terms

Critical Incidents:	Accidents, natural disasters, crimes, terrorism, sabotage, civil unrest, hazardous materials spills, service interruptions, power outages and other events that require emergency response. Critical incidents require swift, decisive action from multiple organizations, often under stressful conditions. Critical incidents must be stabilized prior to the resumption of regular service or activities.
Emergency:	A situation which is life threatening to passengers, employees, or other interested citizens or which causes damage to any company vehicle or facility or results in the significant theft of services and reduces the ability of the company to fulfill its mission.
Emergency Preparedness:	A uniform basis for operating policies and procedures for mobilizing company and other public safety resources to assure rapid, controlled, and predictable responses to various types of operational emergencies.
Fatality:	An operation caused death that occurs within 30 days of the incident.
Injury:	Any physical damage or harm to a person that requires immediate medical attention and hospitalization.
Operation:	A composite of people (employees, passengers, others), property (facilities and equipment), environment (physical, social, institutional), and procedures (standard operating, emergency operating, and training) integrated to deliver an intended service or function in a specific environment.
Operation security:	The application of operating, technical, and management techniques and principles to the security aspects of company operations to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.
Operation security management:	An element of management that defines the operation security requirements and ensures the planning, implementation, and accomplishments of operation security tasks and activities.
Operations security Program:	The combined tasks and activities of security management and security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of an operation life cycle.
Safety:	Freedom from danger.



Secure areas:	Locations within facilities that because of equipment locations, information or materials stored, or operations conducted, are restricted to access by selected individuals and/or at specific times.
Security:	Freedom from intentional danger
Security breach:	An unforeseen event or occurrence that endangers life or property and may result in the loss of services or equipment.
Security Committee:	Persons selected by the Company to review, oversee, and provide guidance/direction for security procedures and activities.
Security incident:	An unforeseen event or occurrence that does not necessarily result in death, injury, or significant property damage but may result in minor loss of revenue.
Security threat:	Any source that may result in a security breach, such as a vandal or a disgruntled passenger or employee; or an activity, such as an assault, intrusion, fire, etc.
Threat:	Any real or potential condition that can cause injury or death to passengers or employees or the motoring public or damage to or loss of company equipment, property, and/or facilities.
Threat analysis:	A systematic analysis of operations performed to identify threats and make recommendations for their elimination or mitigation during all activities.
Threat probability:	The probability a threat will occur during the plan's life. Threat probability may be expressed in quantitative or qualitative terms. An example of a threat-probability ranking system is as follows: (a) frequent, (b) probable, (c) occasional, (d) remote, (e) improbable, and (f) impossible.
Threat resolution:	The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.
Threat severity:	<p>A qualitative measure of the worst possible consequences of a specific threat:</p> <ul style="list-style-type: none"> <li>• <b>Catastrophic.</b> May cause death or loss of a significant component of the operation, or significant financial loss.</li> <li>• <b>Critical.</b> May cause severe injury, severe illness, major damage, or major financial loss.</li> <li>• <b>Marginal.</b> May cause minor injury or damage, or financial loss.</li> </ul>

- **Negligible.** Will not result in injury, damage, or financial loss.

Unsafe condition  
/ act:

Any condition or act that endangers life or property.

Vulnerability:

Characteristics of passengers, employees, vehicles, and/or facilities that increase the probability of a security breach.

# **Section 1: Motorcoach Operator Self-Assessment for Operations Security and Response**

---

<b>Management Structure &amp; Operating Process</b>
<b>Personnel: Information</b>
<b>Personnel: Training</b>
<b>Facility/Terminal Security</b>
<b>Passenger &amp; Baggage Screening</b>
<b>Cyber Security</b>
<b>General Emergency Response Capabilities</b>
<b>Business Continuity</b>

---

The Motorcoach Operator Self-Assessment for Operations Security and Response is a tool that motorcoach companies can use to assess their security needs and response capabilities.

The Motorcoach Operator Self-Assessment for Operations Security and Response is a series of questions designed to help you assess your Company's Security and Response capabilities. Consider each question carefully. If you answer any questions with a "NO", determine its applicability to your company, and determine what actions the company should take to correct the deficiency in the right hand column.

When you have completed this assessment, the company should have a clear understanding of its security and response deficiencies and needs.

## Motorcoach Operator Self-Assessment for Transportation Security and Response

	Yes	No	Action to be Taken
<b>Management Structure &amp; Operating Process</b>			
Am I committed to an activist approach to defeat terrorism?			
Do my “direct reports” know of this commitment? Do they share it?			
Do I have a Security Committee or team made up of senior executives?			
Where is our primary meeting place? Is this location properly equipped for situation assessment and internal and external communication with company assets?			
Where is our secondary meeting location, if the primary location is not functional?			
Can I reach Security Committee members immediately, day or night?			
Can all Committee members reach me immediately, day or night?			
Does the Security Committee meet regularly to discuss plans, operating procedures and security information?			
Does the Security Committee monitor threat data, including the U.S. threat color-code?			
Does the Security Committee meet with federal, state, and local law enforcement, security and emergency response units? If so, which ones?			
Are written minutes or other (electronic) records of the meetings kept?			
Does the Security Committee perform (or commission) security vulnerability assessments of the company’s operating units on at least a quarterly basis?			
Has the Security Committee determined what circumstances can harm the operation of the organization?			

	Yes	No	Action to be Taken
Does the Security Committee practice responses to various threat scenarios? Are these drills documented with quantitative (e.g., timed) measurements?			
Does the Security Committee maintain a list of emergency names, telephone numbers, FAX numbers, and email addresses for federal, state, and local emergency responders? Is this list (and copies) kept in safe but accessible places?			
Does the Security Committee monitor external events (e.g., news, CNN, emergency broadcast networks, traffic advisories, intelligence briefings, etc.) to assess possible threats and impacts on operations?			
Does the company have any assets (i.e., land, facilities, equipment, people, and capital) at risk?			
Does a written "risk analysis" exist?			
Has the "risk analysis" been reviewed by any law enforcement, security or emergency response organizations?			
Can all company assets be located within 2 hours?			
Can Corporate Management establish communication with all operating units within 1 hour?			
Is there a plan to remove or minimize the risk in the operation?			
Is there someone within my organization who is responsible for determining the nature, scope and impact of a crisis on our operations and informing me and other affected employees?			
Does the company have a contact list of public authorities with their telephone numbers and names or titles, and a plan for coordinating with these agencies?			
Does the company communicate with other motorcoach companies for crisis coordination?			
Can key staff be contacted during normal hours, nights, weekends?			
Does each employee know what to do during a crisis? (Each senior manager should ask this question.)			

	Yes	No	Action to be Taken
Does the company analyze technical innovations for possible adoption (e.g., tracking devices, communication systems, etc.)?			
Does the company have its own communications, command, and control center?			
Does the company participate with other companies in a collective command and control system?			
Does the company participate with any trade association communications, command and control, or “fusion” center (e.g., American Trucking Association Highway Watch ISAC)?			
<b>Personnel: Information</b>			
Does a complete, accurate and up-to-date list of all employees exist?			
Does the company maintain emergency contact information on its employees?			
Are employees’ identities checked (e.g., Social Security cards, fingerprinting, photographic IDs)?			
Are criminal background checks completed for drivers and other security-sensitive employees?			
Can personnel with names linked to one of the countries that have been identified as supporters of terrorist activities be identified?			
Do these individuals have passports or other documents which indicate travel (business, educational, pleasure) over the last ten years? Have these documents been reviewed?			
Have detailed background checks been performed on these individuals? Have they been personally interviewed by senior management? When was the last time an interview was performed?			
Is U.S. citizenship verified for applicable employees?			
For individuals who are not U. S. citizens, do we have immigration papers on file? (Remember that terrorists can and do obtain U. S. citizenship if they are patient and determined.)			

	Yes	No	Action to be Taken
Does each driver have access clearance (e.g., internal and/or customer facility access credentials, port/airport access badges, local equivalents of the TWIC advocated by TSA)?			
Are written records maintained on these access clearances?			
Are access clearances reviewed on a periodic basis?			
Does the renewal of access clearance require an updated investigation?			
If anything suspicious arises during the investigative process, is there a defined process to follow?			
Are safeguards in place to avoid violation of civil liberties?			
Do personnel have opportunity for discovery, explanation and challenge of unfavorable information?			
Are appropriate company personnel trained in the National Incident Management System (NIMS)?			
<b>Personnel: Training and Enroute Procedures</b>			
Does the company participate in the Highway Watch Program?			
Have all company personnel received formal training in the threat of terrorism			
Have all company personnel received training in company security objectives, security procedures, employee responsibility, organizational security structure, and security support infrastructure?			
Have company drivers, dispatcher, fleet maintenance personnel and terminal employees received training in observing suspicious behavior and/or events?			
Have company drivers, dispatchers, fleet maintenance personnel, and terminal employees received training in reporting suspicious incidents to the company (internally) and/or to external authorities?			



	Yes	No	Action to be Taken
Have company drivers, dispatchers, fleet maintenance personnel, and terminal employees been trained in how to respond to crisis?			
Have company drivers been trained on how to contact available support resources to help while enroute in the event of a crisis?			
Are drivers provided with effective communication devices while enroute?			
Is instantaneous two-way communication with drivers possible?			
Are vehicles' locations automatically tracked and reported enroute?			
Are drivers (and dispatchers and fleet managers) briefed on possible security threats along their route before departure?			
Are guards ever used to accompany drivers?			
Are drivers, fleet managers, and facility managers trained to vary routines whenever practical?			
<b>Facility/Terminal Security</b>			
Does the company have partnerships with local law enforcement officials, emergency responders, and other public safety agencies with jurisdiction over company facilities (i.e., headquarters and remote facilities)?			
Does the company get intelligence regarding local threats? Does the company have a procedure for reporting suspicious behavior to local law enforcement agencies?			
Does the company have a security plan for each of its facilities?			
Have law enforcement officials reviewed the company's facility security plans?			
Is information on the company's facilities restricted and protected?			
Are security guards used during normal working hours?			
Are security guards used during nights and weekends? (Includes armed, unarmed and canine patrols.)			

	Yes	No	Action to be Taken
Are there external patrols of facility perimeters by law enforcement personnel?			
Do the patrols take place on a regular basis?			
Are these patrols predictable or random?			
Is there fencing around the company's facilities?			
Are fences well maintained?			
Are they protected with supplemental defenses (e.g., razor wire, alarms, locks and other protective equipment)?			
Are surveillance cameras, access control devices, alarm systems, communications equipment, and timed closure devices in use? Are these activities monitored, and by whom?			
Are such devices checked regularly for proper operations, with records kept of their testing?			
Is the lighting adequate for security?			
Is access restricted to a single gate or point-of-entry?			
Are there restrictions on visitor access?			
Are visitors required to register and show a photographic ID?			
Is a visitor log kept?			
Must an employee/security staff escort visitors at all times?			
Do employees wear badges or carry photographic ID when at company facilities?			
Are random, spot security checks conducted on personnel?			
Are random, spot security checks conducted on non-commercial vehicles?			
Are security precautions taken for package/materials pickups and deliveries to company facilities?			
Are all non-company vehicles escorted by employees/security staff?			
Are the mail room security procedures recommended by the U.S. Postal Service in use?			
Do vendors provide advance notification of delivery driver and vehicle number? Are there any vendor screening protocols in place?			

	Yes	No	Action to be Taken
Is there a central delivery point for all packages and deliveries inside the facility?			
Is there a central delivery point at an outside gate?			
Are hazardous materials secured in locked buildings or special fenced areas?			
Are all keys signed out, with records kept of their assignment?			
Are hazardous materials quantitatively inventoried to enable theft recognition?			
Are all valves, manways, and other vulnerable fixtures secured when not in use?			
Are all vehicle power sources disengaged when not in use?			
Are all exterior vehicle doors locked when the vehicle is parked?			
Are all seals and locks tamper-resistant or tamper-evident?			
Are records kept of actual and suspected security incidents?			
Can these records help identify trends and potential vulnerabilities?			
Do facility managers know how to report suspicious incidents?			
Do you know how long it takes from incident detection to authority notification?			
Is this response time tested periodically via drills and practice?			
Do you know the expected response time of law enforcement or other emergency teams?			
Has this response ever been measured in a drill?			
Are affected employees knowledgeable and trained about facility security procedures?			
<b>Passenger &amp; Baggage Screening</b>			
Are passengers screened at the time of ticket purchase?			
Are passengers screened for weapons before boarding?			
Is there a published list of prohibited items for passengers?			

	Yes	No	Action to be Taken
Are passengers separated from their checked baggage for the duration of their trip?			
Do passengers have access to checked baggage at interim points on their trip?			
Is checked baggage matched with actual on-board passengers?			
Is checked baggage screened for explosives before loading?			
Is carry-on baggage checked for weapons?			
Is an oral or written announcement made (or displayed) requesting passengers to report suspicious events/actions that they observe?			
<b>Cyber Security</b>			
Do you have a written Cyber Security Program?			
Are connections to other networks minimized and secure?			
Are there policies and procedures to ensure there are no unattended, unsecured workstations?			
Is there an account management program?			
Is suitable physical protection provided for computer systems?			
Are there backups for electrical power, communication and storage?			
Do you have security and theft prevention countermeasures, systems and procedures in place (e.g. firewalls, encryption, passwords, etc.)?			
Do you have intrusion detection systems?			
Does the company stay abreast of new cyber threats?			
Are company websites, newsletters, etc. controlled and secure for security violations?			
Is access to sensitive information controlled?			
Do employees receive cyber security training?			
Do you have a written cyber security incident reporting and response procedure?			
Are cyber security systems and procedures tested?			
Do you conduct periodic audits of cyber system and security practices?			

	Yes	No	Action to be Taken
<b>General Emergency Response Capabilities</b>			
Does the company have an Emergency Plan?			
Does the company have Emergency Operating Procedures?			
Does the company have an Incident Response Plan for Terrorism, as an appendix to the Emergency Plan or as a separate plan?			
Does the company coordinate with local public safety organizations on the development, implementation and review of the Emergency Plan and procedures?			
Does the Emergency Plan specify use of the Incident Command System?			
Have employees been trained in the Emergency Plan and Procedures?			
Does the company conduct routine drills and refresher training?			
Are there secure protocols for identifying/communicating an event?			
Does the company coordinate its drilling and training for emergency response with local public safety organizations?			
Does the company conduct briefings of after-action reports to assess performance during the drill or exercise and identify areas in need of improvement?			
Have employees of the company participated in Domestic Preparedness Training Programs sponsored by the Federal government (FEMA, FBI, DoD, etc.)?			
<b>Business Continuity</b>			
Has your company developed, tested and implemented a comprehensive Business Continuity Plan (BCP) to be utilized in the continuance of business activities in the event of an emergency?			

	Yes	No	Action to be Taken
Has your company established realistic Recovery Time Objectives (RTOs) as well as Recovery Point Objectives (RPOs) for each of your business functions/processes?			
Have you allocated sufficient resources (human, equipment, financial, management, etc.) to the Contingency Planning effort?			
Does your company have service level agreements (i.e., SLAs) with hot-site recovery facility vendors such as IBM or SunGuard? How current are the agreements? Has a determination been made regarding what is specifically included/excluded in the scope of coverage? Does your company view the SLA as sufficient to address all recovery needs?			
Have you implemented effective communication plans, such that your company can monitor and control the flow of information to all relevant parties (both internal and external) to you company?			
Have you made arrangements for off-site storage: recovery locations and emergency operations located at a safe distance and easily accessible from the site of the incident?			
Do you have processes established to facilitate automatic switching of telephone and data lines?			
Do you have a manual workaround process established to continue operations until information technologies are available?			
Do you have recovery processes established for dealing with loss of information when restoring from backup data?			
Do you have end-to-end process testing done frequently and extensively?			
Do you have plan management and deployment to facilitate maintenance of plans?			
Do you have a BCP awareness program developed and implemented?			

## **Section 2: Risk Assessment**

---

**What Is a Risk Assessment?**  
**Threat Identification and Assessment**  
**Vulnerability Assessment**  
**Consequence Assessment**  
**Calculation of Risk**  
**Prioritizing Needs**  
**Threat Matrix**  
**Vulnerability Matrix**  
**Consequence Matrix**  
**Risk Matrix**

---

See Appendix A for additional information.

## **What Is a Risk Assessment?**

A risk assessment evaluates and compares consequences, vulnerabilities, and threats of potential attacks on critical infrastructure. Development of risk data provides an ability to identify critical assets and their vulnerabilities to threats, to develop and implement countermeasures, and to monitor and improve program effectiveness. This analysis is guided by clear investigation of three critical questions:

- Which assets can we least afford to lose?
- What is our responsibility to protect these assets?
- Where do we assume total liability for risk, and where do we transfer risk to local public responders, technical specialists, insurance companies, and the Federal government?

There are many ways to do a risk assessment, 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. You may also rate the consequence of threats to the system. Combining all three ratings into an overall risk rating can help you identify significant risks and focus your energies and limited resources on those vulnerabilities that lead to these risks. The following sections describe a simple risk assessment strategy that can be applied to your company's Elements of Operation.

## **Threat Identification and Assessment**

The first step in the risk assessment is to develop a set of viable threats to your Elements of Operation. A method used to identify the threats to the company's Elements of Operation is the collection of historical data through incident reports submitted by drivers and supervisors and information provided by local law enforcement and contractors, events which have occurred to other companies, and terrorist acts and activities that could affect company operations.

Information resources include the following:

- Driver incident reports
- Risk management reports
- Facility security inspection reports
- Bus maintenance reports
- Marketing surveys
- Passengers' letters and telephone calls
- Management's written concerns
- Staff meeting notes
- Federal, state and local law enforcement and Homeland Security Advisories
- National Threat Levels determined by the Department of Homeland Security



- Statistical reports
- Special requests
- Type of incidents
  - Crimes against persons
  - Crimes against property
  - General incidents
- Disposition of incidents

The Company Security Committee should review security information resources and determine if additional methods should be used to identify threats and vulnerabilities such as a formal evaluation program to ensure that security procedures are maintained and that security systems are operable.

The threats that are most likely to occur include the following disruptive incidents:

- Drunkenness
- Disorderly conduct
- Disputes
- Minor assaults

Other potential occurrences include:

- Road Rage
- Robberies
- Hijacking
- Improvised Explosive Devices
- Biological or Chemical Weapons

In the Threat Matrix, your company can make an assessment concerning the relative likelihood of occurrence of each of the identified threats against each Element of Operation. This assessment should take into account both the ease with which an attack could be planned and executed and the likelihood that a particular attack would be targeted against the specific Element of Operation.

Threats are evaluated on the relative *likelihood* of a criminal or terrorist act occurring. 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 used as a good substitute.

## **Vulnerability Assessment**

The next step in the risk assessment is to evaluate the vulnerability of the Elements of Operations to each of the identified threats.

Security testing and inspections may be conducted to assess the vulnerability of the company's Element of Operations to each threat. Testing and inspection includes the following three-phase approach:

- Equipment preparedness - to ensure that security equipment is operable and in the location where it belongs
- Employee proficiency - To ensure that employees know how and when to use security equipment
- System effectiveness - To evaluate security by employing security system exercises, including exercises with governmental/law enforcement agencies.

In the Vulnerability Matrix, your company can make an assessment concerning the vulnerability of each Element of Operation to each identified threat. Vulnerability ratings should be based on an evaluation of current security procedures, equipment, and training. Notes should be kept for each asset, identifying specific vulnerabilities or security gaps. These notes will be used in the needs assessment portion of the process to identify risk reduction solutions.

## **Consequence Assessment**

The next step in the risk assessment is to evaluate the consequence of each of the identified threats to the Elements of Operations. The consequence of an event can include a number of impacts to your company, customers, or region, including: casualties, business impact, economic impact, and replacement cost.

In the Consequence Matrix, your company can make an assessment concerning the consequence of each identified threat to each Element of Operations. Each identified threat should be evaluated against the specific Element of Operations. A subjective estimate should be made for the expected level of consequence that would result from a successful attack.

## **Calculation of Risk**

The final step in the risk assessment is to calculate a level of relative Risk for each of the identified threats against each Element of Operations. The level of relative Risk is calculated as the product of the threat rating, the Vulnerability rating, and the consequence rating.

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Consequence}$$

The final calculated relative Risk ratings should be entered into the Risk Matrix. These values represent the overall Risk of each identified threat at each Element of Operations. They will be used to prioritize potential risk reduction solutions.

## **Prioritizing Needs**

Companies have limited security dollars, making it necessary to prioritize the needs to be addressed and the primary security objectives (PSOs). Ultimately, you have to decide which vulnerabilities you need to address, the order in which they should be addressed, and the relative value of various risk mitigation solutions. The risk assessment presented here provides you with a method for prioritizing risks and needs.

The Company Security Committee should review the results of the risk assessment. High-risk threats to Elements of Operations should be identified and prioritized based on the final Risk rating. Reviewing the notes that were developed as part of the vulnerability assessment, specific risk reduction measures should be identified. These measures could include security systems or devices, personnel, response capabilities, training, or exercises. Measures can be prioritized based upon the Risk rating for the threats that they are likely to address, and the relative effectiveness of the measure at reducing those Risks.

An appropriate course of action, acceptable to company management, should be determined and implemented.

## Threat Matrix

Using a scale of 1 to 5, rate each the relative likelihood of occurrence for each identified threat against each element of your operations, with one being the least likely, to five being the most likely. Ratings should take into account both the ease of which an attack could be planned and executed and the likelihood that a particular attack would be targeted against the specific Element of Operation.

\*for example

Elements of Operations (Assets)	Threat														
	Unacceptable Passenger Behavior	Attack on Passenger	Attack on Driver	Robbery	Hijacking	Bomb	Radiological	Biological	Chemical	Fire	Flood	Earthquake	Hurricane	Tornado	
*Maintenance Facility															
*Offices															
*Bus Parking Area															
*Terminal															
*Buses															
*Information Systems															

[Note: the list should be detailed, for example each type of service or each facility. The ‘Threats’ heading should list all potential crimes, terrorist acts, and natural disasters that have occurred or may occur, affecting your operations.]

## Vulnerability Matrix

Using a scale of 1 to 5, rate each element of your operation's vulnerability to all identified threats, with one being the least vulnerable, to five being the most vulnerable (attack is likely to significantly impact the element of operations). Ratings should be based on an evaluation of current security procedures, equipment, and training. Notes should be kept for each asset, identifying specific vulnerabilities or security gaps.

\*for example

Elements of Operations (Assets)	Vulnerability														
	Unacceptable Passenger Behavior	Attack on Passenger	Attack on Driver	Robbery	Hijacking	Bomb	Radiological	Biological	Chemical	Fire	Flood	Earthquake	Hurricane	Tornado	
*Maintenance Facility															
*Offices															
*Bus Parking Area															
*Terminal															
*Buses															
*Information Systems															

[Note: the list should be detailed, for example each type of service or each facility. The 'Threats' heading should list all potential crimes, terrorist acts, and natural disasters that have occurred or may occur, affecting your operations.]

## Consequence Matrix

Using a scale of 1 to 5, rate each the relative consequence of each identified threat against each element of your operations, with one representing the least consequence, to five representing the greatest consequence. Consequence ratings should be based on an evaluation of all potential impacts, including: casualties, business impact, economic impact, and replacement cost.

\*for example

Elements of Operations (Assets)	Consequence														
	Unacceptable Passenger Behavior	Attack on Passenger	Attack on Driver	Robbery	Hijacking	Bomb	Radiological	Biological	Chemical	Fire	Flood	Earthquake	Hurricane	Tornado	
<i>*Maintenance Facility</i>															
<i>*Offices</i>															
<i>*Bus Parking Area</i>															
<i>*Terminal</i>															
<i>*Buses</i>															
<i>*Information Systems</i>															

[Note: the list should be detailed, for example each type of service or each facility. The ‘Threats’ heading should list all potential crimes, terrorist acts, and natural disasters that have occurred or may occur, affecting your operations.]

## Risk Matrix

For each identified Threat and Element of Operation, calculate a level of Risk as the product of the Threat, Vulnerability, and Consequence ratings.

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Consequence}$$

\*for example

Elements of Operations (Assets)	Risk														
	Unacceptable Passenger Behavior	Attack on Passenger	Attack on Driver	Robbery	Hijacking	Bomb	Radiological	Biological	Chemical	Fire	Flood	Earthquake	Hurricane	Tornado	
*Maintenance Facility															
*Offices															
*Bus Parking Area															
*Terminal															
*Buses															
*Information Systems															

[Note: the list should be detailed, for example each type of service or each facility. The ‘Threats’ heading should list all potential crimes, terrorist acts, and natural disasters that have occurred or may occur, affecting your operations.]

# **Section 3: Security and Emergency Preparedness Plan Guidelines**

---

---

<b>Title Page</b>
<b>Division of Responsibilities</b>
<b>Responsibility Matrices</b>
<b>Existing SEPP Capabilities and Practices</b>
<b>Training and Exercising</b>
<b>Coordinating with Public Safety Agencies</b>
<b>Coordination with Other Companies</b>
<b>Evaluation</b>
<b>Modification and Update</b>

---

---

This Guideline is a means from which a motorcoach operator can prepare a Security and Emergency Preparedness Plan that is customized to its operation and size.

See Appendices A, B, C, D & E for additional information.



**Title Page**

# **Security and Emergency Preparedness Plan (SEPP)**

**[Company Name]**

**Date:**

**Revision History:**



## **CONFIDENTIAL AND SECURITY SENSITIVE INFORMATION**

This document is confidential and security-sensitive. Any reproduction or dissemination of any portion of this document is prohibited without the written consent of the Chief Operating Officer of the Company.



This Security and Emergency Preparedness Plan (SEPP) will attempt to ensure that, if confronted with a security event or major emergency, [NAME OF COMPANY] personnel will respond effectively, using good judgment, ensuring due diligence, and building on best practices, identified in drills, training, rules and procedures.

This level of proficiency requires the establishment of formal mechanisms and procedures to be used by all personnel to identify security threats and vulnerabilities associated with operations, and to develop controls to eliminate or minimize them. This Plan also requires processes for:

- Coordinating with law enforcement and other public safety agencies to manage response to an incident that occurs on a vehicle or affects operations, and
- Identifying a process for integrating company resources and capabilities into the community response effort to support management of a major event affecting the community.

Management expects all employees, volunteers and contractors, especially those working directly with passengers, to support this Plan.

## **Division of Responsibilities**

### **All Personnel**

All personnel must understand and adopt their specific roles and responsibilities, as identified in the SEPP, thereby increasing their own personal safety and the safety of our passengers and the motoring public, during normal operations and in emergency conditions.

To ensure the success of the SEPP, the following functions must be performed by personnel:

- Immediately reporting all suspicious activity, no matter how insignificant it may seem, to the Operations Manager or his/her designee;
- Immediately reporting all security incidents
- Using proper judgment when managing disruptive passengers and potentially volatile situations
- Participation in all security and emergency preparedness training, including drills and exercises
- Becoming familiar with, and operating within, all security and emergency preparedness procedures for the assigned work activity

- Notifying the Chief Executive Officer or his/her designee when a physical or mental condition, or required medications or therapies, may impair the employee's ability to perform security or emergency preparedness functions
- Accurately completing "Employee Statements" and appropriate reports as quickly as possible
- Cooperating with/assisting first responders as necessary

## **Chief Executive Officer (CEO)**

The Chief Executive Officer (CEO) has the overall authority to develop and execute the company's SEPP. Ultimate accountability for implementation of the SEPP rests with the Chief Executive Officer. In addition, the CEO is responsible for the following specific activities:

- Ensuring that sufficient resources and attention are devoted to the SEPP, including:
  - Development of standard operating procedures related to employee security duties
  - Development and enforcement of safety and security regulations;
  - Development of emergency operating procedures to maximize company response effectiveness and minimizing service interruptions during emergencies and security incidents;
  - Provision of proper training and equipment to employees to allow an effective response to security incidents and emergencies
- Development of an effective notification and reporting system for security incidents and emergencies
- Designating a Point of Contact (POC) to manage the SEPP
- Establishing a Security Committee
- Communicating security and emergency preparedness as top priorities to all employees
- Developing relations with outside organizations that contribute to the EPP Program, including local public safety and emergency planning agencies

## **SEPP Point of Contact (POC)**

To ensure coordinated development and implementation of the SEPP, the CEO has designated [INSERT TITLE OR NAME] as the Security and Emergency Preparedness Point of Contact (POC) for development and implementation of the SEPP. The POC, who reports directly to the CEO, has been granted the authority to utilize specific company resources to develop the SEPP, to monitor its implementation, and to ensure attainment of security and emergency preparedness goals and objectives.

The [INSERT TITLE OR NAME] has the responsibility for overseeing the SEPP on a daily basis. The [INSERT TITLE OR NAME] will be the direct liaison with the company's drivers and dispatchers, regarding the Program. The [INSERT TITLE OR NAME] will also serve as the

primary contact with public agencies. To the extent that liaison is necessary with local, state and federal agencies, the [INSERT TITLE OR NAME] will serve as the lead liaison for the company. The [INSERT TITLE OR NAME] will also be responsible for the agenda items for Security Committee meetings and actions.

In managing this Program, the POC will:

- Be responsible for successfully administering the SEPP and establishing, monitoring, and reporting on the company's security and emergency preparedness objectives
- Review current company safety, security and emergency policies, procedures, and plans, and identifying needed improvements on a semi-annual basis
- Develop and implement plans for addressing identified improvements
- Coordinate with local public safety agencies, local community emergency planning agencies, and local human services agencies to address security and emergency preparedness; including participation in formal meetings and committees
- Develop, publish, and enforce reasonable procedures pertinent to company activities for security and emergency preparedness
- Provide adequate driver training and continuing instruction for all employees (and volunteers and contractors) regarding security and emergency preparedness
- Review new company purchases to identify security related impacts
- Ensure performance of at least one emergency exercise annually

### **Security Committee (SC)**

Given the nature and scope of [NAME OF COMPANY] operations, it has been determined that a separate Security Committee is [necessary or unnecessary]. [If unnecessary, start here.] As a continuing responsibility of the [Vehicle Accident Prevention or Safety Committee], [If necessary, start here] there will be a permanent agenda oriented toward security and emergency preparedness matters, ranging from comments on the management of the SEPP to liaison with public agencies and feedback from employees. It will also be an ongoing part of the security agenda to determine the level of compliance with company policies, rules, regulations, standards, codes, procedures, and to identify changes or new challenges as a result of incidents or other operating experience.

The SEPP POC will be responsible for managing the security agenda during the Security Committee meetings. When appropriate, members of local fire and police departments, state and federal agencies will be invited to participate in the Committee meetings.

The Security Committee provides the primary mechanism through which the company:

- Identifies security conditions and problems at the company
- Organizes incident investigations and develops and evaluates corrective actions to address findings
- Obtains data on company security performance
- Develops strategies for addressing company security problems
- Coordinates the sharing of security responsibilities and information

- Manages the integration of security initiatives and policies in company operations
- Evaluates the effectiveness of the security program
- Manages the development and revision of company policies, procedures, and rulebook
- Coordinates interaction with external agencies
- Reviews, evaluates and recommends approval of reports from company staff

The Committee also ensures that all company employees, volunteers and contractors:

- Have a full knowledge of the security program and emergency preparedness programs
- Make security and emergency preparedness a primary concern while on the job
- Cooperate fully with the company and local, state and federal agencies regarding any incident investigation
- Raise security and emergency preparedness concerns

## **Supervisors**

Supervisors are responsible for communicating the company's security and emergency preparedness plan and procedures to all employees, volunteers and contractors. For this reason, supervisors must have full knowledge of all security rules and policies. Supervisors must communicate those plans and procedures to operations personnel in a manner that encourages them to incorporate SEPP practices into their everyday work. The specific responsibilities of supervisors include the following.

- Having full knowledge of all standard and emergency operating procedures, and are strongly encouraged to be trained in the National Incident Command System (NIMS).
- Ensuring that drivers make security and emergency preparedness a primary concern when on the job.
- Cooperating fully with the SEPP regarding any accident investigations as well as listening and acting upon any security concerns raised by the drivers.
- Immediately reporting security concerns to the SEPP POC.

In addition, when supporting response to an incident, supervisors are expected to:

- Provide leadership and direction to employees during security incidents;
- Handle minor non-threatening rule violations;
- Defuse minor arguments;
- Determine when to call for assistance;
- Make decisions regarding the continuance of operations;
- Respond to service complaints;
- Respond to security related calls with law enforcement officers when required, rendering assistance with crowd control, victim/witness information gathering, and general on-scene assistance;
- Complete necessary security related reports;
- Take photographs of damage and injuries;
- Cooperate and coordinate with all outside agencies at incident scenes

## **Drivers**

In addition to the general responsibilities identified for ALL PERSONNEL, drivers (including volunteers and contractors) are responsible for exercising maximum care and good judgment in identifying and reporting suspicious activities, in managing security incidents, and in responding to emergencies. Each driver will:

- Conduct vehicle security inspections
- Take charge of a security incident scene until the arrival of supervisory or emergency personnel
- Collect fares in accordance with company policy (if applicable)
- Attempt to handle minor non-threatening rule violations
- Respond verbally to complaints
- Attempt to defuse minor arguments
- Determine when to call for assistance
- Maintain control of the vehicle
- Report all security incidents to dispatch
- Complete all necessary security related reports
- Support community emergency response activities as directed by company policies, plans and procedures

## **Other Personnel**

Other personnel also have responsibilities for the SEPP.

Dispatchers are expected to:

- Receive calls for assistance
- Dispatch supervisors and emergency response personnel
- Coordinate with law enforcement and emergency medical service communications centers
- Notify supervisory and management staff of serious incidents
- Establish on-scene communication
- Complete any required security related reports
- Provide direction to on-scene personnel

Mechanics (including volunteers and contractors) are expected to:

- Conduct vehicle security inspections
- Report suspicious behavior, packages, or situations
- Report vandalism
- Report threats and vulnerabilities of vehicle storage facilities
- Provide priority response to safety and security critical items such as lighting
- Maintain facility alarm systems

Human Resources personnel are expected to:

- Ensure all pre-employment screening processes are carried out effectively
- Notify the Chief Executive Officer of employee disciplinary action that may result in the affected employee becoming a risk to company facilities, systems, passengers, employees or other assets
- Educate employees on employee ID policy and procedure
- Ensure confidentiality of employment records and personal employee data

Communications (Marketing-Customer Service-Community Relations) are expected to:

- Request assistance from public safety resources as needed for special events
- Provide insight into potential threats and vulnerabilities through feedback from customer focus groups and other information sources
- Designate a Public Relations Coordinator (PRC) for media contact regarding security incidents and issues

### Other Critical Roles and **Responsibilities**

- *Location Response Coordinator (if company has more than one location)* - This person will be responsible for carrying out all required activities at his/her operating location. This person may direct others at their location to assist in accomplishing necessary actions, but must be kept fully informed of progress and activities for immediate reporting to the Security Crisis Response Coordinator. The Location Response Coordinator will directly report to the Security Crisis Response Coordinator during the use of this plan. (Suggested personnel: General Manager or Terminal Manager)
- *Public Relations Coordinator* - This person will be responsible for interacting with the media. This person should be in the same location as the Security Crisis Response Coordinator and should be kept fully informed of all activities and issues. No other person will interact with the press, or engage in any public relations related to the security threat or incident.
- *Passenger Assistance Coordinator* - A person at each operating location will be designated to coordinate and assist all affected passengers to ensure their comfort and safety throughout a security related crisis. This person will also be responsible to answer calls of family members regarding the status and whereabouts of affected passengers. Other staff members may be assigned to assist in responding to family calls as needed. (Suggested Personnel: Dispatchers and Safety Directors)
- *Driver Support and Direction Coordinator* - This person will be responsible for attending to drivers' needs during the crisis and preparing them for resumption of normal activities. This person will also be responsible for answering calls from family members regarding the status and whereabouts of the driver. (Suggested Personnel: Dispatchers and Safety Directors)



## Security & Emergency Preparedness Practices & Actions

[Summarize methods and procedures, devices, and systems utilized by the company to minimize and respond to security incidents and emergencies\*]

\*for example

\*A summary of the existing proactive methods, procedures, and actions to prevent, deter, or minimize security incidents include:

- Emphasis on company personnel awareness
- Participation in local law enforcement and emergency response training and drills
- Review of local law enforcement and emergency response materials
- Analysis of security incidents and suspicious activities to refine and improve courses of action including:
  - Identifying potential and existing problem areas
  - Developing and refining action plans
  - Implementing the plans
  - Measuring results
- Hosting an annual meeting with local law enforcement
- Annual meeting with local emergency management agency
- Review of company emergency plans
- Review of TSA documentation on system security and emergency preparedness
- Coordinate with DHS/TSA
- Posting of contact data for law enforcement and DHS/TSA
- Conducting security surveys with local law enforcement as a formal threat and vulnerability analysis process
- Local police notification/participation in employee discharge and/or discipline process as needed
- Evaluation of security/emergency response procedures for completeness and accuracy
- Participation by local law enforcement in training of new drivers as requested to increase awareness in security matters
- Presentations by local police and company personnel to employees, the public or other groups interested in security matters
- Development and distribution of crime prevention information on company brochure for passengers and the public
- Conducting criminal background investigations of employment applicants
- Conducting inspections of facilities
- Conducting security awareness training for employees, contractors and volunteers
- Conducting security inspections
- Identifying and purchasing necessary security technologies
- Conducting crisis training for employees
- Defining system shutdown protocols
- Conducting mock system shutdown
- Coordinating with public emergency response organizations

- Conducting Business Continuity Exercise

## **Training and Exercising**

[Company should formulate SEPP training and exercising program taking into account the considerations identified below]

1. This section should describe basic and refresher security and emergency-related training programs for personnel with associated responsibilities.
2. Description of all security-related training including refresher for non-security staff provided, including content, duration.
3. Description of the process used to identify security-related training needs, to develop and present training classes, and to determine qualifications for instructors.
4. This section should explain how the company determines what training to offer and ensures that all individuals are trained appropriately.

A sample Training & Exercising Description is as follows:

- All personnel will receive emergency response and evacuation training for facility-related events upon hire.
- All applicable personnel will receive Operation Secure Transport training within 90 days of hire.
- All employees will receive refresher Operation Secure Transport refresher training on a biannual basis.
- All applicable personnel will receive Highway Watch Training as soon as possible after hire.
- A mock system shutdown or a mock local security incident will be scheduled to monitor company and employee preparedness and to determine areas for improvement. A review of all security incidents will be conducted on an annual basis to identify improvements to training and exercising. Any improvements identified will be incorporated into future employee training and exercising.

## **Coordination with Public Safety Agencies**

[Identify (by name and contact number) the local, state and federal law enforcement, fire services, emergency medical services, and emergency planning agencies within the company's service area]

To support improved emergency and incident preparedness and response the company will participate in, at a minimum, one exercise or drill with local public safety organizations in order to:

- Review current plans and policies
- Identify current security and emergency considerations
- Develop procedures (if necessary)
- Establish and maintain ongoing communication
- Update communications plan, ensure interoperability with local law enforcement in service areas

## **Coordination with Other Companies**

[Identify (by name and contact number) companies within your county or neighboring counties that may need to be contacted in the event of a critical incident]

## **Evaluation**

### **Internal**

The SEPP is a “living document” and needs to address issues associated with system security and emergency preparedness on a timely and proactive basis. It is incumbent upon all appropriate personnel to constantly evaluate the effectiveness of the SEPP as well as implementation. The POC will work with the SC to ensure that the SEPP is evaluated for effectiveness [ENTER TIME FRAME (e.g. every 6 months)].

### **External**

The SEPP POC will also serve as the company liaison with external agencies involved in the auditing of existing procedures associated with the SEPP.

## **Modification and Update**

If during the internal or external evaluations, or based upon SC findings and activities, the company will revise its SEPP and supporting documentation and training to reflect new practices, policies, and procedures. The SC is responsible for screening changes and modifications to facilitate ongoing revisions to keep the SEPP current.

## **Section 4: Emergency Response Procedures Guidelines**

**Sample Emergency Contact Directory  
Emergency Response Procedures  
Operational Procedures to be Followed Throughout a  
Security Threat or Incident**

This guideline is a means from which a motorcoach operator can prepare Emergency Response Procedures that are customized to operation and size.

Based upon your operation and size, the following topics should be considered for response procedures:

- Emergency Contact Directory
- Facility Emergencies
  - Emergency Evacuation/Shelter Procedures and Routes
  - Emergency Shutdown Procedures
  - Employee Accountability Procedures Following an Emergency Evacuation
  - Emergency Response, Rescue and Medical Duties
  - Assistance to Emergency Responders
- In Vehicle Emergency Procedures
  - Vehicle Breakdowns
  - Vehicle Accidents
  - Sick or Injured Passenger
  - Fire or Smoke on Bus
  - Aggressive/Confrontational Passenger Behavior
  - Bomb Threat
  - Terrorist Attack
  - Suspicious Package
- Operational Procedures to be Followed Throughout a Security Threat or Incident

## **Sample Emergency Contact Directory**

**COMPANY:**

**ADDRESS:**

### **COMPANY CONTACTS:**

SEPP POC (Emergency Response Coordinator):  
General Manager:  
Safety Director:

### **LOCAL GOVERNMENT AGENCIES**

Emergency Services (OES):  
Sheriff/Coroner:  
Police:  
Coroner:  
Health Dept.:  
Animal Control:  
Mental Health Services:  
Crisis Line:

### **LOCAL MEDICAL CENTERS:**

Hospital Emergency:  
\_\_\_\_\_ Clinic:  
\_\_\_\_\_ Clinic:  
\_\_\_\_\_ Clinic:  
Mental Health Services:  
Crisis Line:

## Emergency Response Procedures

### 1. FACILITY EMERGENCIES

#### Types of Emergency:

- Fire
- Explosion
- Tornado/Weather
- Bomb Threat
- Chemical Spill/Leak
- Violence
- Medical
- Other

#### Emergency Evacuation/Shelter Procedures and Routes

- Emergency evacuation/shelter procedures have been developed. Each employee receives these procedures when hired, reassigned, etc. Persons accountable for this task are:

NAME	TITLE	WORK AREA

- Evacuation/shelter master maps have been posted in each identified work area and are kept current. Persons accountable for this task are:

NAME	TITLE	WORK AREA

- Evacuation/shelter assistance during emergencies will be provided by designated employees in each work area. These employees will have received training in assisting employees during evacuation movements to shelter locations.

NAME	WORK AREA	TRAINING RECEIVED	DATE OF TRAINING	NAME OF TRAINER

- Training is/was provided for employees when:
  - a. The plan was initiated or has changed
  - b. Responsibilities change
  - c. Employees are hired or transferred

Persons accountable for this task are:

NAME	TITLE	WORK AREA	DATE OF TRAINING	NAME OF TRAINER

### Emergency Shutdown Procedures

During some emergency situations, it will be necessary for some specifically assigned and properly trained employees to remain in work areas that are being evacuated long enough to perform critical operations. These assignments are necessary to ensure proper emergency control. The following personnel have been assigned these duties.

NAME	WORK AREA	JOB TITLE	DESCRIPTION OF ASSIGNMENT

These individuals have received special instructions and training by their immediate supervisors to ensure their safety in carrying out the designated assignments. A training record describing the instructions provided and the detailed procedures to be followed is maintained in the Emergency Response Coordinator's Office.

### Record of Emergency Shutdown Procedures/Critical Operations Training

NAME	ASSIGNMENT	DATE OF TRAINING	NAME OF TRAINER



## **Employee Accountability Procedures Following An Emergency Evacuation**

Each supervisor is responsible for accounting for each assigned employee following an emergency evacuation. This will be accomplished by performing the procedures established for such an eventuality.

### **Employee Accountability**

1. Reassembly locations have been established for all evacuation/shelter routes and procedures. These locations are designated on each posted work area evacuation/shelter route map.
2. All work area supervisors and employees must report to their designated reassembly locations immediately after an evacuation or move to a sheltered location.
3. Each employee is responsible for reporting to his or her supervisor so that an accurate head count can be made. Supervisors will check off the names of all those reporting and will report those not checked off as missing to the Emergency Response Coordinator.
4. The Emergency Response Coordinator will be located at one of the following locations:
  - A. Primary Location: \_\_\_\_\_
  - B. Secondary Location: \_\_\_\_\_
5. The Emergency Response Coordinator will determine the method to be utilized to locate missing personnel.

### **Emergency Response, Rescue and Medical Duties**

It may become necessary in an emergency to respond to the source of the emergency (e.g. fire) to rescue personnel and perform some specified medical duties, including first-aid treatment. All employees assigned to perform such duties will have been properly trained and equipped to carry out their assigned responsibilities properly and safely.

The following employees have accepted specific assignments and received specific training:

NAME	LOCATION	SPECIFIC ASSIGNMENT	SPECIFIC TRAINING PROVIDED	DATE OF TRAINING	NAME OF TRAINER

## Assistance to Emergency Responders

It may be necessary to assist emergency responders in entering and searching facilities. All employees assigned to perform such duties will have been properly trained and equipped to carry out their assigned duties properly and safely.

NAME	ASSIGNMENT	TRAINING PROVIDED	DATE OF TRAINING	NAME OF TRAINER

## Special Instructions and Procedures

All personnel performing emergency rescue and medical duties must follow these instructions:

---

---

---

---

---

---

---

## 2. In Vehicle Emergency Procedures

These procedures have been established to respond to emergencies involving vehicles. The following general principles apply to all such emergencies:

- Take charge
- Save lives
- Save property
- Call for help
- Gather information

Drivers will be responsible for initiating these procedures. Dispatch, Safety and other applicable personnel are responsible for assisting and coordinating necessary actions to address the emergency.

- **Vehicle Breakdowns**

### **DRIVER**

- Stop bus in safe location
- Explain to customer
- Set out emergency triangles and put

### **DISPATCHER**

- Upon notification from driver – who, what, where, when and driver/customer cell phone if

- on flashers
- Contact dispatcher – who, what, where, when and driver/customer cell phone if available
- If you suspect fire or danger evacuate the bus
- If on highway keep customers on the bus

- **Vehicle Accidents**

**DRIVER**

- Contact 911 – who, what, where, when and driver/customer cell phone if available
- Check for injuries
- Set out emergency triangles and put on flashers
- Contact dispatcher – who, what, where, when and driver/customer cell phone
  - Pass out passenger cards
  - Courtesy Cards to witnesses
  - Seating chart
  - Accident report
- Stay until released by dispatcher
- DO NOT ADMIT RESPONSIBILITY. Only make statements to police, company supervisors, or other company personnel
- Do not move the bus until instructed to do so by a police officer or company supervisory personnel
- The Accident Report must be completed immediately after the accident

- **Sick or Injured Passenger**

**DRIVER**

- Stop bus in safe location
- Look for Medic-Alert bracelet or necklace
- Contact 911 and dispatcher – who,

available

- Contact local police to inform of bus location
- Contact Safety Director
- Contact General Manager

**DISPATCHER**

- Contact 911 – who, what, where, when and driver/customer cell phone if available
- Contact General Manager
- Contact Safety Director

**DISPATCHER**

- Upon notification from driver – who, what, where, when and driver/customer cell phone if available

what, where, when and driver/customer cell phone if available

- Ask for passengers with medical help, “Doctor, nurse, EMT on board?”
- Render whatever assistance they are capable of
- Caution should be taken to avoid coming in contact with blood or other bodily fluids
- Await for instructions from dispatcher

- Contact 911 – who, what, where, when and driver/customer cell phone if available
- Contact Safety Director
- Contact General Manager
- Direct all media calls to SEPP POC, General Manager or Safety Director
- Select another bus driver and bus to meet that driver
- Contact SEPP POC if appropriate

- **Fire or Smoke on Bus**

**DRIVER**

- Stop bus immediately, turn engine off, and open doors
- *Getting customers off bus is first priority*
- Control the fire using the fire extinguisher, *remember arm’s width.*
- After evacuating Contact 911 and dispatcher – who, what, where, when and driver/customer cell phone if available
- Await for instructions from dispatcher
- Fill out accident reporting kit
  - Pass out passenger cards
  - Courtesy Cards to witnesses
  - Seating chart
  - Accident report
- Stay until released by passenger
- DO NOT ADMIT RESPONSIBILITY. Only make statements to police, company supervisors, or other company personnel.
- Do not move the bus until instructed to do so by a police officer or company supervisory personnel
- Accident Report must be completed immediately

**DISPATCHER**

- Contact driver get update
- Select another bus driver and bus to meet the driver
- Coordinate tow truck/mechanic
- Direct all media calls to SEPP POC, General Manager or Safety Director
- Get accident forms from driver upon return from accident

- **Aggressive/Confrontational Passenger Behavior**

### **DRIVER**

Hold Ups, Hijacking, Shootings, Homicides,  
Hostage Situations, Assaults and Severe  
Passenger Disturbances on the Bus

- Do not resist or try to overwhelm attacker(s)
- If possible, try to pull the bus over in a safe location
- If possible, signal the dispatcher using a duress code
- If possible, signal to police
- If possible, contact 911 and dispatcher – who, what, where, when and driver/customer cell phone if available
- Remember details of the person(s) and get away vehicle if any – *Think of CYMBALS*

#### **Persons**

- C = Color (hair, skin, eyes)
- Y = Year of birth (age)
- M = Make (Italian, Asian, Hispanic)
- B = Body (Height & Weight)
- A = Attire (color & type)
- L = Looks (tattoo, beard, hair type)
- S = Sex (male or female)

#### **Get Away Car**

- C = Color
- Y = Year
- M = Make/Model
- B = Body Style
- A = All Others (damage, signs or attachments)
- L = License Plate Number
- S = State
- Wait for instructions from dispatcher

### **DISPATCHER**

- If you hear a duress code, respond to driver, try to get – who, what, where, when and driver/customer cell phone if available
- If no answer try to contact driver every 15 minutes with “bus \_\_\_\_\_ you failed to check in, what is your location?”
- Contact 911 – who, what, where, when and driver/customer cell phone if available
- Contact Safety Director
- Contact General Manager
- Contact SEPP POC
- Select another bus driver and bus to meet that driver if applicable
- Direct all media calls to General Manager or Safety Director

- **Bomb Threat**

**DRIVER**

- DO NOT PANIC . . . most bomb threats are false
- Stop the bus at a safe location
- Put on emergency flashers
- Stand up, face the customers and announce “Please do not panic, we are having a problem with the bus, take all your packages, please exit the bus and stand by the tree (any location at least 300 feet away)”
- Do not answer any questions, firmly ask customers to leave the bus
- Check bus for left behind passengers
- DO NOT TOUCH ANY EXPLOSIVE DEVICES OR SUSPICIOUS PACKAGES
- DO NOT USE THE BUS RADIO OR A CELLULAR TELEPHONE NEAR A SUSPICIOUS PACKAGE
- After evacuating tell passengers about the bomb threat
- After evacuating Contact 911 and dispatcher – who, what, where, when and driver/customer cell phone if available
- Await instructions from dispatcher

**DISPATCHER**

- DO NOT PANIC . . . most bomb threats are false
- Contact Safety Director
- Contact General Manager
- Contact SEPP POC
- If unable to reach General Manager or Safety Director within 5 minutes:
  - If directed to a particular bus notify driver
  - Get a bus and driver out to pick up the passengers from the threatened bus immediately
- If unable to reach General Manager or Safety Director within 5 minutes:
  - Call all buses “this is a general threat warning only extra vigilance requested, there has been a general bomb threat against [NAME OF COMPANY] or [GEOGRAPHIC DESCRIPTION]
- Direct all media calls to SEPP POC

- **Terrorist Attack**

**DRIVER**

- Contact 911 and dispatcher – who, what, where, when and driver/customer cell phone if available
- Stay away from impact area
- Dispatch/police will inform you of best evacuation route
- If in smoke shut all windows and vents
- If chemical attack explain to passengers;

**DISPATCHER**

- Contact 911 – who, what, where, when and driver/customer cell phone if available
- Contact SEPP POC
- Contact Safety Director
- Contact General Manager
- Start coordinating alternate plans
- Direct all media calls to SEPP POC

- Not to leave
- They need to be decontaminated by authorities
- May take a long time – be patient
- If they go home they may get sick and infect others

- **Suspicious Package**

**DRIVER**

- Stop Bus in a safe location
- **DO NOT TOUCH THE PACKAGE**
- Make a general announcement to try to determine ownership
- Check with other employees to see if they can identify the owner
- Contact 911 and dispatcher; coordinate response– who, what, where, when and driver/customer cell phone if available

**DISPATCHER**

- Upon notification from driver – who, what, where, when and driver/customer cell phone if available
- Talk with driver get details on package:
  - **TELL DRIVER NOT TO TOUCH THE PACKAGE**
  - Why is it suspicious?
  - Is the package sealed or closed?
  - Does the package have ownership information, if so contact owner
  - Is the package in an area not normally visited by the public/customer?
  - Make a general announcement to try to determine ownership
  - Ask customers in the area if they misplaced the package
  - Check with other employees to see if they can identify the owner
  - Does the package exhibit any suspicious indicators, such as protruding wires, oily stains or odors?
  - Are there any unusual noises coming from the package, such as an electric hum or ticking noises?
  - Is the package leaking fluid

or powder?

- Consider package suspicious if a package is sealed with no marking and left in a place not normally used by the employees or public; or
  - There are unusual noises, smells, wires, leaking fluid or powder; or
  - You have some other reason to believe it is suspicious
- Contact Safety Director
- Contact General Manager or Location Manager (if applicable)
- Contact SEPP POC
- Direct all media calls to SEPP POC or designated person
- Select another bus driver and bus to meet the driver



## **Recommended Operational Procedures to Be Followed Throughout a Security Threat or Incident**

- A call is received from a person making a threat or from an individual informing us of an incident. Information regarding this call must be transferred immediately to the General Manager at the location where the call was received. The General Manager will immediately inform the SEPP POC.
- All phone numbers known to the public must have real voice 24 hour answering capabilities.
- All people who will answer phones must be trained in security awareness to detect suspicious situations.
- If a threat or an actual event is communicated by the driver and involves a person or situation on the coach, immediate notification of the appropriate law enforcement and other appropriate first response agencies may be made, while informing the SEPP POC.
- The SEPP POC will detail actions to be taken as a whole or at each particular location to the Location Response Coordinators. The Location Response Coordinators will, in turn, carry out these activities through communications with appropriate management personnel, drivers, and others, as necessary.
- Cell phones will be the primary means of communication from each location to all drivers. It is therefore important that each vehicle be equipped with a cell phone which can be carried by the driver at all times when away from the vehicle and away from the home base. Alternately, drivers may be issued company cell phones which must be required to be carried at all times when they are away from the home base with a motorcoach.
- A complete listing of all cell phone numbers issued to drivers or assigned to units as well as a complete listing of all home phone numbers for drivers and other employees must be developed and kept up to date at each location. A copy of a current listing must also be forwarded to the SEPP POC.
- If cell phones cannot be used during a

crisis, alternate methods of regular contact or emergency contact must be developed. These can include a listing of numbers where drivers are housed during off duty periods (e.g. hotels or other locations based upon scheduled service, charter or tour itineraries). Drivers should be provided with specific instructions that, if cell phones do not work, they attempt to contact dispatch during any known crisis and then re-contact dispatch as directed.

- The location of all motorcoaches must be accounted for. When drivers are contacted, specific locations should be reported. Any units which are not driven should be accounted for at one of the facilities.
- A daily inventory of coaches must be made. To accomplish this, the bus inventory form will be completed at each location for all units assigned to it. Any unit not accounted for must be reported immediately to the General Manager and then to the SEPP POC.
- Satellite global positioning technology is suggested for all buses. This technology should be investigated, costs estimated, and efforts to obtain funding for implementation should be made.
- The Location Response Coordinator will provide appropriate instructions to drivers.
- Each location should contact and work with local emergency responding agencies to determine the most appropriate response to bomb threats or biohazard threats, and should seek information then to determine their desired response by the Company if a threat is made upon one or all of our buses. If an actual incident occurs, we must know where we should evacuate our passengers.
- A directory of all emergency phone numbers including TSA, FBI, DHS, state and local agencies should be developed and kept up to date at each

location. This list should be forwarded to the SEPP POC.

- The accommodation and safety of passengers must be achieved by the Passenger Assistance Coordinator.
- Any passengers experiencing a medical emergency must be attended to directly and locally through contact of medical authorities by the driver.
- Reasonable accommodations (hotels, transportation to and from designated areas, etc.) must be detailed and deployed by the Passenger Assistance Coordinator.
- The Passenger Assistance Coordinator must provide information concerning the status and whereabouts of affected passengers to inquiring family member.
- Use of e-mail notifications and the website should be maximized for this purpose.
- The Driver Support and Direction Coordinator should provide coordination and assistance to drivers throughout the crisis.
- Appropriate information regarding the status and whereabouts of the drivers should be provided to their families when requested.
- The SEPP POC will direct the resumption of normal operations after the crisis has passed and/or clearance has been provided by law enforcement or first responder agencies.
- If no national emergency has been declared, hours of service must be considered for the resumption of normal service.
- Notification of resumption of normal service to passengers should be achieved through the website and e-mail notification as much as possible.

# Appendices

<b>Appendix A:</b>	<b>Addressing Varying Threat Levels</b>
<b>Appendix B:</b>	<b>Security Plan Considerations</b>
<b>Appendix C:</b>	<b>Security Issues to be Integrated into Risk Management of Fleet Operations</b>
<b>Appendix D:</b>	<b>Considerations for Conducting Emergency Crisis Response Exercises</b>
<b>Appendix E:</b>	<b>Reference Documents and Helpful Industry Websites</b>

## Appendix A: 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 trip destinations or the location of your facility, even if the national threat level is not raised. For example, there was an 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 following table.

Threat Conditions		Measures
<b>LOW</b> 	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.
<b>GUARDED</b> 	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.
<b>ELEVATED</b> 	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.
<b>HIGH</b> 	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.
<b>SEVERE</b> 	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.

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 individuals with no visible badge or credentials;
- 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 at irregular intervals to spot individuals not displaying their badges;
- Check vehicle inventory and account for all vehicles on a daily basis; and
- Occasionally test employee response to individuals without visible badges or credentials.

*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 for 24-hour (around the clock) coverage.

*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.

## **Appendix B: Security Plan Considerations**

### **Corporate vs. Facility 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 or operation location, each facility would need to have a site-specific security assessment, considering its unique characteristics. Each facility 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 facility level. Plans should be reviewed on a regular basis.

Some companies may group their facilities according to the nature of their operations and the types and levels of service that they accommodate. 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 service levels 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 vehicles take when leaving your terminals, and the destinations of the routes or trips. 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.

### **Security Plan Components**

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.

This section offers more examples on how to structure the primary objectives and select specific security measures that meet them. 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.



## 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;
- Check if applicant is listed on the FBI Watch List;
- 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.

#### *Additional Sample Security Measures to Implement at Condition Orange*

- Former employees must return all company-issued credentials at the time of their separation from the Company;
- 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. 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.

## **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;
- Have security/law enforcement periodically check located infiltration/egress routes for criminal or terrorist use around the site; and
- Have security/law enforcement periodically check the buffer zones around any facility.

## 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;
- Test cyber-security protocols and back up plans on a semi-annual basis; and
- Locking hardware for gates should be casehardened 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
- Backup 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 and video surveillance system (if applicable) into local law-enforcement department;
- Have a video camera monitor areas not under direct observation;
- Employ explosive/GBR 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 and procedures for emergency closure;
- When a trip 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
- Periodically test cyber-security protocol.

## En-route Security

A vehicle in transit represents not just a moving target, but also 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; and
- Install theft-protection devices to disable fuel, hydraulics, and/or electrical systems;

- Driver should always have a communication device readily available to him;
- Purchase all other necessary technology devices to be installed; and
- Routinely use primary means of communications.

*Additional Sample Security Measures to Implement at Condition Blue*

- Train with new equipment and test plan for primary, secondary, and tertiary means of communications;
- Periodically use secondary means of communication.

*Additional Sample Security Measures to Implement at Condition Yellow*

- Periodically use tertiary means of communication.

## Appendix C: Security Issues from the SEPP to be Integrated into Policies and Procedures Governing Fleet Operations

<b>FLEET OPERATIONS COMPONENT</b>	<b>POLICIES AND PROCEDURES</b>	<b>ADDITIONAL ISSUES IN SEPP</b>
<b>TITLE</b>		
<b>MANAGEMENT COMMITMENT</b>	<ul style="list-style-type: none"> <li>➤ Safety Policy Statement</li> </ul>	<ul style="list-style-type: none"> <li>➤ SECURITY AND EMERGENCY PREPAREDNESS</li> </ul>
<b>COMPLIANCE RESPONSIBILITIES</b>	<ul style="list-style-type: none"> <li>➤ Operations/Safety Manager</li> <li>➤ Drivers, mechanics and others operating company vehicles (and volunteers)</li> <li>➤ Accident Prevention Committee</li> <li>➤ Safety incentive program(s)</li> </ul>	<ul style="list-style-type: none"> <li>➤ EXPANDED TO ADDRESS SEPP</li> <li>➤ CREATION OF SEPP POINT OF CONTACT (POC)</li> <li>➤ SECURITY COMMITTEE</li> <li>➤ SEPP AGENDA FOR QUARTERLY SECURITY COMMITTEE MEETINGS</li> </ul>
<b>DRIVERS – INITIAL HIRE</b>	<ul style="list-style-type: none"> <li>➤ Application</li> <li>➤ Interviews</li> <li>➤ Driver Performance History</li> <li>➤ Physical Requirements/Examinations</li> <li>➤ Drug Testing</li> <li>➤ Age</li> <li>➤ Knowledge of English</li> <li>➤ Driver Licensing</li> <li>➤ Operating Skills</li> <li>➤ Ability to perform simple math</li> <li>➤ Reasonable knowledge of the service area and ability to read basic maps</li> <li>➤ A road test given by a designated Company Supervisor is required</li> </ul>	<ul style="list-style-type: none"> <li>➤ CRIMINAL RECORDS CHECK</li> <li>➤ EXPANSION OF NEW HIRE BACKGROUND CHECK</li> <li>➤ EXPANSION OF NEW HIRE APPLICATION PROCESS TO EMPHASIZE IMPORTANCE OF SAFETY AND SECURITY</li> </ul>



<b>FLEET OPERATIONS COMPONENT</b>	<b>POLICIES AND PROCEDURES</b>	<b>ADDITIONAL ISSUES IN SEPP</b>
<b>TITLE</b>		
<b>INITIAL TRAINING</b>	<ul style="list-style-type: none"> <li>➤ Company Policies and Procedures</li> <li>➤ Federal and State Regulations</li> <li>➤ Pre and Post Trip Inspections</li> <li>➤ Vehicle Familiarization</li> <li>➤ Basic Operations and Maneuvering</li> <li>➤ Special Driving Conditions</li> <li>➤ Backing</li> <li>➤ Bad Weather</li> <li>➤ Boarding and Alighting Passengers</li> <li>➤ Defensive Driving</li> <li>➤ Passenger Communication and Assistance Training</li> <li>➤ Off Road</li> <li>➤ On Road</li> </ul>	<ul style="list-style-type: none"> <li>➤ ADDITIONAL TRAINING TO ADDRESS SECURITY AWARENESS, REPORTING SUSPICIOUS ACTIVITY, REPORTS AND DOCUMENTATION, PRE AND POST TRIP INSPECTIONS, AND RESPONDING TO SECURITY-RELATED CRISES</li> </ul>
<b>DRIVERS- ONGOING SUPERVISION AND TRAINING</b>	<ul style="list-style-type: none"> <li>➤ Training - refresher/remedial</li> <li>➤ Evaluation and supervision</li> <li>➤ Motor vehicle record checks</li> <li>➤ Physical examination</li> <li>➤ Drug/Alcohol testing</li> <li>➤ Safety meetings</li> <li>➤ Seat-belt usage</li> <li>➤ Discipline/recognition</li> <li>➤ Preventable accidents/injuries</li> </ul>	<ul style="list-style-type: none"> <li>➤ ADDITIONAL REFERSHER TRAINING AND “PROFICIENCY TESTS” FOR KNOWLEDGE OF EMERGENCY PROCEDURES</li> <li>➤ ADDITIONAL RESPONSIBILITIES FOR SUPERVISION</li> </ul>
<b>EMERGENCY PROCEDURES</b>	<ul style="list-style-type: none"> <li>➤ Emergency driving procedures</li> <li>➤ Accident causes <ul style="list-style-type: none"> <li>○ Slippery road surfaces</li> <li>○ Driving at night</li> <li>○ Driving in mountainous areas</li> <li>○ Winter driving</li> <li>○ Driving in very hot weather</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>➤ EXPANSION OF EMERGENCY PROCEDURES TO INCLUDE ADDITIONAL SECURITY AND EMERGENCY CONDITIONS</li> <li>➤ EXPANSION OF EMERGENCY PROCEDURES TO INCLUDE SUPPORT OF COMMUNITY RESPONSE TO A</li> </ul>

<b>FLEET OPERATIONS COMPONENT</b>	<b>POLICIES AND PROCEDURES</b>	<b>ADDITIONAL ISSUES IN SEPP</b>
<b>TITLE</b>		
	<ul style="list-style-type: none"> <li>➤ Vehicle breakdowns and unavoidable stops</li> <li>➤ Vehicle fire/evacuation</li> <li>➤ Hold up/robbery</li> <li>➤ Hijacking</li> <li>➤ Natural disasters <ul style="list-style-type: none"> <li>○ Tornado</li> <li>○ Flood procedures - vehicle</li> </ul> </li> </ul>	<p>MAJOR EVENT OR EMERGENCY</p> <ul style="list-style-type: none"> <li>➤ EXPANSION OF PROCEDURES FOR MANAGING DIFFICULT AND THREATENING PASSENGERS, INCLUDING ASSAULT AND HIJACK</li> <li>➤ EMERGENCY TRAINING AND EXERCISING</li> </ul>
<b>PASSENGER SAFETY</b>	<ul style="list-style-type: none"> <li>➤ General guidelines</li> <li>➤ Seatbelts (if applicable)</li> <li>➤ Child safety seats</li> <li>➤ Mobility device securement and passenger restraint systems</li> <li>➤ Difficult passengers</li> <li>➤ Medical condition/medical assistance</li> <li>➤ Basic First Aid</li> <li>➤ Bloodborne pathogens/infection control</li> </ul>	<ul style="list-style-type: none"> <li>➤ EXPANSION OF PROCEDURES FOR RESPONSE TO BOMB THREATS AND CHEMICAL, RADIOLOGICAL AND BIOLOGICAL EVENTS</li> </ul>
<b>VEHICLES &amp; EQUIPMENT</b>	<ul style="list-style-type: none"> <li>➤ Vehicles &amp; equipment <ul style="list-style-type: none"> <li>○ A Level Inspection</li> <li>○ B Level Inspection</li> <li>○ C Level Inspection</li> </ul> </li> <li>➤ Pre &amp; post trip inspections</li> <li>➤ Emergency equipment on vehicles and usage</li> <li>➤ Use of emergency equipment on vehicle</li> <li>➤ Vehicle security</li> <li>➤ Vehicle safety in and around the shop or yard</li> </ul>	<ul style="list-style-type: none"> <li>➤ EXPANSION OF VEHICLE SECURITY PROCEDURES</li> <li>➤ EXPANSION OF MAINTENANCE PROCEDURES FOR IDENTIFYING AND REPORTING VANDALISM, SUSPICIOUS SUBSTANCES, OR VEHICLE TAMPERING</li> <li>➤ EXPANSION OF VEHICLE PROCUREMENT PROCEDURES TO ADDRESS AND INCLUDE SECURITY TECHNOLOGY</li> </ul>

<b>FLEET OPERATIONS COMPONENT</b>	<b>POLICIES AND PROCEDURES</b>	<b>ADDITIONAL ISSUES IN SEPP</b>
<b>TITLE</b>		
<b>ACCIDENT MANAGEMENT</b>	<ul style="list-style-type: none"> <li>➤ Accident documentation packet</li> <li>➤ Accident notification procedures – driver responsibility</li> <li>➤ Accident investigation – management responsibility</li> <li>➤ Accident investigation kit</li> <li>➤ Reconstruction &amp; analysis</li> <li>➤ Drug and alcohol tests</li> <li>➤ Media relations and crises communication after an accident</li> </ul>	<ul style="list-style-type: none"> <li>➤ ADDITIONAL TOOLS FOR ACCIDENT DOCUMENT PACKET TO ADDRESS SECURITY</li> <li>➤ ADDITIONAL TOOLS FOR MEDIA RELATIONS</li> </ul>
<b>INSURANCE CLAIMS AND LITIGATION MANAGEMENT</b>	<ul style="list-style-type: none"> <li>➤ Dealing with adjusters</li> <li>➤ Dealing with attorneys – ours/theirs</li> </ul>	<ul style="list-style-type: none"> <li>➤ ADDITIONAL CONSIDERATIONS FOR COVERAGE</li> </ul>
<b>DAY TO DAY OPERATIONS – MONITORING FOR SAFETY</b>	<ul style="list-style-type: none"> <li>➤ Record keeping</li> <li>➤ Keeping informed <ul style="list-style-type: none"> <li>○ Websites</li> <li>○ Publications</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>➤ ADDITIONAL REPORTS FOR SECURITY-RELATED INCIDENTS</li> </ul>

## **Appendix D: Considerations for Conducting Emergency/Crisis Response Exercises**

Experience shows that exercises are the most practical, efficient, and cost effective way to measure preparedness for disasters and crises. The aim for any company should be to develop a progressive exercise program, a long-term approach in which exercises are planned, conducted, and evaluated as building blocks to competency in crisis management.

There are two principal benefits of such a program. First, people practice their role and gain proficiency in crisis management. Second, the coordination among service providers and local emergency response agencies is improved. These benefits arise not from exercising alone, but from evaluating the exercise and acting upon those results. An exercise has value only when it leads to individual and/or collective improvement.

Key terms used in the development of exercises include the following:

- **Progressive Exercise Program:** A commitment from the company and community public safety agencies to plan and conduct increasingly more challenging exercises over a period of time, to achieve and maintain competency in executing the local crisis management plan.
- **Objective:** A goal expressed in simple, clear, specific, and measurable terms. Serves as the foundation of all exercise planning.
- **Scenario:** The overall outline of how an exercise will be conducted. Includes the narrative, major/detailed sequence of events, problems or messages, and expected actions. Often used interchangeably with the term narrative.
- **Narrative:** A word “picture” that includes all essential elements of information concerning the incident used to initiate an exercise.

Types of exercises include the following:

- **Drill:** Supervised activities that test, develop, or maintain skills in a single response procedure (such as: communications, notification, lockdown, shutdown, fire) and the possible or probable interaction with local government agency functions (such as: incident command posts, rescue squad entry, police perimeter control) will involve actual field response. These activities help prepare for more complex exercises in which several functions are coordinated and tested.
- **Activity Exercise:** Designed to promote emergency preparedness; test or evaluate emergency operations, policies, plans, procedures or facilities; train personnel in emergency duties; and demonstrate operational capabilities.

- Full-Scale Exercise: Evaluates the operational capability of emergency response management systems in an interactive manner. Includes the mobilization of emergency personnel and resources required to demonstrate coordination and response capability. Tests total response capability as close to a real emergency as possible.
- Functional Exercise: A fully simulated interactive exercise; tests one or more functions in a time-pressured realistic simulation; focuses on policies, procedures, roles, and responsibilities.
- Orientation Seminar: An informal discussion designed to familiarize participants with roles, plans, procedures, and resolve questions of coordination and assignment of responsibilities.
- Tabletop Exercise: Simulates an emergency situation in an informal, stress-free environment. Designed to elicit discussion as participants examine and resolve problems based on existing crisis management plans.

The National Incident Management System (NIMS) protocols should be incorporated into exercises conducted by the company as much as practical.

## **Appendix E: Reference Documents and Helpful Industry Web Sites**

### **Reference Documents**

The following are resources used to develop the policies and procedures documented in this template:

Title: **Operation Secure Transport: Security Awareness Training for Motorcoach Operators**

Authors: Daecher Consulting Group, Inc. and SPS Enterprises, Inc.

Year: 2004

Sponsoring Agencies: United Motorcoach Association and the American Bus Associations through grants provided by the Transportation Security Administration

Available: [www.OnlineSafetyTraining.com](http://www.OnlineSafetyTraining.com)

Title: **High Threat Security**

Author: Jeff Beatty

Year: 2002

Sponsoring Agency: American Bus Association

Available: [www.buses.org](http://www.buses.org)

Title: **Critical Incident Management Guidelines**

Authors: Annabelle Boyd and James Caton

Year: 1998

Sponsoring Agency: Federal Transit Administration (FTA)

Volpe Report #: DOT-VNTSC-FTA-98-05

DOT Number: FTA-MA-26-7009-98-1

Available: [www.transit-safety.dot.gov](http://www.transit-safety.dot.gov)

Title: **Protecting Surface Transportation Systems and Patrons from Terrorist Activities – Volume One**

Author: Brian Michael Jenkins

Year: January 1997

Sponsoring Agency: San Jose University, Mineta International Institute for Surface Transportation Policy Studies

Report Number: IISTPS 97-4

Full text available at: [www.transweb.sjsu.edu/publications/terrorism/Protect.htm](http://www.transweb.sjsu.edu/publications/terrorism/Protect.htm)

Title: **Protecting Surface Transportation Systems Against Terrorism and Serious Crime – 2001 Update**

Author: Brian Michael Jenkins

Year: October 2001

Sponsoring Agency: San Jose University, Mineta International Institute for Surface Transportation Policy Studies

Report Number: IISTPS 01-7

Full text available at: [www.transweb.sjsu.edu/publications/terrorism/Protect.htm](http://www.transweb.sjsu.edu/publications/terrorism/Protect.htm)

**Title: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Title X, Section 1012**

Year: October 25, 2001

Enacted by Congress

Full text available at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162>:

**Title: Terrorism in the United States 1999, 30 Years of Terrorism A Special Retrospective Edition**

Year: 1999

Sponsoring Agency: U.S. Department of Justice, Federal Bureau of Investigation

Full text available at: [www.fbi.gov/publications/terror/terror99.pdf](http://www.fbi.gov/publications/terror/terror99.pdf)

**Title: Life After Terrorism, What You Need to Know to Survive in Today's World**

Author: Bruce D. Clayton

Year: 2002

Available for Purchase at: [www.paladin-press.com](http://www.paladin-press.com)

## Helpful Industry Websites

American Bus Association: [www.buses.org](http://www.buses.org)

Center for Defense and International Security Studies: [www.cdiss.org/hometemp.htm](http://www.cdiss.org/hometemp.htm)

Center for Security Policy: [www.security-policy.com](http://www.security-policy.com)

Chemical and Biological Defense Information Analysis Center: [www.cbiac.apgea.army.mil](http://www.cbiac.apgea.army.mil)

Commercial Vehicle Safety Alliance: [www.cvsa.org](http://www.cvsa.org)

Critical Infrastructure Assurance Office: [www.ciao.gov](http://www.ciao.gov)

Daecher Consulting Group, Inc.: [www.safetyteam.com](http://www.safetyteam.com)

Defense Threat Reduction Agency: [www.dtra.mil/index.htm](http://www.dtra.mil/index.htm)

Department of Homeland Security: [www.dhs.gov](http://www.dhs.gov)

Emergency Net News: [www.emergency.com](http://www.emergency.com)

Federal Computer Incident Response Capability: [www.fedcirc.gov](http://www.fedcirc.gov)

Federal Motor Carrier Safety Administration: [www.fmcsa.dot.gov](http://www.fmcsa.dot.gov)

Institute for the Advanced Study of Information Warfare: [www.psycom.net/iwar.l.html](http://www.psycom.net/iwar.l.html)

International Policy Institute for Counterterrorism: [www.ict.org.il](http://www.ict.org.il)

National Infrastructure Protection Center: [www.nipc.gov](http://www.nipc.gov)

National Security Agency: [www.nsa.org](http://www.nsa.org)

National Terrorism Preparedness Institute: [terrorism.spjc.cc.fl.us](http://terrorism.spjc.cc.fl.us)

Overseas Security Advisory Council: [www.ds-osac.org](http://www.ds-osac.org)

Rapid Response Information System: [www.rris.fema.gov](http://www.rris.fema.gov)

Terrorism Research Center: [www.terrorism.com](http://www.terrorism.com)

Training Alternatives Group, LC: [www.taglp.com](http://www.taglp.com)

Transportation Security Administration: [www.tsa.gov](http://www.tsa.gov)



United Motorcoach Association: [www.uma.org](http://www.uma.org)

US Department of Transportation, Office of Hazardous Materials Safety: [hazmat.dot.gov](http://hazmat.dot.gov)

US Secret Service National Threat Assessment Center: [treas.gov/uss/ntac.htm](http://treas.gov/uss/ntac.htm)

US State Department, Office of the Coordinator for Counterterrorism: [www.state.gov/s/ct](http://www.state.gov/s/ct)