U.S. Department
of Transportation

Federal Transit Administration

The Public Transportation System Security and Emergency Preparedness Planning Guide

U.S. Department of Transportation
Research and Special Programs Administration
John A. Volpe National Transportation Systems Center
Cambridge, Massachusetts 02142-1093

January 2003
Final Report

FEDERAL TRANSIT ADMINISTRATION

REPORT DOCUMENTATION PAGE

Form Approved
OMB No.

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE January 2003	3. REPORT TYPE AND DATES COVERED
4. TITLE AND SUBTITLE The Public Transportation System Security and Emergency Preparedness Planning Guide		5. FUNDING NUMBERS U3066/TM363
6. AUTHOR(S) John N. Balog, Annabelle Boyd, James E. Caton		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U. S. Department of Transportation Research and Special Programs Administration Volpe National Transportation Systems Center 55 Broadway, Kendall Square Cambridge, MA 02142-1093		8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-FTA-03-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Transportation Federal Transit Administration Office of Program Management, Office of Safety and Security Washington, DC 20590		10. SPONSORING/MONITORING AGENCY REPORT NUMBER DOT-FTA-MA-26-5019-03-01
11. SUPPLEMENTARY NOTES		
12a. DISTRIBUTION/AVAILABILITY STATEMENT		12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Recent events have focused renewed attention on the vulnerability of the nation's critical infrastructure to major events, including terrorism. The Public Transportation System Security and Emergency Preparedness Planning Guide has been prepared to support the activities of public transportation systems to plan for and respond to major security threats and emergencies. It emphasizes the importance of developing critical relationships, preparing strategies and policies, and setting training and funding priorities. It offers practical guidance for planning effectively, spending wisely, and making the public transportation infrastructure safer. This Guide builds on two previous Federal Transit Administration (FTA) publications. These are the Transit System Security Program Planning Guide and the Transit Security Handbook. These earlier publications are available on the Guide CD-ROM. This Guide is based on research to identify practical steps that systems can take to be better prepared for all emergencies. These recommendations support the industry's commitment to prevent those events that can be prevented and to minimize the impact of those that cannot. Emphasizing balanced, common sense measures, this Guide helps transportation systems answer many questions.

14. SUBJECT TERMS Public Transportation, Transit, System, Security, Emergency Preparedness, Terrorism, Plan, Prevention, Incident Command, Safety, Law Enforcement, Policy, Management, Threat, Vulnerability, Crime, Bus, Rail, Paratransit, Employee, Procedures, Passenger, Police			15. NUMBER OF PAGES 164 16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT

Acknowledgements

The Public Transportation System Security and Emergency Preparedness Planning Guide reflects the results of research conducted by the McCormick, Taylor & Associates, Inc. Research Team. The Guide was sponsored by a grant from the Transit Cooperative Research Program (TCRP) Rapid Response Research Project in cooperation with the Federal Transit Administration (FTA) and the American Public Transportation Association (APTA). TCRP is administered by the Transportation Research Board (TRB) of the National Research Council (NRC). Upon acceptance by the TCRP Committee for Project J-10A, the Guide was delivered to FTA for approval and was subject to FTA's revision and publication process through the Volpe National Transportation Systems Center.

John Balog, of McCormick, Taylor & Associates, Inc. and Annabelle Boyd and Jim Caton, of Boyd, Caton & Grant Transportation Group, Inc. were responsible for the research, development, and preparation of this guide and its accompanying CD-ROM. Valuable assistance in the editing and preparation of this guide was provided by Peter N. Bromley and Jamie Beth Strongin, of McCormick, Taylor & Associates, Inc. and Anne Singleton, of Boyd, Caton & Grant Transportation Group, Inc.

For their guidance and technical direction, the authors give special thanks to Mr. Robert Jamison, Ms. Susan Knisely, Mr. Harry Saporta, Mr. Jerry Fisher, Mr. Len Diamond, and Mr. David Martin of FTA. This study was managed by Stephan J. Parker, Senior Program Officer, who worked with the consultants, FTA and APTA representatives, and the J-10A project committee in the development and review of the guide. Special thanks are given to the members of the TCRP Committee for Project J-10A:

CHAIR
Ms. Maureen A. Milan
New Jersey Transit Corporation

MEMBERS
Mr. Gerald L. Blair
Indiana County (PA) Transit Authority
Mr. Cecil Bond
Southeastern Pennsylvania Transit Authority
Mr. John David Claflin
Regional Transportation District - Denver
Ms. Dorothy W. Dugger
San Francisco Bay Area Rapid Transit District
Ms. Polly L. Hanson
Metro Transit Police -WMATA
Mr. Randy Isaacs
Isaacs & Associates / Greyhound State Gov't Affairs
Mr. Thomas C. Lambert
Metropolitan Transit Authority - Houston
Mr. Paul J. Lennon
Los Angeles County Metropolitan Transportation Authority
Mr. William T. McArdle
Port Authority of Allegheny County (PA)
Dr. Fran Nielsen
National Institute for Standards and Technology
Mr. James D. O'Donnell
Metropolitan Transportation Authority
Mr. Robert L. Smith
Chicago Transit Authority
Mr. Eugene Wilson, Jr.
Metropolitan Atlanta Rapid Transit Authority

FTA LIAISONS
Ms. Rhonda M. Crawley
Mr. Brian Cronin
Mr. Jerry Fisher
Mr. Robert D. Jamison
Mr. Jeffrey G. Mora

OTHER LIAISONS
Mr. Robert Adduci
Volpe National Transportation Systems Center
Mr. Scott Bogren
Community Transportation Association
Ms. Karen Wolf-Branigan

APTA LIAISONS
Mr. Greg Hull
Ms. Vivienne Williams

TRB LIAISONS
Ms. Joedy W. Cambridge
Marine Transportation Specialist
Dr. Peter Shaw
Public Transportation Specialist

TCRP STAFF
Mr. Stephan A. Parker
Senior Program Officer, TCRP

INTERSTED OBSERVER
Mr. Frederick C. Goodine
Washington Metropolitan Area Transit Authority

Table of Contents

Foreword xi
1 Executive Overview 1
1.1 Building Vision 1
1.2 Managing Uncertainty 2
1.2.1 Location Makes a Difference 2
1.2.2 Vigilance is the Best Defense 4
1.2.3 Security Should Be Responsive to Available Resources 4
1.2.4 Other Recommendations 5
1.3 Investment in Security and Emergency Preparedness 7
2 Security and Preparedness in a Diverse Industry 13
2.1 Diversity in Public Transportation 13
2.2 Existing Threat Management Process 14
2.3 Implications for Terrorism 14
2.4 Meeting the Threat 16
2.5 System Security and Emergency Preparedness (SSEP) 17
2.6 Benefits of SEPP 18
2.7 Steps in the Program 20
3 Developing the Security and Emergency Preparedness Program (SEPP) 23
3.1 Authority 23
3.2 Goals and Objectives 26
3.3 Organization 27
3.3.1 Management Level 28
3.3.1.1 Top Management 28
3.3.1.2 Division and Department Heads 28
3.3.2 Managers 29
3.3.2.1 Supervisors 29
3.3.2.2 Employees 29
3.3.2.3 Proactive Security Committee 30
3.3.2.4 Security Breach Review Committee 30
3.3.2.5 Function within Program 31
3.4 Resources 33
3.4.1 Personnel 34
3.4.2 Budget 34
3.4.3 Management Support 34
3.5 Deliverables 34
3.6 Schedule 35

3.7 Assign Tasks and Perform Work 36
3.8 Preparing the SEPP 36
3.9 Comprehensiveness of the Plan 37
3.9.1 Purpose 37
3.9.2 Scope 37
3.9.3 Responsibilities 37
3.9.4 Implementation 38
3.10 Clarity of the Plan 38
3.11 From Plan to Procedure 38
3.12 Growth of the Plan 39
3.13 Integrating the SEPP into Local Planning 39
3.13.1 Local Government 39
3.13.2 State Government Emergency Planning Program 42
3.13.3 Nuclear Regulatory Commission (NRC) Requirements 44
3.13.4 Emergency Planning and Community Right-to-Know Act (EPCRA) 44
3.13.5 Inter-organizational Emergency Memoranda of Understanding 46
4 Capabilities Assessment 47
4.1 Establish the Team 47
4.2 Program Review 48
4.2.1 Existing Plans 48
4.2.2 Security Master Planning 49
4.2.3 Standard Operating Procedure (SOP) Review and Development 49
4.2.4 Emergency Preparedness and Disaster Planning 50
4.2.5 Facility or on-Site Security Review 55
4.3 Documenting Results 56
4.3.1 Note on Use 56
5 Reducing Threat and Vulnerability 64
5.1 Asset Analysis 64
5.2 Threats, Vulnerabilities, and Consequences 67
5.2.1 Threats 67
5.2.2 Vulnerabilities 67
5.2.3 Scenario Analysis 69
5.2.4 Consequences 71
5.2.5 Prioritized Listing of Vulnerabilities 72
5.2.6 Developing Countermeasures 72
5.2.7 Rings of Protection 73
6 Procedures for New Threats 77

6.1 Sample Bomb Threat Procedures 77
6.1.1 Threats by Phone 77
6.1.2 Threats by Mail 78
6.1.3 Manager's Responsibility 78
6.1.4 Executing the Response 78
6.1.5 Search Plans 79
6.1.5.1 No Bomb Found 80
6.1.5.2 Unusual or Out-of-place Object Found 80
6.1.5.3 After-Action Plan 81
6.2 Managing Hoaxes and Unusual or Out-of-place Objects 81
6.3 Response to Calls of Reports Suspecting A Chemical Agent Release 86
6.3.1 Responding to an Actual Chemical or Biological Agent Release 88
6.3.2 Support Community Response 90
6.4 Release of Sensitive Information to the Public 91
7 Training and Exercising 94
7.1 Principles of Training for Preparedness 94
7.2 Existing Training Programs 94
7.3 Exercising for Preparedness 97
7.4 Building a Progressive Exercise Program 100
7.5 Designing Exercises 101
7.6 Exercise Evaluation 103
8 Design and Technology Review 107
8.1 Security By Design 107
8.2 Crime Prevention Through Environmental Design and Situational Crime Prevention 108
8.3 Security Technology 112
8.4 Considerations from the Department of Justice 113
8.5 Assessing Technology Options 118
8.5.1 Available Technologies 118
8.5.1.1 Considerations for Technology Evaluation 121
Appendix A: Glossary of Terms 124
Appendix B: Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment 133
Appendix C: Security Contacts at the Top 35 Largest Public Transportation Systems 142
Appendix D: Detailed Capabilities Assessment Worksheet 150
Appendix E: Fact Sheet-Grant Processing Guidelines 161
Appendix F: A Memorandum of Understanding Between [Local Public Safety Agency] and the [Local Transit Agency] 162

List of Figures

Figure 1: Requirements for Security and Emergency Preparedness 9
Figure 2: Elements of Protection 12
Figure 3: Common Threats and Evaluation Matrix 15
Figure 4: System Security Approach to Prevention and Response 19
Figure 5: Steps in the System Security Methodology 20
Figure 6: Coordination With Local Systems 21
Figure 7: Activities to Develop the SEPP 24
Figure 8: Resources for SEPP 34
Figure 9: Sample Assignment Matrix 36
Figure 10: Agencies Involved in Planning 41
Figure 11: Possible Transportation Responsibilities 43
Figure 12: Capabilities Assessment Program Review 48
Figure 13: Transportation System Resources 54
Figure 14: Characteristics of Transportation Sites 56
Figure 15: Threat and Vulnerability Process 65
Figure 16: Scenario Evaluation Criteria 71
Figure 17: Sample Rings of Protection 74
Figure 18: Active Security Strategies for Bus Vehicles 76
Figure 19: Response to Chemical and Biological Threats 83
Figure 20: Planning, Training, and Exercising Inter-Relationships 99
Figure 21: Sample Decontamination Scene Staging Area Schematic 156
Figure 22: Sample Operational Shifts 160

List of Tables

Table 1: Program of Commitments 1
Table 2: Industry Security Snapshot, Fiscal Year 2000 10
Table 3: Law Enforcement or Security Personnel, Fiscal Year 2000 10
Table 4: US Public Transportation Inventory 13
Table 5: Program Roles and Responsibilities Matrix 31
Table 6: Summary Findings – Capabilities Assessment 57
Table 7: Transportation Assets 66
Table 8: Threats from Terrorism 68
Table 9: Relevant Bus Scenarios 70
Table 10: Relevant Rail Scenarios 70
Table 11: Public Transportation Countermeasures 75
Table 12: Categories of Potentially Sensitive Information 92
Table 13: Preparedness Review of Training Programs 98
Table 14: Exercise Development Checklist 102
Table 15: Checklist for Evaluating the Transportation Emergency Exercise Program 103
Table 16: Security by Design 111

Acronyms

ARC	American Red Cross
ATTF	Anti-Terrorism Task Force
CFR	Code of Federal Regulations
CBRN	Chemical, Biological, Radiological and Nuclear
CDC	Centers for Disease Control and Prevention
CPTED	Crime Prevention through Environmental Design
CWA	Clean Water Act
DOE	U.S. Department of Energy
EMA	Emergency Management Agency
EOC	Emergency Operations Center
EOP	Emergency Operating Procedures
EPA	U.S. Environmental Protection Agency
ESFs	Emergency Support Functions
FBI	U.S. Federal Bureau of Investigation
FEMA	U.S. Federal Emergency Management Agency
FHWA	U.S. Federal Highway Administration
FRA	U.S. Federal Railroad Administration
FRERP	Federal Radiological Emergency Response Plan
FRP	Federal Response Plan
FTA	U.S. Federal Transit Administration
FTE	Full Time Equivalent
FY	Fiscal Year
GIS	Geographical Information System
HAZMAT	Hazardous Materials
IAP	Incident Action Plan
IC	Incident Commander
ICS	Incident Command System
LEPC	Local Emergency Planning Committee
MMRS	Metropolitan Medical Response Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NRC	Nuclear Regulatory Commission
OSC	On-Scene Coordinator
OSHA	U.S. Occupational Safety and Health Administration
SAR	Search and Rescue
SARA	Superfund Amendments and Reauthorization Act
SCP	Situation Crime Prevention
SEOC	State Emergency Operations Center
SEPP	Security and Emergency Preparedness Plan
SERC	State Emergency Response Commission
SOP	Standard Operating Procedures
SSPP	System Safety Program Plan
UC	Unified Command
USC	United States Code
WMD	Weapons of Mass Destruction

Preface

The events of September 11th emphasized the responsibilities placed on industry to keep the nation's communities safe and moving. Transit systems are inherently "open" environments. They are designed to move people quickly through an urban area, and, therefore, must provide unimpeded, easy access to passengers. In addition, they are intended to make low-cost transportation alternatives available to everyone, and, therefore, must have cost structures that support affordable transportation.

Over the past year, gains in protection and preparedness have required tremendous management initiative, interagency coordination, and financial investment. At many agencies, major projects and on-going programs for maintenance and operational up-grades have been delayed or re-directed to provide the resources and personnel necessary to address security and preparedness requirements.

The industry's willingness to experiment with different alternatives; to share information; and to support Federal, State and local partners in homeland security has promoted rapid advancement in security and preparedness programs. Agencies have learned what works, and, just as importantly, what does not work, in their operating environments. Managers and executives have had to make difficult decisions regarding the trade-offs inherent in cost, mobility and security, using increasingly sophisticated risk assessment processes.

Defending against terrorism is not new to industry. Since the early 1990s, the nation's 100 largest rail and bus properties, which combined move approximately 85 percent of all passengers who use public transportation, have been working to address the credible threat from terrorism. Well before the al-Qaeda attacks in this country, two decades of bombings and assaults in Europe, the Middle East, India and Latin America demonstrated the inherent susceptibility of the public transportation infrastructure to a broad range of terrorist methods and weapons. These experiences informed the plans, training and exercising which sustained industry preparedness throughout the 1990s.

For more than a decade, FTA has supported industry programs for security and preparedness through training, research, guidelines and even regulation. 49 CFR Part 659, which went into effect on January 1, 1998, requires all rail transit agencies to document their security and preparedness programs in System Security Program Plans, reviewed and approved by State Oversight Agencies. On-going FTA auditing of this requirement ensures that agency plans and procedures are up-to-date and address a range of contingencies.

Working with the U.S. Department of Transportation, Office of Intelligence and Security, FTA has also coordinated closely with national domestic preparedness programs, developed after the 1995 Sarin release on a Tokyo subway killed 12 and sent thousands of others to local hospitals. The *Defense Against Weapons of Mass Destruction Act of 1996* (more commonly known as the Nunn-Lugar-Domenici bill) initiated an ambitious program to provide training and equipment for first responders to deal with terrorist incidents, including those involving weapons of mass destruction (WMD), in 120 of the highest risk cities in the country. The presence of public transportation infrastructure was a defining characteristic in this initial assessment of risk, which has been expanded and amended to include a mixture of 157 cities and counties.

Public transportation police and operations personnel have been active partners in these programs, and also have participated in the Land Transportation Antiterrorism Training Program developed cooperatively between U.S. DOT and the Federal Law Enforcement Training Center (FLETC). Combined, over the last 5 years, these programs provided the opportunity for transportation agencies to develop preliminary plans and programs for addressing terrorism and WMD. Community drilling and exercise programs have always been a significant component of public transportation emergency preparedness, and were continually emphasized prior to September 11.

Since the attacks in New York and Washington, FTA has continued to work closely with the public transportation industry. In response to new threats of terrorist activity, FTA launched a multipart transit security initiative. This program includes the following elements:

⇒ **Security assessments**: FTA deployed teams, comprised of experts in anti- and counter-terrorism, transit operations, and security and emergency planning, to assess security at 36 transit agencies. FTA chose the 36 agencies on the basis of their ridership, vulnerability, and the potential consequences of an attack. Each assessment includes a threat and vulnerability analysis, an evaluation of security and emergency plans, and a focused review of the agency's unified command structure with external emergency responders. FTA plans to extend the assessments to additional agencies after the first 36 assessments are complete.

⇒ **Emergency response planning**: FTA is providing technical assistance to the 60 largest transit agencies on security and emergency plans, and emergency response drills.

⇒ **Emergency response drills**: FTA offered transit agencies grants (up to $50,000) for organizing and conducting emergency preparedness drills. FTA has awarded $3.4 million to over 80 transit agencies through these grants.

⇒ **Security training – Connecting Communities Forums**: FTA is offering free emergency preparedness and security training to transit agencies and their local responders through its *Connecting Communities Forums*. These forums are being offered throughout the country and are designed to bring together small and medium-sized transit agency personnel with their local public safety agencies, including law enforcement, fire and emergency medical services, and specialized units for hazardous materials and explosives ordinance disposal. These forums provide participants with the opportunity to:

- ⇒ network and coordinate with your local transit, police, fire, and emergency officials to share the latest techniques, strategies and best practices;
- ⇒ understand the role of a transit agency in responding to emergency/disaster situations in your community;
- ⇒ discuss how to activate alternative transportation methods within your community during a crisis;
- ⇒ identify the elements, people, organizations, procedures, equipment and facilities needed for an effective emergency management program, as

well as understand how the interaction of these elements affects the management of emergency situations;

- ⇒ discuss existing transit system emergency management, disaster recovery and security plans;
- ⇒ explore the interagency role in handling emergency response; and
- ⇒ understand the roles and responsibilities of community officials, transit system personnel, emergency response personnel (police, fire, EMS, OEM and hospital) and media during an emergency.
- ⇒ Attendees will also receive a wealth of resources and visual guides to educate their agency's employees on the lessons learned from the forums.

⇒ **Security training – National Transit Institute:** In addition, through NTI, FTA created two courses for specifically for the transit industry, to support suspicious activity/awareness training and to promote safe and effectiveness management of security reports and incidents. These courses, developed in cooperation with transit agencies, labor unions, and security professionals not only help a transit system "harden the target" relative to terrorism, but also will improve its overall security – helping to reduce all levels of crime. These courses are available through a variety of delivery mechanisms including direct deliveries and train-the-trainers.

⇒ The *System Security Awareness for Transit Employees* course is targeted directly at front-line employees and supervisors who have direct contact with the public or the vehicles and facilities used by the public. The course covers skill sets for observing, determining and reporting people and things that are suspicious or out-of-place. It encourages employees to use common sense when faced with various circumstances so operations can run safely, smoothly, and efficiently. A focus is also placed upon an employee's initial priorities at the scene of a threat or incident. The time needed to deliver the course content will range from two to four hours depending on the job functions of the class participants and the level of detail an agency wishes to cover.

⇒ *Security Incident Management for Transit Supervisors* is a two-hour add-on course for road supervisors, dispatchers, foremen, and other front-line managers. The course addresses a transit front-line manager's fundamental responsibilities: communication, information gathering and analysis, hazard and risk identification, decision making, and plan implementation. Several scenario-based exercises allow students to solve problems and apply the skills presented in the programs.

⇒ **Research and development**: FTA increased the funding of its safety- and security-related technology research and has accelerated the deployment of the PROTECT system, a partnership with the Department of Energy to test and deploy chemical sensors in public transportation stations, tunnels and vehicles. The program is pursuing a systems approach to the problem of release detection and management, including modeling and simulation to identify the most effective application of sensor-based technology, communications systems, automated decision support systems, decontamination procedures and technology, training tools, and exercise and response planning. FTA has also initiated a unique research partnership with

the Transportation Research Board (TRB) and the American Public Transportation Association (APTA) to support targeted, rapid response research to a range of policy issues identified by transit executive leadership.

⇒ **Memorandum of Understanding with TSA**: FTA has been working closely with TSA and the Office of Homeland Security (OHS), which may ultimately incorporate TSA as part of a new Department of Homeland Security. In this capacity, FTA is developing a Memoranda of Understanding to outline roles and responsibilities in the Federal strategy to protect the nation's critical transportation infrastructure.

⇒ **Transit System Protective Measures to Support Responses to the Homeland Security Advisory System (HSAS)**: FTA is supporting the development of transit system protective measures to promote a consistent and effective transit industry response to threat conditions defined by the Department of Homeland Security (DHS). The FTA response model supplements the HSAS model with Black and Purple designations for further refine transit industry activities when an event is in progress and during the post-event recovery of transit services and facilities. The guidance document outlines protective measures in relation to the direction provided by DHS.

Foreword

Attention to security and emergency preparedness is a natural corollary to the public transportation industry's existing safety culture. Security and emergency preparedness programs protect both the community and the system. They keep the system operational and effective, even under adverse conditions.

The Public Transportation System Security and Emergency Preparedness Planning Guide builds on two previous Federal Transit Administration (FTA) publications. These are the Transit System Security Program Planning Guide[1] and the Transit Security Handbook[2]. These earlier publications are available on the Guide CD-ROM.

This Guide is based on research to identify practical steps that systems can take to be better prepared for all emergencies. These recommendations support the industry's commitment to prevent those events that can be prevented and to minimize the impact of those that cannot. Emphasizing balanced, common sense measures, this Guide helps transportation systems answer many questions.

- ⇒ Who at my system should be responsible for security and emergency preparedness?
- ⇒ What is my system's current level of security and preparedness?
- ⇒ What additional threats should we consider for our operations?
- ⇒ What steps can we take to identify and prioritize action for mitigating and managing these threats?
- ⇒ How can we cooperate more effectively with law enforcement and other emergency responders?

Organization of Guide

This Guide is organized into eight sections and six appendices.

- ⇒ **Executive Overview** presents an overview of the Guide, highlighting key activities to be performed by public transportation systems to enhance prevention and to improve response capabilities. This section will be most useful to mid- and senior level managers who must evaluate the system's current level of preparedness and implement programs to address the impacts of changing threat conditions.

- ⇒ **Preparedness in a Diverse Industry** identifies the challenges of security and preparedness in the public transportation industry. It emphasizes the necessity of tailoring practices to address the diversity of operations and services provided by the more than 7,500 local systems receiving some form of federal assistance.

---

[1] Balog, John N., Anne N. Schwarz, and Bernard C. Doyle, *Transit System Security Program Planning Guide*, US Department of Transportation, Federal Transit Administration, November 1997.

[2] Boyd, M. Annabelle and M. Patricia Maier, *Transit Security Handbook*, US Department of Transportation, Federal Transit Administration, May 1998.

⇒ **Developing the Security and Emergency Preparedness Program (SEPP)** provides guidance on how transportation systems can develop internal security, incident management systems, and external plans for coordinating with local law enforcement, other local responders, local planning agencies, and state or federal agencies. While this section emphasizes planning for terrorism, basic principles and concepts are applicable to all emergency situations. This section also includes recommendations for applying the SEPP Planning Template on the Guide CD-ROM to create documentation for the system's program.

⇒ **Capabilities Assessment** supports the efforts of transportation systems to evaluate their current level of security and emergency preparedness. It provides a summary checklist for documenting findings, as well as recommendations for consideration by the team conducting the assessment.

⇒ **Reducing Threats and Vulnerabilities** describes the methodology used to conduct a threat and vulnerability assessment. It emphasizes techniques to support recommendations appropriate to the unique requirements of each system's operation.

⇒ **Procedures for New Threats** provides sample procedures and recommendations for managing threats in the new environment. It includes managing bomb threats; managing hoaxes and unusual or out-of-place packages and substances; responding to a possible chemical agent release; and managing the dissemination of information to the public.

⇒ **Training and Exercising** highlights those elements of existing public transportation training and supervisory programs that can be revised or updated to reflect new requirements resulting from heightened threat conditions. This section also describes those activities that can be performed to integrate the transportation system into community-based exercises, and to develop and conduct tabletops, drills, and full-scale exercises.

⇒ **Design and Technology Review** explains available design strategies and technologies to support improved public transportation security and to enhance both normal and emergency operations. This section concludes with a list of considerations appropriate to all transportation systems investigating technology procurements.

⇒ **Appendix A: Glossary of Terms** provides an explanation of terms used in this document.

⇒ **Appendix B: Federal Bureau of Investigation (FBI) Vulnerability Self-Assessment** provides the worksheets used by local law enforcement to identify potential targets for terrorist activity and to report these targets, as part of a jurisdictional assessment, to the FBI.

⇒ **Appendix C: Security Contacts for the Top 35 Transportation Systems** provides contact information for transportation police and security departments with experience in developing security and emergency preparedness programs.

- ⇒ **Appendix D: Detailed Capabilities Assessment Worksheet** provides additional questions for consideration when conducting the capabilities assessment described in Section 4 of the Guide.

- ⇒ **Appendix E: Sample Emergency Grant Processing Guidelines** provides information that can be used to establish grants for emergency preparedness drills. The purpose, goals and objectives, requirements, and sample eligible expenses are outlined.

- ⇒ **Appendix F: A Memorandum of Understanding Between [Local Public Safety Agency] and the [Local Transit Agency]** provides a sample language for a Memorandum of Understanding to support coordinated emergency preparedness between the public transit system and emergency responder agencies in its surrounding community.

Public Transportation Security and Emergency Preparedness Guide CD-Rom

To supplement information provided in this Guide, a CD-ROM is included that contains over 200 documents, prepared by federal and state organizations, industry associations, law enforcement, emergency management organizations, and the military. These documents explain the roles and responsibilities of the 47 Federal agencies involved in homeland security and provide useful technical assistance on a range of security and emergency management subjects. Sample procedures and model plans for transportation operators are also included on the Guide CD-ROM. These tools, most of which can be downloaded as Microsoft Word files, encourage the ready transfer of lessons learned. The CD-ROM contains an interactive shell to support easy navigation of contents and display of materials.

Assumptions Used in Guide Development

This Guide was written using the following assumptions.

- ⇒ The Guide serves as a primary focus to provide a single resource to support security and preparedness planning in the transportation environment.

- ⇒ Executive Overview is directed towards an audience of management personnel who must understand the challenges, management principles, and potential transportation roles and responsibilities sufficient to guide planning efforts for major events, including WMD terrorism. The remainder of this Guide, including the CD-ROM, is directed at those personnel with responsibilities of developing, implementing, and evaluating policies, procedures, training, and exercises to support security and emergency preparedness.

- ⇒ This Guide presumes it is the responsibility of transportation operators to heighten their concern for critical infrastructure protection and be willing to improve and increase integration with the local community preparedness effort. This Guide does not answer questions concerning levels of involvement. Rather, this Guide describes how transportation personnel can identify resources, capabilities, and needs to actively seek improvement and integration into the community homeland security initiative.

⇒ The majority of recommendations in this Guide build on existing safety, security, and emergency management practices in public transportation. Many transportation systems located in large urbanized areas have initiated comprehensive planning, technology, and training programs with resources and capabilities not available to smaller transportation operators. This Guide should provide these larger systems with useful tools to support their on-going review of program implementation.

⇒ For smaller systems, with less experience in critical infrastructure protection, this Guide should provide an overview of key issues to consider. Templates, policies and procedures, located on the Guide CD-ROM, support implementation of tailored practices to enhance physical security and emergency preparedness.

⇒ The authors of this Guide recognize the special burdens placed on small and some medium systems in addressing heightened security concerns. In response to pressures that these systems may be under to develop documentation for security and emergency preparedness programs, tools and templates available on the CD-ROM support easy integration of standard practice and lessons learned into transportation procedures and rulebooks.

⇒ Without investing the time to read this Guide and to build partnerships with local law enforcement and other emergency responders, small and medium operators who use the CD-ROM templates will not receive their full benefit. These systems may run the risk of advertising a level of preparedness in their documentation that is not reinforced in training, exercising, and coordination with local responders.

⇒ The Guide emphasizes the capacity of the transportation system to communicate with first responders (fire fighters, police officers, and other federal, state, and local agency personnel) and build on those existing emergency management experiences and capabilities. Using established concepts, such as the Incident Command System (ICS) and all-hazards management, this Guide explains how transportation systems can improve coordination with their communities during emergencies, including those incidents involving weapons of mass destruction agents or devices.

⇒ This Guide draws on the existing body of open-source knowledge compiled by federal, state, and local agencies and practitioners, analysts, and transportation operations personnel regarding the management of WMD terrorism (much of which is included on the CD-ROM). Special emphasis has been placed on the results of studies and assessments detail lessons learned from the response to the September 11, 2001 attacks on the World Trade Center and the Pentagon.

1 Executive Overview

Recent events have focused renewed attention on the vulnerability of the nation's critical infrastructure to major events, including terrorism. This Guide has been prepared to support the activities of public transportation systems to plan for and respond to major security threats and emergencies. It emphasizes the importance of developing critical relationships, preparing strategies and policies, and setting training and funding priorities. It offers practical guidance for planning effectively, spending wisely, and making the public transportation infrastructure safer.

1.1 Building Vision

Major incidents, such as train accidents, fires, floods, violent crime, and terrorist attacks, have been an issue for public transportation since the first vehicles were placed into service more than a century ago. During these events, personnel from multiple disciplines and agencies must come together to manage the incident, performing such tasks as perimeter and traffic control; rescuing or evacuating passengers; supporting the transportation of emergency responders and equipment; managing victims and their families; controlling crowds; repairing facilities; communicating with the media; and restoring service.

Emergency management in public transportation is constantly evolving, incorporating lessons learned from major events, as well as facing new threats. Public transportation systems at the forefront of security and emergency management offer the vision illustrated in Table 1 to guide industry efforts for enhanced capabilities. This vision supports the industry's activity to manage current threats and reinforces a strong tradition of emergency operations.

Table 1: Program of Commitments

COMMIT to a program that enables the public transportation system to:

- ⇒ **PREVENT** incidents within its control and responsibility, effectively protect critical assets;
- ⇒ **RESPOND** decisively to events that cannot be prevented, mitigate loss, and protect employees, passengers, and emergency responders;
- ⇒ **SUPPORT** response to events that impact local communities, integrating equipment and capabilities seamlessly into the total effort; and
- ⇒ **RECOVER** from major events, taking full advantage of available resources and programs.

In adopting this vision, planning is more of a process than a product. Planning identifies potential targets and risks, vulnerabilities to various forms of attack, crime, and natural disaster, and allows these targets to be hardened and the risks to be mitigated. It also allows for modifications and amendments to procedures and operations based on experience and lessons learned. Planning provides the agency

an opportunity to ensure redundancy in critical system operations, including personnel for all major functions. It supports a flexible approach that can be expanded or contracted based on available personnel, resources, capabilities, and needs.

1.2 Managing Uncertainty

Legendary Coach John Wooden's somber reminder that "failure to prepare is preparing to fail" applies to the challenge of preparing for terrorism and other major events in the transportation environment. During these events, response decisions must be executed very quickly to prevent additional harm.

The capability to perform effectively with uncertainty is the result of practice and self-assessment. Systems that know their own strengths and weaknesses, and have invested in developing core capabilities, skills, and knowledge, will be better off. Not only will they succeed in managing responses to terrorist attacks, but in handling all events with the potential to result in the loss of life and property.

Terrorism is a rare occurrence. Even more traditional emergencies, such as major accidents, hazardous material spills, natural or technological disasters, and riots happen infrequently. A bus or rail supervisor may experience only one of these events in his or her entire career.

Given this lack of frequency, it is difficult to expect competency in these highly charged situations. Yet, the consequences of poor decision-making in response to extraordinary events are grave. Unless adequate preparation is provided, transportation personnel may be unable to mobilize effectively to manage critical incidents on their systems and to support community response when most needed.

General advice, prepared by sources ranging from industry associations, to the Federal Transit Administration (FTA), and the Federal Bureau of Investigation (FBI), reinforces previous findings that security and emergency preparedness are not one-size-fits-all propositions. There is no universal cookbook-for-preparedness, and there are no assurances that even the most protected assets will not be targeted. However, within this framework of uncertainty, evidence does suggest that:

⇒ location makes a difference;
⇒ vigilance is critical; and
⇒ resource availability must be respected.

1.2.1 Location Makes a Difference

According to the FBI, what makes a specific facility or location attractive to a terrorist is not always easy to identify. Based on current intelligence, the FBI urges transportation systems serving communities with the following characteristics to consider themselves at a higher level of risk:

- ⇒ availability of targets with symbolic meaning for the United States government or its culture and way of life;
- ⇒ availability of targets with precursor elements for major destruction (chemical or nuclear/radiological material);
- ⇒ availability of targets whose destruction would provide the potential terrorist element (PTE) with visibility and prestige;
- ⇒ availability of targets with the potential to significantly impact not only a single community, but also a state and the nation;
- ⇒ availability of high-value targets (e.g., high replacement costs, high commercial impacts of delay and destruction, high loss on US economy);
- ⇒ availability of major targets that provide relative ease of access (ability of PTE to ingress and egress with equipment and personnel required for attack); and
- ⇒ availability of targets that would produce mass casualties (in excess of 500 persons).

In a cooperative partnership with state and local law enforcement, the FBI has requested completion of vulnerability self-assessments emphasizing the above characteristics for each community. Appendix B contains the full vulnerability self-assessment supplied by the FBI, which is also included on the Guide CD-ROM. Using this worksheet, transportation systems should attempt to identify the specific vulnerabilities of their facilities. Based on the results of this assessment, the transportation organization may wish to share a copy with local law enforcement, or to include a representative from law enforcement in the assessment process, to support their understanding of the transportation function and role in the community.

Tools discussed in this Guide, including the Capabilities Assessment (Section 4) and the Threat and Vulnerability Assessment (Section 5), will help transportation personnel evaluate the specific requirements of their operations.

It should be noted that neither the FBI Vulnerability Self-Assessment, nor the additional tools provided in this Guide are definitive in their findings. Their use by law enforcement and industry professionals does not mean that a terrorist event cannot occur in a rural community or small or medium-sized city. It only means that, in the words of terrorism analyst Brian Jenkins, "attacks in such areas are less likely." As he reports:

"Historically, the United States, although a comparatively violent country, has not suffered high levels of terrorist violence. Within the United States, six major metropolitan areas (New York, Miami, Washington, D.C., Chicago, San Francisco, and Los Angeles) account

for a majority of the terrorist incidents [including active investigations and interdictions]."[3]

1.2.2 Vigilance is the Best Defense

All sectors indicated that the most important threat reduction measure is vigilance on the part of the transportation system's staff, their awareness of anything out of the ordinary, and their prompt communication of that information to the organization's security team or management.

To this end, management should promote awareness and encourage familiarity with the spectrum of threats. Some questions to consider are listed below.

- ⇒ What types of weapons might be used against public transportation vehicles, operators or passengers?
- ⇒ How can system personnel recognize a chemical or biological incident?
- ⇒ What are special conditions that could be observed by operators, maintenance personnel, and passengers?
- ⇒ How can transportation staff and passengers be effective eyes and ears for the community?

Procedures, training, and reinforcement should be provided to all employees to make sure that they understand what constitutes an unusual event and what they should do upon observing one. Managers should be committed to developing internal procedures for handling reports of unusual activity or objects and should encourage their enforcement.

These procedures, when integrated into day-to-day operations, may have other benefits as well. Improved internal coordination and reports from the field may encourage better system housekeeping and more responsive maintenance practices for quality-of-life issues, such as burned-out light bulbs and over-grown shrubbery. To receive maximum benefit, consistency in the system's approach to security and awareness is critical. It hurts the program when managers speak passionately about the importance of security and then fail to deliver support and encouragement to employees who report incidents meeting system criteria that are later revealed to be of little or no consequence.

1.2.3 Security should be Responsive to Available Resources

Cost is a legitimate criterion in designing security and preparedness measures. Many of the security measures recommended by federal, state, and local systems have also been found to contribute to the

[3] Jenkins, Brian Michael, *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*, Mineta Transportation Institute, MTI Report 01-14, October 2001, Page 2.

efficiency of public transportation operations (vehicle locating systems, multimodal communications), passenger safety (design and materials used in station and coach construction), and making systems more convenient and attractive to passengers (good lighting, clean interiors, timely information on system status, visible presence of staff), and to reducing ordinary crime [closed-circuit television (CCTV), high-profile and undercover patrolling].

Many of these measures involve only modest expenditure. For example, improving liaison with local police and other emergency responders, establishing crisis management plans, conducting exercises, and putting procedures in place for handling bomb threats and suspicious objects are not costly undertakings.

1.2.4 Other Recommendations

Other recommendations to transportation executives are included below.

⇒ **Develop a security and emergency preparedness program (SEPP) plan**. In many cases, this plan will bring together many of the system's existing activities, integrating them into an overall security and preparedness effort, rather than a disparate set of technologies and procedures. Use the CD-ROM templates and tools to support documentation of the plan, communication with employees, and coordination with local responders.

⇒ **Consider a security staff position.** If at all feasible, it is recommended that every transportation system assign security planning and preparedness assessment responsibilities to a single individual. Clear leadership in planning is critical.

⇒ **Take a balanced approach, commiserate with system resources and capabilities.** Threat levels and protection requirements vary with the size of the community and the features of the service area. Evaluate threats and vulnerabilities using realistic scenarios that identify those elements of service with the potential for mass casualty events. Preparation should focus on the most likely threats in order to insure that budgets and human capital are distributed appropriately. Transportation activities should be coordinated with each community's on-going emergency planning effort and integrated into mutual aid agreements and the state emergency operations plan.

⇒ **Plan first, then spend.** Extreme spending in response to a recent crisis is not sustainable over the long-term. Security and emergency preparedness programs must be accountable for their return on investment. Managers must be careful not to initiate programs that will eventually fall into disrepair under a different set of threat conditions.

⇒ **Get involved.** A national effort is underway to address the many institutional issues that have challenged emergency preparedness programs for the last decade. Transportation organizations should work to be included in this process. Transportation organizations also offer valuable resources to support their communities. These resources should be identified and incorporated into the overall homeland security effort.

⇒ **Identify an adequate level of preparedness.** Every transportation system should set goals by which to assess its state of readiness. These goals will help establish benchmarks to determine how much preparedness is enough and establish funding and training priorities to meet that level. For example, transportation providers may play a special role in the sheltering or evacuation of communities and the management of medically vulnerable populations. In this case, emphasis should be placed on reviewing or developing plans and procedures to promote and assess readiness in this area.

⇒ **Emphasize readiness in system activities**. Role-playing in operator meetings and tabletop simulations, answering questions addressed to staff, and practicing drills and interagency exercises are vital to ensure that employees and local responders are familiar with plans and equipment and develop needed skills. Interacting through exercises also provides an opportunity for systems to develop working relationships and mutual trust.

⇒ **Develop robust emergency management plans based on an all-hazards approach.** When multiple systems that may or may not be familiar with one another respond to a disaster, their management teams need to be highly integrated to avoid confused, delayed, or redundant response efforts. An emerging paradigm of operational command, known as the incident command system (ICS), is now widely adopted by state and local response agencies. Transportation providers should ensure that they are able to access this system. Local law enforcement can be a valuable resource in explaining ICS and clarifying transportation roles and responsibilities.

⇒ **Plan for public reassurance.** A public affairs function can impact preparedness because it gathers, packages, and disseminates crucial information from the government to the public. The media play a critical role in both warning and informing the public. Terrorism broadcasts in real-time have powerful impacts on citizens. Providing accurate and timely information throughout a crisis can establish and maintain public trust in the government, calm anxieties, and instruct the public regarding actions they should and should not take. Recent experience has shown that inconsistent messages from different portions of government can

have significantly negative impacts. It is also vital that the chief executive and key staff members are available to the media to both inform and reassure the public with a clear and consistent message.

1.3 Investment in Security and Emergency Preparedness

It is important to recognize that security and emergency planning in public transportation includes not only the system, including its employees, facilities, passengers, and operations, but also those local agencies upon which the system relies for public safety support:

⇒ local responders (police, fire, emergency medical services, coroner, and local public health department);
⇒ planning organizations [local emergency management agency (EMA), local emergency planning committee (LEPC), and local government]; and
⇒ mutual aid partners and regional agencies (who provide critical support during an emergency and support coordinated planning activities).

As indicated in Figure 1, the level of activity required by the public transportation system for security and emergency planning typically has a direct correlation to:

⇒ the number of passengers moved by the system;
⇒ the number of fixed facilities operated by the system; and
⇒ the number of local jurisdictions within the system's service area.

Increasing numbers of passengers and facilities bring the potential for increased loss, which requires more sophisticated protection and preparedness capabilities. Transportation systems serving multiple jurisdictions must extend additional resources for coordination and incident response. This often requires the capacity to develop a Memoranda of Understanding and other formal agreements for mutual aid and support.

The relationships depicted in Figure 1 are reflected in the resources currently allocated to security by industry. Disproportionately, these resources are assigned to the (relatively) small number of systems that serve large urban areas.

⇒ Collectively, the nation's 75 largest public transportation systems devote just over 4 percent of their annual operating funds to security personnel and equipment. These systems serve the nation's top 50 cities, and move 85 percent of all passengers who use public transportation.[4]

⇒ Most of these systems provide fixed-route bus services; approximately 40 also have heavy, light, and/or commuter rail systems. All of these systems

[4] As reported to the NTD for FY 2000, the 7 largest public transportation systems each provide in excess of a million passenger trips every day; the next 5 largest agencies provide in excess of 500,000 passenger trips. Each of the remaining top 35 agencies moves more than 100,000 passengers daily. Lastly, the remaining 40 systems, rounding out the top 75, provide between 50,000 and 100,000 daily trips.

provide paratransit service in accordance with the Americans with Disabilities Act (ADA) requirements and community agreements.

⇒ Heavy and commuter rail systems typically have their own sworn police departments or a dedicated unit of local law enforcement. In most instances, these operations are multimodal, so police responsibilities often extend to bus and paratransit operations. Appendix C provides a listing of transportation law enforcement and security contacts at these agencies.

⇒ Of the remaining systems in the top 75, a few bus-only and bus-light rail operations have sworn transportation police. Many more have security departments that oversee contractual arrangements with local law enforcement or non-sworn security personnel for security support and fare enforcement.

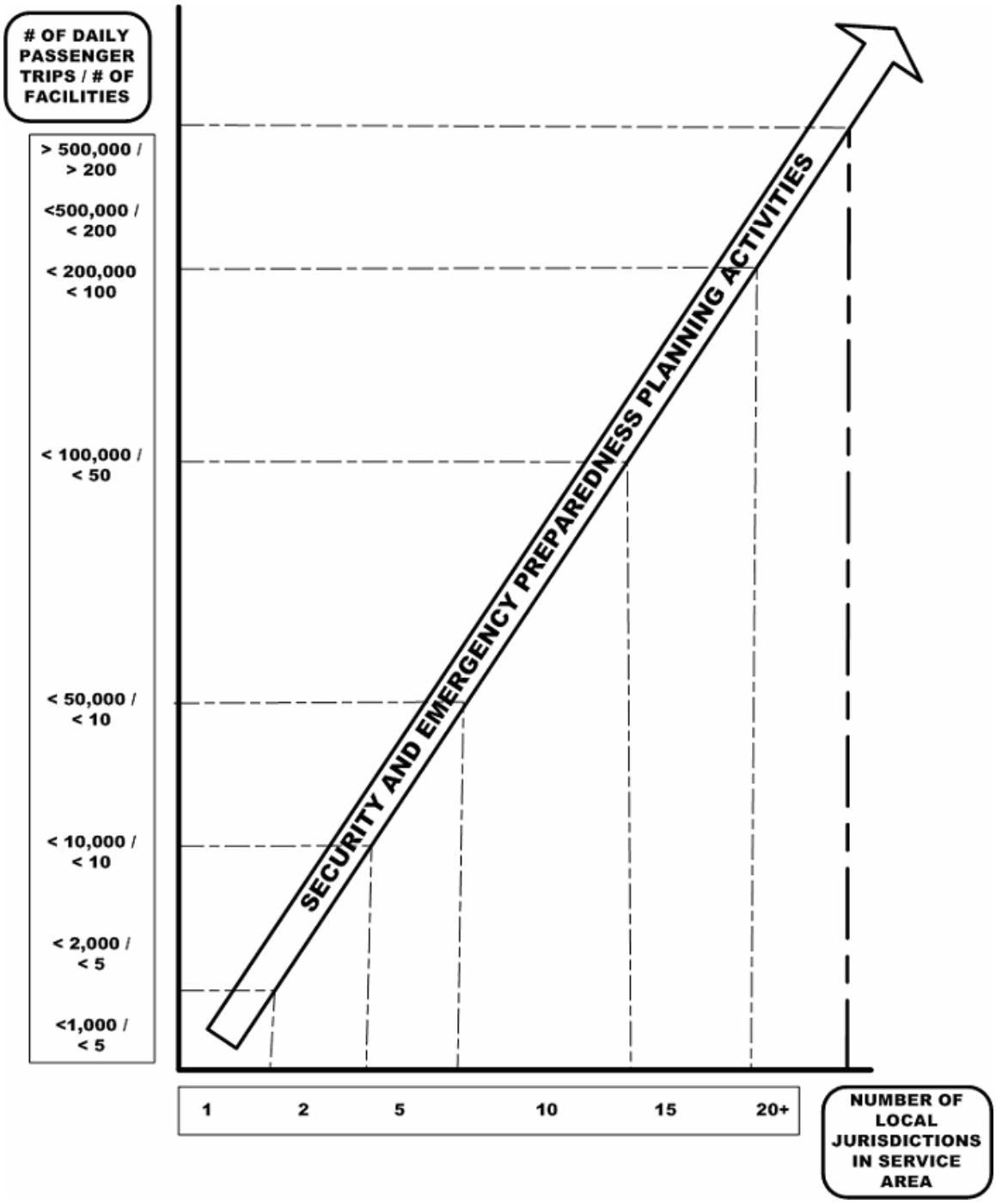


Figure 1: Requirements for Security and Emergency Preparedness

Tables 2 and 3 both illustrate valuable industry resources currently devoted to security.

Table 2: Industry Security Snapshot, Fiscal Year 2000

Category of Transportation System (by ridership)	% of Total U.S. Ridership, FY 2001	Total Annual Unlinked Passenger Trips	% of Annual Operating Expenses Spent on Security	Average Cost of Security per Rail Passenger Unlinked Trip	Average Cost of Security per Bus Passenger Unlinked Trip
Top 75 Transportation Systems	85 percent	8 billion	4.2%	$0.18	$0.04
Systems 76 to 150	7 percent	660 million	.05%		$0.02
Systems 101 to 500	5 percent	450 million	.05%		<$0.01
Remaining Systems (approx. 7,000)	3 percent	300 million	.03%		< $0.01

Table 3: Law Enforcement or Security Personnel, Fiscal Year 2000

Category of Transportation System (by ridership)	% of Total US Ridership, FY 2001	Total Annual Unlinked Passenger Trips	Average Cost to Deploy a Full-time Law Enforcement Officer	Average Cost to Deploy a Full-time Security Guard	Security Personnel per Million Unlinked Passenger Trips
Top 75 Transportation Systems	85 percent	8 billion	$70,000	$50,000	1.28
Systems 76 to 150	7 percent	660 million	$50,000	$35,000	.04
Systems 101 to 500	5 percent	450 million			
Remaining Systems	3 percent	300 million			

⇒ Systems falling between 76 and 150 in terms of ridership provide between 50,000 and 10,000 passenger trips each weekday. Primarily, these trips are comprised of fixed-route and demand-response paratransit service. The larger systems in this category may have a designated security function to oversee a contract with local law enforcement or non-sworn security. In a few instances, these systems have dedicated units of local law enforcement. However, the majority of these systems rely on operator and supervisor training, security technology, and close coordination with local law enforcement to protect passengers and respond to incidents. These systems often emphasize the critical role played by operators and supervisors in

maintaining controlled environments on their vehicles, as well as the legal responsibility of local law enforcement for the criminal offences occurring on the streets and sidewalks of its jurisdiction.

⇒ The nation's remaining operators (small motor bus, paratransit, and rural and community service), who collectively provide eight percent of all trips on public transportation, have no dedicated security personnel. Security is addressed as part of general safety; risk management, operations, or facilities maintenance. Some of these systems may have contracts with local law enforcement or private security for limited program support or special events. These systems typically have very limited resources for security considerations and limited experience in managing security-related threats. If an event should arise, these systems typically work closely with their primary clients to resolve the situation. A client list may include public transportation boards, community organizations, or regional programs.

This Guide recommends that, wherever possible, transportation personnel coordinate with their local partners to invest in strategies that promote integrated assessment of threat and response capabilities. The coordinated management of security and preparedness issues enhances the system's ability to protect critical assets from those events that can be prevented and mitigated.

Figure 2 (on the last page of this section) illustrates the elements of protection in the transportation environment.

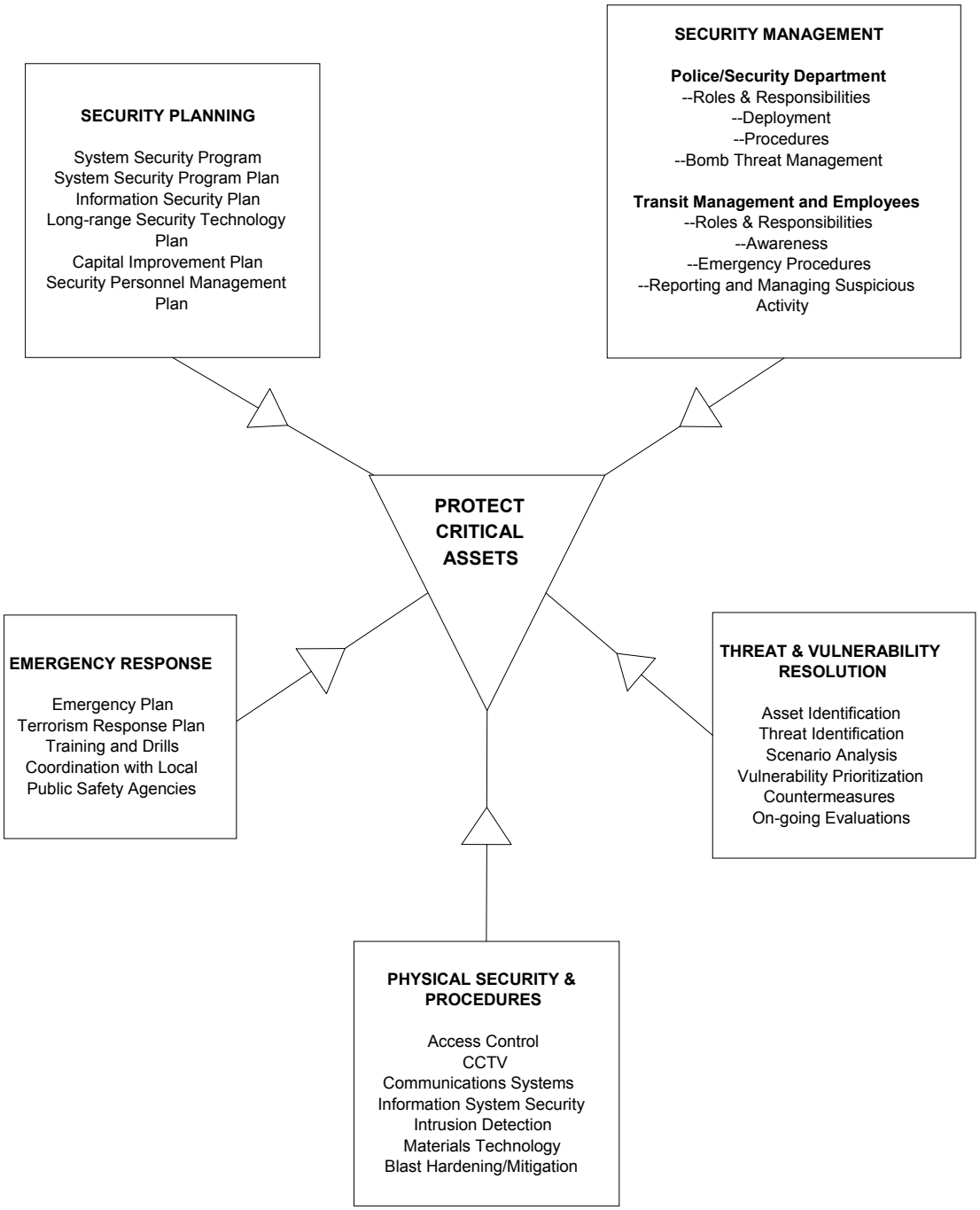


Figure 2: Elements of Protection

2 Security and Preparedness in a Diverse Industry

There are over 7,500 local public transportation systems in the United States today. The main challenge of the federal government is to encourage security and preparedness programs that will protect them all. This may seem like an impossible task when taking a closer look and comparing the many different systems across the country to each other. Each system has a unique way of carrying out security measures that best suit each particular system's needs.

Table 4 illustrates the diversity of the nation's public transportation network.

Table 4: US Public Transportation Inventory

INVENTORY	Motor Bus	Heavy Rail	Light Rail	Demand Response	Ferry Boat	Commuter Rail	TOTALS
Number of Systems	2,262	14	33	5,254	28	18	**7,609**
>1,000 Buses	10						
999>500 Buses	20						
499>200 Buses	38						
199>50 Buses	404						
<49 Buses	1,790						
Number of Employees	195,548	45,155	6,048	47,509	3,433	22,399	**320,092**
Number of Vehicles	75,754	10,301	1,205	32,899	124	4,907	**125,190**
Unlinked Passenger Trips	5.8 billion	2.7 billion	315 million	113 million	52 million	421 million	**9.4 billion**
Operating Expenses	$11.1 billion	$3.5 billion	$600 million	$1.3 billion	$270 million	$2.5 billion	**$19.3 billion**
Average Fare	$0.69	$0.96	$0.58	$1.60	$1.32	$3.40	

2.1 Diversity in Public Transportation

Every day in the US, publicly funded transportation systems provide approximately 32 million passenger trips. These systems serve commuters, students, tourists, people of age, persons with disabilities, and others who rely on trains, buses, ferries, vans, and other accessible vehicles and facilities to reach their final destinations. The public transportation infrastructure is varied and dynamic, including:

⇒ the nation's largest system, the Metropolitan Transportation Authority (MTA) New York City Transit (NYCT), which employs 40,000 professionals and transports over 8 million daily passengers, using one of the world's largest networks of bus and rail vehicles and supporting infrastructure;

- ⇒ a medium to small sized bus system in the Midwest, serving a mixed rural-small urban regional area, and providing 7,000 daily passenger trips; and
- ⇒ a non-profit, demand-responsive system in the southwestern United States, with two vans and a car pool program, serving an isolated rural community with volunteer drivers, providing 30 daily passenger trips.

2.2 Existing Threat Management Process

The public transportation industry faces many threats, all of which have the potential for disrupting local communities, causing casualties, and damaging and destroying public and private property. At a national level, the industry will be affected by several major events each year; ranging from floods, earthquakes, hurricanes, tornados, major accidents, hazardous materials spills, fires, violent crime, and, potentially, terrorism.

Figure 3 provides common categories of threats and a typical evaluation matrix for determining the relative impacts of these threats, based upon the likelihood that the threat will result in an actual event and the expected severity of the consequences should that event occur. The Federal Emergency Management Agency (FEMA) and the Federal Bureau of Investigation (FBI) use this tool to support the activities of communities in developing threat mitigation programs and emergency plans.

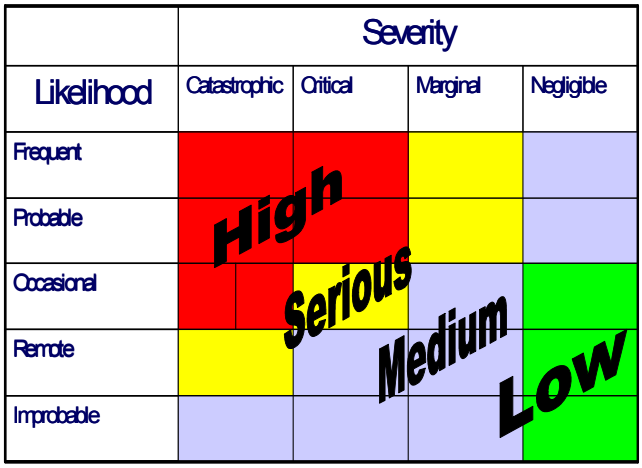
Using this approach, a small operator in Ohio may determine that the threat of tornados is sufficient to justify a sky-watcher training program for key field personnel. A large provider in southern California may invest in the development of design criteria to enhance structural integrity and redundancy in power and communications to support earthquake resistance and rapid restoration of service. This evaluation process is iterative, ongoing, and responsive to new and emerging threats.

2.3 Implications for Terrorism

In this era of heightened concern regarding terrorism, transportation managers have good reason to attend to the security and preparedness of their operations. Threat assessments issued by the Federal Bureau of Investigation (FBI) have consistently placed public 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.

CATEGORY	LIKELIHOOD OF OCCURRENCE	SEVERITY OF OCCURRENCE
HAZARD TYPE	**(SEE BELOW)**	**(SEE BELOW)**

NATURAL
Drought
Earthquake
Flash flooding
Flooding (river or tidal)
High winds
Hurricane
Landslide
Tornado
Wildfire
Winter storm
TECHNOLOGICAL
Dam failure
Energy or fuel shortage
Hazmat or oil spill (fixed site)
Hazmat or oil spill (transport)
Major structural fire
Nuclear facility incident
Water system failure
SOCIETAL
Civil unrest or riot
Strike
Civil panic or looting
SECURITY
Violent crime (Part I crime)
Other crime (Part II crime)
Bomb threats
Chem-bio-nuclear agent threats
Workplace violence
Explosive device/detonation
Chem-bio-nuclear device/release
Other terrorism



LIKELIHOOD OF OCCURANCE

Frequent:	Event will occur
Probable:	Expect event to occur
Occasional:	Circumstances expected for that event; it may or may not occur
Remote:	Possible but unlikely
Improbable:	Event will not occur

SEVERITY OF OCCURANCE

Catastrophic:	Disastrous event
Critical:	Survivable but costly
Marginal:	Relatively inconsequential
Negligible:	Limited or no impact

Figure 3: Common Threats and Evaluation Matrix

Acts of terrorism have many common characteristics both in the United States and other areas of the world. To guide the threat posture for the emergency planning

and response community, the International Association of Fire Chiefs (IAFC) provides the following observations regarding terrorist acts.[5]

⇒ All terrorist acts are crimes. Most involve violence or threats of violence.
⇒ Terrorists target civilians; where they work, live, and congregate.
⇒ Terrorist actions are designed to receive maximum publicity.
⇒ Terrorist actions are intended to produce effects beyond immediate physical damage, to instill fear and devastation in the civilian population.
⇒ Once a terrorist incident is underway, the success rate is nearly 75%. The presence of suicide bombers raises the success rate to over 95%.
⇒ Law enforcement, fire, rescue, and emergency management personnel may not be better trained or equipped than terrorists.
⇒ Terrorists will not have the same perspective as first responders regarding consequences of the initial event, and may attempt to exploit the vulnerability of first responders arriving on an emergency scene by using secondary devices or staging attacks involving other weapons. Worldwide, secondary devices will be deployed about 50% of the time.
⇒ The American public now expects that an extraordinary rescue effort will occur after any terrorist incident.
⇒ The tactics of terrorism are constantly changing, yet the basic objectives remain the same: to create fear and mistrust in government.
⇒ The events of September 11 established a new benchmark in sophistication of terrorist attacks, demonstrating advancing skills and willingness to kill thousands of people indiscriminately.
⇒ Responders should be prepared for terrorist incidents that escalate in scope and magnitude.
⇒ Terrorist acts are not accidents or disasters; they are intentional actions designed to inflict civilian casualties.

2.4 Meeting the Threat

For most transportation systems, addressing this threat requires activities designed to:

⇒ recognize and prevent potential security incidents and emergencies; and
⇒ enhance response capabilities.

At many systems, developing a security and preparedness program is a central component of these activities. The first step in creating this program is often to build consensus in two critical areas:

⇒ Where is the risk?
⇒ Whose responsibility is it?

[5] *Enhancing Fire Service Response to Today's Terrorism Threat,* http://www.iafc.org/downloads/index.shtml.

The first question focuses on the system's ownership of risk. Managers must understand which parts of its operation are at risk and why. By evaluating risk, managers are determining their needs to ensure that the organization does not spend valuable resources on unnecessary safeguards while, at the same time, exposing itself to unprotected loss.

Responsibility refers to conscious decisions about whether to deny, accept, or transfer risk. Responsibility and accountability for security should determine resource investment. At all times, managers should remember that no decision or avoidance of decision-making is still a decision.

2.5 System Security and Emergency Preparedness (SSEP)

System security and emergency preparedness (SSEP) offers a valuable tool to support the efforts of transportation managers to answer system security questions. System security is defined as:

---

the application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources

---

⇒ System security provides a structured methodology for analyzing threats and weighing the consequences of the cost of their resolution against the capabilities of the system to fund improvements.

⇒ This process builds on the transportation industry's strong safety culture, applying analysis techniques and management processes traditionally used for safety hazards to security threats and vulnerabilities.

⇒ System security identifies security and emergency preparedness measures that protect both the community and transportation employees, while keeping the system operational and effective, even under adverse conditions.

⇒ This process allows the system; whatever its size, service, or operating environment; to implement the most effective security and preparedness program possible within its available resources.

Within the context of this approach, emergency preparedness is a central feature of the program, ensuring the capability to mitigate and manage those events that cannot be prevented. Emergency preparedness is defined as:

---

a uniform basis for operating policies and procedures for mobilizing public transportation

---

System security promotes an integrated approach to protection, identifying how all system activities come together as part of an interdependent system that deters,

detects, assesses, and responds to threats. As indicated in the Figure 4, this process has the following components:

⇒ physical resources to delay and deter the adversary;
⇒ equipment installed to detect and assess alarms and support surveillance;
⇒ personnel used for security systems management, operations, and response;
⇒ procedures essential for system operation and effectiveness; and
⇒ training, exercising, and assessment to assure response capabilities.

2.6 Benefits of SEPP

Because security has historically been managed as part of day-to-day transportation operations, many systems may not recognize the benefits of preparing a formal security plan. Yet, the planning process:

⇒ provides a systematic vision for its security and preparedness activities;
⇒ enhances the system's ability to coordinate with local authorities;
⇒ supports development of best practices and technology programs; and
⇒ provides the basis for training and exercises.

In an era of heightened public concern and expectation, formal security planning ensures that the public transportation system is doing all that it can to leverage limited resources for physical protection and effective emergency response.

By investing time and money in security and preparedness efforts, transportation managers can reduce the likelihood of adverse effects on employees, passengers, and the environment, as well as help to avoid costly losses that would result from a major event. This program can also be a valuable tool for maintaining operational integrity.

Some of the benefits of implementing an SEPP include:

⇒ safeguarding employees, passengers, first responders, the community, and the environment;
⇒ reducing litigation risk, insurance costs, and theft;
⇒ reducing the risk of vandalism and sabotage by employees and non-employees;
⇒ improving relationships with local authorities and surrounding communities;
⇒ providing a mechanism for personnel control and accounting ; and
⇒ supporting effective crisis communications internally and with passengers.

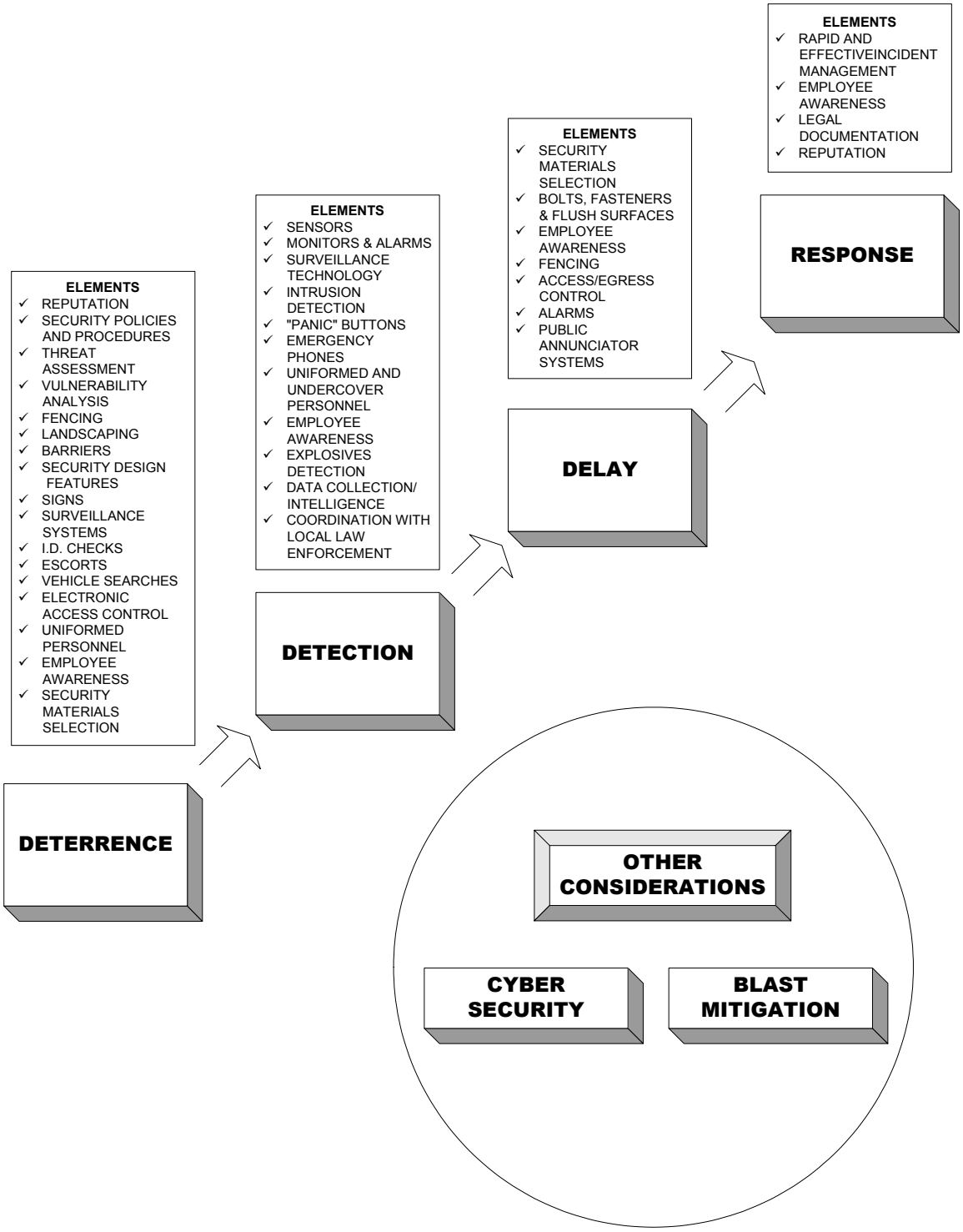


Figure 4: System Security Approach to Prevention and Response

2.7 Steps in the Program

For most systems, this program consists of the following seven steps, which are also depicted in Figure 5.

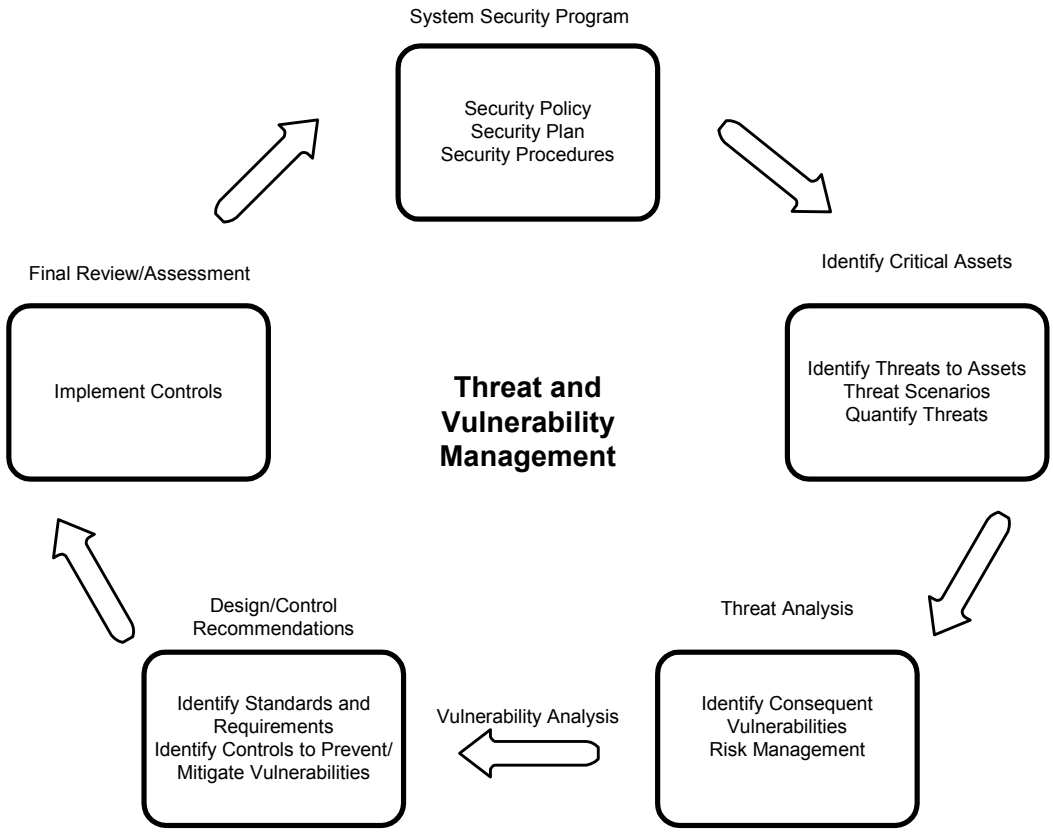


Figure 5: Steps in the System Security Methodology

⇒ **Step 1**: Designate an organizational capability to manage security issues for the system. For small systems, this assignment can be part-time for a single employee. For the nation's larger systems, dedicated transportation police perform this function.

⇒ **Step 2:** Create a Security and Emergency Preparedness Planning (SEPP) Team. For small systems, this can be the existing Bus/Vehicle Operators Committee or an Ad Hoc Committee, including representatives from systems served or contractors used to provide service. Larger systems may have several distinct committees (security planning, security operations, security breach review, as well as committees that focus on emergency management and coordination with local responders).

⇒ **Step 3:** Perform a SEPP capabilities assessment to develop a snapshot of the system's current level of readiness. If applicable, the system should also identify baseline security practices that are consistent across its operations or modes of service.

Most transportation systems work closely with local public safety agencies, local planning organizations, and regional or mutual aid partners in creating their programs. Figure 6 demonstrates how these activities are coordinated at many systems.

Activity	Transportation Security Manager	Transportation Police/Security Department	Security & Emergency Preparedness Planning Team	Local Public Safety Agencies	Local Planning Agencies	Regional/Mutual Aid Agencies
Perform Capabilities Assessment						
Identify Assets						
Identify Threats						
Identify Vulnerabilities (Perform Scenario Analysis; FBI Self-Assessment Worksheet)						
Prioritize Vulnerabilities						
Establish Physical Security Baseline						
Identify Other Measures						
Establish Preparedness Planning and Procedures						
Conduct Training, Exercises, and Evaluation						
Maintain Interagency Coordination						
Update Plans and Training						
Commit to Institutional Learning						

Lead Role

Support/Review Role

No Likely Role

Figure 6: Coordination with Local Systems

⇒ **Step 4**: Conduct a Threat and Vulnerability Assessment to identify critical assets, vulnerability to specific threats, based on the likelihood of occurrence and the severity of occurrence (given current security baselines and/or practices), and to develop passive and active counter-measures for addressing prioritized vulnerabilities.

⇒ **Step 5:** Develop a System Security and Emergency Preparedness Plan to describe system roles and responsibilities for these activities. Small systems may have one combined plan. Larger systems may have multiple plans (System Security Plan, Basic Emergency Plan and Incident Annexes, and Terrorism Response Plan). The Guide CD-ROM provides a complete template for this plan.

⇒ **Step 6:** Develop a work plan for implementing countermeasures. This may include, in the short-term, issuing bulletins to operators and meeting with local law enforcement. Long-term implementation measures include developing annual programs for exercising emergency notification and response procedures and developing a master plan for CCTV implementation at the system.

⇒ **Step 7**: Emphasize readiness in all system activities, including role-playing in operator meetings, tabletop simulations, what if exercises, tabletop simulations, drills, and interagency exercises are vital to ensure that transportation employees and local responders are familiar with plans and equipment and develop needed skills. Interacting through exercises also provides an opportunity for systems to develop working relationships and mutual trust.

3 Developing the Security and Emergency Preparedness Program (SEPP)

Creating a security and emergency preparedness program (SEPP) formalizes top management's commitment. Without clear management authority and written policies and procedures, the system's activities for security and emergency preparedness will remain vulnerable to misunderstandings and confusion in the field. Heightened public accountability also encourages prudent transportation management to commit its program in writing.

⇒ Documented programs are more credible to employees, local law enforcement and emergency planning agencies, ridership associations, and the media. A written plan issued under executive management signature conveys a level of professionalism and commitment appropriate to a system dedicated to the safe and secure transportation of passengers.

⇒ The process of documenting the program encourages the identification of opportunities for physical security enhancements, technology acquisition, operations improvements, and greater coordination within the system, with local law enforcement and/or other response agencies.

⇒ Review of the program also identifies weakness in current practices, provides a management tool to support revision of procedures, and enhances enforcement and implementation of the program.

⇒ A written plan can be used to train and simulate exercises with personnel, ensuring that employees understand what is required in a variety of situations.

⇒ A written plan can be shared with local response agencies, to increase their understanding of transportation operations and security priorities.

⇒ A written plan supports brainstorming and proactive identification of what could happen and how the system would ideally like to respond.

⇒ A written plan can be a priceless resource in an actual emergency.

Figure 7 identifies activities that can be performed by a transportation system to develop its SEPP.

3.1 Authority

At a particular transportation system, security and emergency preparedness management responsibility generally should be assigned to one person. The FTA highly recommends that a full-time person be designated to these responsibilities, however if circumstances don't allow for a full-time person an upper level management person should be in charge of this effort, even if he or she has other responsibilities.

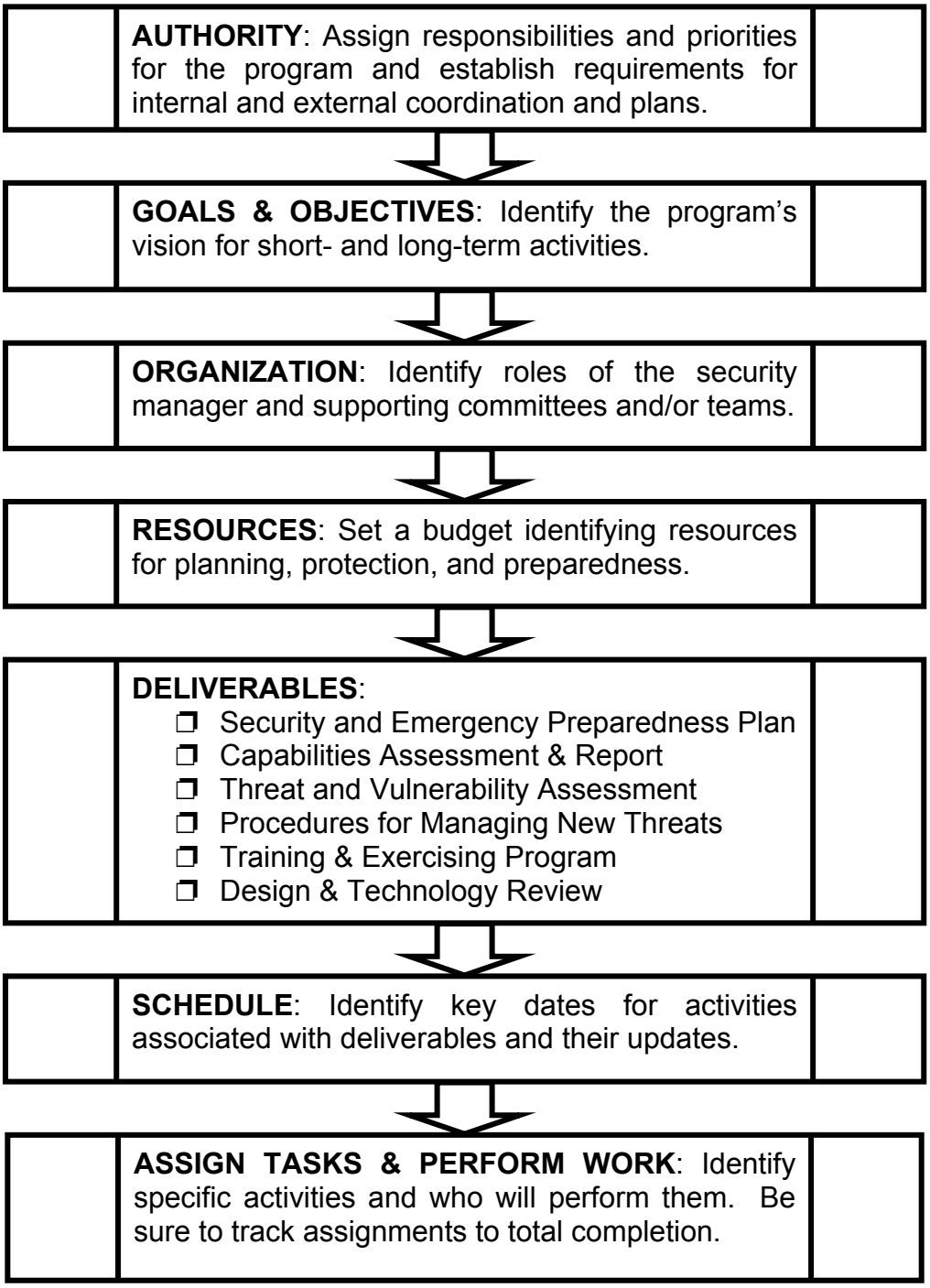


Figure 7: Activities to Develop the SEPP

The person assuming this role can coordinate a number of important functions, such as:

⇒ developing plans and policies;

- ⇒ managing annual capabilities and threat and vulnerability assessments;
- ⇒ establishing relationships with law enforcement agencies and other responders;
- ⇒ developing and managing incident and unusual event reporting systems;
- ⇒ boosting employees' security awareness;
- ⇒ referring security breaches for investigation;
- ⇒ coordinating emergency response; and
- ⇒ periodically assessing the system's security program.

In recognition of system-to-system variations, this Guide uses the term **security manager** to refer to the person ultimately responsible for the SEPP at each transportation system. No single staffing recommendation is adequate for all transportation systems; each security program must be developed and evolve to address local conditions and resources.

- ⇒ Depending on the size and resources of the system, the security manager may be the Chief of Transportation Police or the Director of the system's Security Department, with in-house or contracted sworn and non-sworn personnel to support passenger, employee and facility protection, and emergency response.

- ⇒ For smaller operations, the Chief Operations Officer, the Director of Safety, the Risk Manager, or the Facilities Manager may incorporate these activities into their duties, supported by a committee comprised of operating and administrative personnel, coordinated with local law enforcement.

- ⇒ Rural and community transportation providers have tapped a wide range of personnel for this function, including part-time dispatchers with previous law enforcement experience, supervisors or operators who manage other system committees, or the human services liaison with the local community planning organization. An ad hoc committee or another type of planning team can also support this function.

In determining the appropriate designation of responsibility for security and emergency preparedness, the transportation system may wish to consider which function can best:

- ⇒ validate routine practices already in place for managing security incidents, accidents, and medical emergencies; working with hazardous materials; preparing for spills; and managing conflicts or disorderly conduct on-board vehicles;
- ⇒ expand existing employee management and supervision practices to more fully address security and emergency planning; and
- ⇒ consolidate these practices, to develop an integrated program, coordinated with local response and planning agencies.

Whatever organizational structure is established by the transportation system, this Guide recommends that the security manager:

- ⇒ become a direct report to the system's executive director;
- ⇒ receives a separate budget line item for security activities;
- ⇒ receives clear authority for signing off on policies, procedures, construction projects, and plans; and
- ⇒ receives authority in overseeing the inclusion of security or emergency preparedness issues in the system's procurement and contracting process.

3.2 Goals and Objectives

The public transportation system can consider many possible goals for the program that should emphasize the major elements to be accomplished.

- ⇒ Develop a coordinated program to ensure that the transportation system, local emergency responders, and local planning agencies work together to identify vulnerabilities to acts of terrorism and other emergencies.

- ⇒ Encourage clear definition of security and emergency response roles and responsibilities, both within the transportation system and with local responders.

- ⇒ Support implementation of the Incident Command System (ICS) for major events occurring in the community.

- ⇒ Promote greater consistency in local, state, and federal requests for program funding, training, and exercising involving public transportation.

- ⇒ Identify and review the role of public transportation in community plans.

- ⇒ Develop an inventory of available equipment and resources that the transportation system can contribute to community emergencies.

- ⇒ Establish joint policies and procedures for evacuation and in-place protection in the event of contamination by chemical, biological, or radiological agents.

- ⇒ Identify how public transportation personnel should support scene management requirements at a major incident, including staging for mass casualties, search and rescue, and debris removal.

- ⇒ Identify how public transportation can support management of medically vulnerable populations during major emergencies.

- ⇒ Coordinate plans for special events in the community, such as fairs, concerts, and fireworks displays.

Objectives are specific measures required to implement goals. The public transportation system can consider many possible objectives for the program that should emphasize the more day-to-day elements to be accomplished.

⇒ Ensure that all transportation system employees and contractors:
- understand the requirements of the program;
- make security and preparedness a primary concern while on the job;
- cooperate fully with the system regarding any incident investigation; and
- raise security and emergency preparedness concerns to management.

⇒ Review current system safety, security, and emergency policies, procedures, and plans. Identify needed improvements among these documents.

⇒ Develop and implement plans for addressing identified improvements.

⇒ Coordinate with local public safety, community emergency planning, and human services agencies to address security and emergency preparedness, including participation in formal meetings and committees.

⇒ Develop, disseminate, and incorporate procedures pertinent to system activities into training for security and emergency preparedness.

⇒ Provide adequate driver training and continuing instruction for all employees and contractors regarding security and emergency preparedness.

⇒ Ensure performance of at least one emergency exercise annually.

⇒ Add a permanent agenda item oriented toward security and emergency preparedness matters on all standing safety and risk management committees.

⇒ Ensure status reporting from operating, training, and human resource departments to determine the level of compliance with system security and emergency preparedness policies, rules, regulations, standards, codes, and procedures to identify changes or new challenges as a result of incidents or other operating experience.

⇒ Ensure that the system's current organizational committee structure provides sufficient opportunity to:
- identify security conditions and problems at the system;
- organize incident investigations;
- develop and evaluate corrective actions;
- develop strategies for addressing system security problems;
- coordinate the sharing of security responsibilities and information; and
- coordinate interaction with external agencies.

3.3 Organization

While it is often said that security is everyone's responsibility, developing a program organization that clearly identifies security responsibilities can be challenging. In meeting this challenge, transportation systems typically organize activities by transportation system management level and function within the program.

These two approaches are discussed below. Sample organizational responsibilities are provided for both classification systems.

3.3.1 Management Level

By clarifying relationships between and among management levels within the system, a well-documented program supports the ability of the security manager to be proactive when addressing security and preparedness concerns. The security manager understands his or her role in the system and which management personnel have responsibility for approving, reviewing, and enforcing security policies and procedures.

3.3.1.1 Top Management

Top management is accountable for the safety and security of the system and the effectiveness of emergency response. Program responsibilities are typically identified for the executive director or general manager and the vice president or assistant general manager.

3.3.1.2 Division and Department Heads

Division and department heads are responsible for the security and preparedness of their divisions and departments, including employees, facilities, equipment, operations, and services provided. Additional responsibilities may include:

⇒ reviewing new security activities to determine how they impact the areas for which each manager is responsible;
⇒ developing implementation strategies for security-related activities to be assigned within the department safety and security action plans;
⇒ planning fiscal requirements of security activities; and
⇒ sharing security concerns and ideas for improvement.

Program responsibilities are typically identified for the following:

⇒ Director of Law Enforcement or Security;
⇒ Director of Transportation Development;
⇒ Director of Communications and Marketing;
⇒ Director of Finance;
⇒ Director of Rail Services;
⇒ Director of Bus Operations;
⇒ Director of Maintenance;
⇒ Director of Human Resources; and
⇒ Director of Legal Services.

3.3.2 Managers

Other types of managers are responsible for the security and preparedness of their sections, including employees, facilities, equipment, operations, and services provided. They are also responsible for conducting inspections and evaluating threats, vulnerabilities, and security concerns. The security manager, system safety manager, facilities manager, and/or risk manager are typically responsible for developing and monitoring implementation of the SEPP and reporting to top management.

3.3.2.1 Supervisors

Supervisors are responsible for the security and preparedness of their units, including employees, facilities, equipment, operations, and services under their supervision. They are also responsible for conducting inspections and evaluating threats, vulnerabilities, and security concerns. Typical personnel include the following:

⇒ Rail Operations Supervisor,
⇒ Controller and Trainer;
⇒ Bus Operations Supervisor,
⇒ Dispatcher and Trainer; and
⇒ Rail and Bus Maintenance Supervisors.

3.3.2.2 Employees

Each employee is responsible for working safely, securely, and for following established rules, procedures, policies, and safe work practices. All employees are responsible for:

⇒ considering the security of passengers, vehicles, and facilities in the performance of all of their regular activities and
⇒ offering suggestions for the improved security of transportation passengers, vehicles, and facilities to their division or department head, the system security manager (SSM), or to members of appropriate committees.

Employee security program responsibilities are typically identified for:

⇒ Bus Operator;
⇒ Rail Operator;
⇒ Bus or Rail Maintainer or Mechanic;
⇒ Maintenance of Way Maintainer;
⇒ Claims Processor;
⇒ Revenue Collector;
⇒ Employee Coordinator; and
⇒ Environmental Program Coordinator

3.3.2.3 Proactive Security Committee

This committee generally reports to top management through the chief operating officer or director of operations. The major task of this committee is to identify and resolve potential security risks that the transportation system may encounter. This is often accomplished by review and assessment of the following areas:

⇒ conduct system-wide security assessments to identify and to eliminate or lessen potential security concerns in existing facilities;
⇒ review of new facility designs to ensure that security principles have been incorporated into the design;
⇒ review of existing training programs and development of additional training programs, based on security needs identified by the committee;
⇒ review of existing and proposed security policies, rules, regulations, standards, codes, and procedures to identify and neutralize potential security problems;
⇒ identify organizational issues that may contribute to recurring security incidents or less effective responses to incidents;
⇒ promote security awareness through campaigns and security related events; and
⇒ assess response readiness by conducting simulation drills and readiness exercises.

3.3.2.4 Security Breach Review Committee

This committee also typically reports to top management through the chief operating officer or director of operations. This committee often consists of the same members as the proactive security committee, and additional representatives from outside agencies, such as local law enforcement and the public, whose presence the committee members feel would be useful. The major task of the committee is to identify security breaches and to review incidents to determine if the breach occurred because of:

Security Integration

Functions provided by the Proactive Security and Security Breach Committees are an integral part of public transportation agency system development and operations. These committees should not be isolated, but should be integrated into the agency's decision making process (for example during the design review of a system modification). This will ensure that all security issues that affect or will affect system operations are evaluated from a security perspective.

⇒ inadequate or ineffective policies or procedures;
⇒ failure by employees to properly follow policies or procedures;
⇒ an identified, accepted risk;
⇒ unforeseen actions against the transportation system; or
⇒ some combination of the above.

This committee has the authority to propose or recommend additions or changes to policies and procedures. It can further recommend specific courses of action to prevent or minimize security breaches of a similar nature.

3.3.2.5 Function within Program

Once management roles have been clarified, the program can establish the specific activities to be performed. A program matrix is often used to document this activity. This matrix can stand-alone but is recommended to be incorporated into the overall management matrix of the organization to insure that security is part of all management review and decisions. This matrix identifies tasks for the program by operating department, often specifying the level of responsibility using the following conventions:

⇒ **P, Primary Task Responsibility**. The identified participants are responsible for the preparation of the specified documentation.
⇒ **S, Secondary or Support Responsibility**. The identified participants are to provide support to accomplish and document the task.
⇒ **C, Comment Responsibility**. The identified participants are to review and provide comment on the task or requirement.
⇒ **A, Approval Responsibility**. The identified participants are to review, comment, and subsequently approve the task or requirement.

Table 5 presents a sample for consideration by transportation systems, organized according to the sections of the Security and Emergency Preparedness Plan contained on the Guide CD-ROM.

Table 5: Program Roles and Responsibilities Matrix

		TRANSPORTATION SYSTEM							
PARAGRAPH NUMBER	TASK OR ACTIVITY	Management	Operations	Maintenance	Security or Safety	Training	Engineering	Human Resources	Risk Management
1.0	System Security Program Introduction	A	A	C	P	C	C	C	C
1.1	Purpose of System Security Program Plan and Program	A	A	C	P	C	C	C	C
1.2	Goals, Objectives, & Tasks for the Program	A	A	C	P	C	C	C	C
1.3	Scope of Program	A	A	C	P	C	C	C	C
1.4	Security & Law Enforcement	A	A	C	P	C	C	C	C
1.5	Management Authority & Legal Aspects	A	A	C	P	C	C	C	C
1.6	Government Involvement	A	A	C	P	C	C	C	C

Table 5: Program Roles and Responsibilities Matrix

		TRANSPORTATION SYSTEM							
PARAGRAPH NUMBER	TASK OR ACTIVITY	Management	Operations	Maintenance	Security or Safety	Training	Engineering	Human Resources	Risk Management
1.7	Security Definitions	A	A	C	P	C	C	C	C
2.0	System Description	C	C	C	P	C	C	C	C
2.1	Background & History of System	C	C	C	P	C	C	C	C
2.2	Organizational Structure	C	C	C	P	C	C	C	C
2.3	Human Resources	C	C	C	P	C	C	C	C
2.4	Passengers	C	C	C	P	C	C	C	C
2.5	Services or Operations	C	C	C	P	C	C	C	C
2.6	Operating Environment	C	C	C	P	C	C	C	C
2.7	Passenger, Vehicle, & System Safety program Plan	C	C	C	P	C	C	C	C
2.8	Current Security Conditions	A	A	C	P	C	C	C	C
2.9	Capabilities & Practices	A	A	C	P	C	C	C	C
3.0	Management of the System Security Plan	A	A	C	P				C
3.1	Responsibility for Mission Statement & System Security	A	A	C	P	C	C	C	C
3.2	Management of the Program	A	A	S	P	S	S	S	S
3.2.1	General Manager	A	C	S	S	S	S	S	S
3.2.2	Chief Operating Officer	A	A	S	S	S	S	S	S
3.2.3	System SSM	A	A	C	P	S	S	S	S
3.3	Division of Security Responsibilities	A	A	C	P	C	C	C	C
3.3.1	Job-specific Security Responsibilities	C	A	S	P	S	S	S	S
3.3.2	Operations Division Responsibilities	A	P	S	S	S	S	S	S
3.3.3	System SSM & Contract Law Enforcement	A	A	S	P	S	S	S	S
3.3.4	Proactive Security Committee	C	A	S	P	S	S	S	S
3.3.5	Security Breach Review Committee	C	A	S	P	S	S	S	S
4.0	System Security Program: Roles & Responsibilities	C	S	S	P	S	S	S	S
4.1	Planning	S	S	S	P	S	S	S	S
4.2	Proactive Measures	S	S	S	P	S	S	S	S
4.3	Training	S	S	S	P	S	S	S	S
4.4	Day-to-Day Activities	S	S	S	P	S	S	S	S
5.0	Security Program Threat & Vulnerability Identification, Assessment, & Resolution	C	P	P	P	C	P	S	C
5.1	Threat & Vulnerability Identification	C	P	C	P	S	S	S	C

Table 5: Program Roles and Responsibilities Matrix

		TRANSPORTATION SYSTEM							
PARAGRAPH NUMBER	TASK OR ACTIVITY	Management	Operations	Maintenance	Security or Safety	Training	Engineering	Human Resources	Risk Management
5.1.1	Security Testing and Inspections	C	P	C	S	S	S	S	C
5.1.2	Data Collection	C	P	S	S	S	S	S	S
5.1.3	Reports	C	P	S	S	S	S	S	S
5.1.4	Security Information Flow	C	P	S	S	S	S	S	S
5.2	Threat & Vulnerability Assessment	C	C	S	P	S	S	S	S
5.2.1	Responsibility	C	C	S	P	S	S	S	S
5.2.2	Data Analysis	C	F	S	P	S	S	S	S
5.2.3	Frequency & Severity	C	C	S	P	S	S	S	S
5.3	Threat & Vulnerability Resolution	C	P	C	P	S	S	S	S
5.3.1	Emergency Response	A	A	S	P	S	S	S	S
5.3.2	Breach Investigation	A	A	S	P	S	S	S	S
5.3.3	Research and Improvements	A	A	S	P	S	S	S	S
5.3.4	Eliminate, Mitigate, or Accept	A	A	S	P	S	S	S	S
6.0	Implementation & Evaluation of System Security Program Plan	C	P	C	P	S	S	S	C
6.1	Implementation Goals & Objectives	C	P	C	P	S	S	S	C
6.2	Implementation Schedule	C	P	C	P		S	S	C
6.3	Evaluation	C	P	C	S	S	S	S	S
6.3.1	Internal Review – Management	C	C	C	P	S		S	
6.3.2	External Audits	S	P	S	S	S	S	S	S
7.0	Modification of the System Security Program Plan	S	P	S	S	S	S	S	S
7.1	Initiation	C	C	S	P	S	S	S	S
7.2	Review Process	C	P	S	P	S	S	S	S
7.3	Implement Modifications	P	P	S	P	S	S	S	S

3.4 Resources

To be effective, the program must have adequate resources to perform its identified activities. As indicated in Figure 8, program resources are commonly categorized as:

⇒ personnel;
⇒ budget; and
⇒ management support.

3.4.1 Personnel

Who is available to perform program activities, including in-house personnel, contractors, local law enforcement personnel, other responders, and local emergency planning agencies and committees? Security and emergency preparedness is an agency-wide activity. Cross-training of personnel is critical to promote effective emergency response and increase security awareness.

3.4.2 Budget

How much money is available, both in the short and long term, to fund physical protection, training, and preparedness enhancements? Are additional funding sources available from federal, state, local, and/or private sources? Are expenses for emergency response accounted for by the agency?

3.4.3 Management Support

How much authority does the security manager have to develop and implement the program? Will supervisors enforce these plans and procedures?

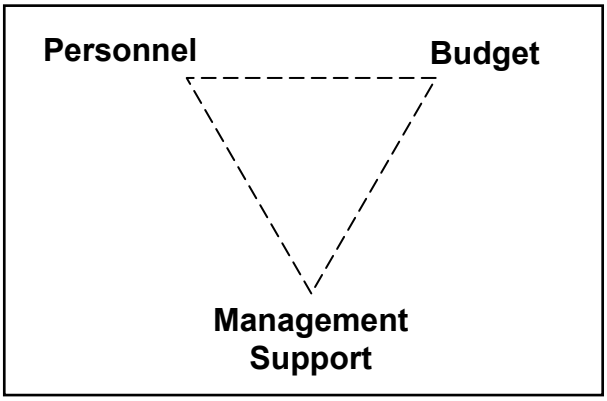


Figure 8: Resources for SEPP

Each transportation system should determine the resources available to develop and manage the program. This Guide recommends preparation of a budget for the program to clarify the resources allocated for activities and to support prioritization of activities.

3.5 Deliverables

The activity performed by the security manager and supporting personnel (whether a designated committee, internal transportation police or security department, contractor, or closer coordination with local law enforcement and fire services) requires an abundance of program resources. This Guide recommends that, whatever the size of the transportation system, the program needs to commit to the development of the following:

⇒ Security and emergency preparedness plan (SEPP) to document the system's program, organization, roles, and responsibilities. This may be supported by other emergency plans and procedures, emerging from coordination with the local community's planning process.

⇒ Capabilities assessment and report to identify the system's current activities for security and emergency preparedness and to make recommendations regarding the update or revision of existing plans, procedures, and training programs. See Section 4 of this Guide for more information.

⇒ Threat and vulnerability assessment to identify how heightened concerns over terrorism and other emergencies may create new risks for the operations and to recommend countermeasures for their resolution. See Section 5 of this Guide for more information.

⇒ Procedures for managing new threats to ensure that transportation personnel understand how to manage response to unusual events that may involve chemical, biological, radiological, or nuclear agents. See Section 6 of this Guide for more information.

[redacted]

⇒ Training and exercising to test and evaluate the system's emergency response preparedness and to encourage coordination with local responders. See Section 7 of this Guide for more information.

⇒ Design and technology review to investigate design concepts and security equipment. Technology that may improve facility and vehicle protection is available. See Section 8 of this Guide for more information.

3.6 Schedule

The security manager should prepare a schedule to help ensure that all activities are identified, assigned, coordinated, and tracked. As a rule of thumb, most systems require 12 to 18 months to complete the initial deliverables specified above. Many systems, depending on their size, perform annual or biennial reviews and updates, which typically are completed over a 3-month period. When setting a schedule for program activities, this Guide encourages transportation systems to use the SMART mnemonic.

When developing schedules, it is important to remain realistic regarding the amount of time allocated for review, revision, and evaluation. This practice is critical when system activities will be coordinated with local law enforcement and emergency planning agencies, whose staff may have scheduled monthly meetings for review of submitted materials from local organizations.

3.7 Assign Tasks and Perform Work

Figure 9 identifies a standard project management configuration for documenting ownership of specific deliverables. Dark circles indicate primary responsibility whereas white circles indicate supporting responsibility. Assignments for project deliverables should be a two-way negotiation beginning with deliverable definition and delegation. The negotiation should end with acceptance by the designated personnel for the responsibility to complete the deliverable in the required time.

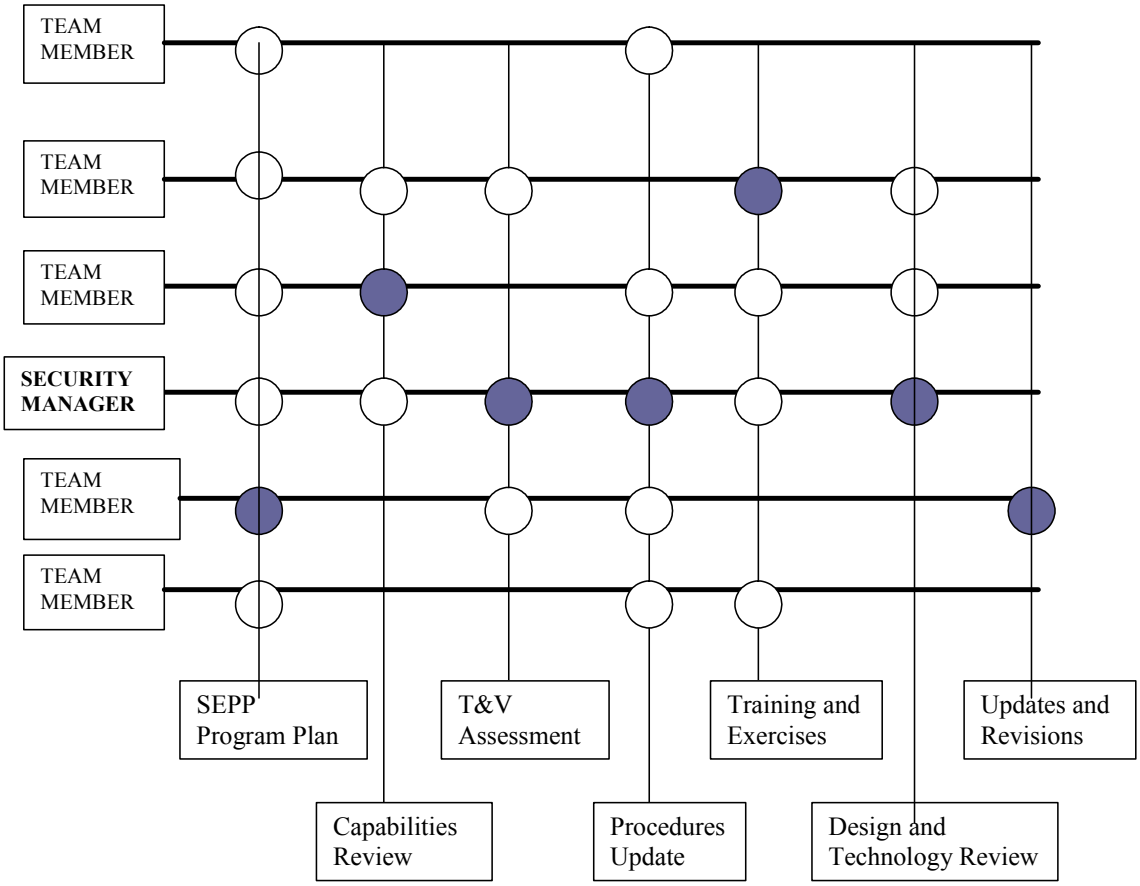


Figure 9: Sample Assignment Matrix

3.8 Preparing the SEPP

On the CD-ROM accompanying this Guide, there is a folder that contains a planning template that can be used by transportation personnel to create their system's own SEPP. This template is not intended to be the end product for any transportation system. It should be customized to reflect local needs and issues, documenting actual activities performed by the system.

3.9 Comprehensiveness of the Plan

When completing the draft template, management and its supporting committees should examine the plan to ensure that it is comprehensive. SEPP plans should address all system activity for security and emergency preparedness. To meet this objective, make sure the plan adequately addresses the purpose, scope, responsibilities, and implementation involved with the plan.

Employee Considerations

During major emergency/disaster conditions one consistent and successful activity employers have discovered is that in order for their employees to report to, and remain at work, they must be comfortable that their families are safe and unharmed. Employers should develop plans and procedures that allow a designated agency representative(s) to locate employee family members so that indirect communication can be maintained. The agency should encourage employees to maintain and submit, for example, a *Family Member Locator Plan* that details contact information for family members and loved ones.

The agency's plan and/or procedures should provide policies on what and how information will be disseminated and collected. Each employee should be given a copy of the plan and policy and share this with his/her own family members.

3.9.1 Purpose

SEPP plans usually contain a statement, often at the beginning of the plan, describing the reason it is being established and any associated goals. This purpose provides a key motivator for the system and is often unique to the culture and operation of the service. It should be stated that the security plan is an integral portion of the safety plan and program.

3.9.2 Scope

SEPP plans should define the level of organization covered. Does it include planning, design, construction, and procurement, or only revenue-service? How extensively are human resources, passenger services, legal counsel, and risk management involved in the implementation of the plan? The plan should also include specific information about the personnel, equipment, facilities, and services being covered.

3.9.3 Responsibilities

SEPP plans assign appropriate responsibilities to operators, supervisors, managers, and department heads. For instance, management is responsible for general compliance in order to satisfy the requirements and goals of the plan. The human resource department is responsible for implementing specific penalties and disciplinary actions to ensure enforcement of the policy. Department supervisors may also need to take on this disciplinary role. These responsibilities must be clearly defined for effective implementation.

3.9.4 Implementation

SEPP plans should provide for implementation and on-going evaluation. They should define the reports, inspections, training, committee meetings, and/or other activities to ensure that employees fully understand the system's security and emergency response procedures.

3.10 Clarity of the Plan

Management should examine the plan to see if it is clear, concise, and accurate. SEPPs should not require activities or commit to programs that are not feasible for the system or unfamiliar to employees. Plans should be clear, concise, and accurate.

⇒ The plan should be readable and its meaning should be clear. It must have the appropriate procedures and practices referenced.

⇒ The plan should not attempt to document and explain every security and emergency activity performed by employees. Rather, the plan should provide a security management tool that emphasizes processes, roles, responsibilities, and accountability. Specific procedures should be referenced, but not included.

⇒ Most security plans will be publicly available under the Freedom of Information Act (FOIA). In the event of a potential legal action or media inquiry, these plans must describe system operations. An incomplete or in-progress plan is far preferable to a plan that exaggerates security capabilities and requirements. Those who must implement the plan and earn additional respect and credibility for the security program will also appreciate accuracy.

3.11 From Plan to Procedure

Management should examine the relationship between the plan and its supporting procedures. SEPP plans should explain how the program will be managed and how general policies will be addressed by the system.

⇒ Procedures should detail how things are actually done. Procedures give plans their teeth and operating reality, but are not included as part of the plan (only referenced).

⇒ The system's rulebook, bulletins, notices, or special orders should consistently address the activity required in the SEPP plan.

⇒ In the event that few procedures are documented for the program, some employees may resist an effort to create them. But, what happens when they are not there? How will an off-peak emergency be managed if no one has contact names and phone numbers, or knows how to reach a specific agency (the coroner's office, for example) or a specialized vendor to make an immediate repair on a vital piece of security equipment?

3.12 Growth of the Plan

Management needs to examine the plan to make sure it can grow with the program. SEPP plans should remain open to change based on new risks and vulnerability, especially following an incident. Management of training exercises and actual incidents provides some of the greatest opportunities to improve processes, policies, and procedures. This offers a small window of opportunity to make changes while organizational inertia is temporarily suspended. Management should ensure that the plan takes advantage of these special conditions and circumstances.

3.13 Integrating the SEPP into Local Planning

Effective response does not happen by accident. It is the result of planning, training, exercising, and intra/interagency cooperation, coordination, and communication. Integration into the local community's emergency planning process is central to the success of the SEPP and to the preparedness of the system.

In the SEPP, the transportation system will have defined its internal processes for identifying security events, mitigating their consequences, and managing effective response. For some systems, the process of preparing the SEPP and documenting preparedness for security and other events may be sufficient planning. For other systems, the SEPP is but one in a series of plans that document the system's emergency response capabilities and performance requirements. Whatever the system's position and resources regarding the appropriate documentation of its emergency program, coordination with the local community is essential to successfully fulfill all SEPP functions. These include proactive planning, exercising and training, threat mitigation, consequence management planning and implementation, and an after action report.

Local, state, and federal emergency managers use an all-hazards approach in developing comprehensive preparedness, mitigation, response, and recovery plans for man-made and natural disasters. Planners set up basic disaster functions (i.e., rescue, sheltering, and medical care) and assign agencies and volunteer groups at the local, state, and federal levels to carry them out. Responders have the responsibility to implement these plans and to work within their legal authorities and capabilities to resolve critical incidents. The transportation system should be included in this process and reflect its activities as appropriate. For review and consideration, sample transportation emergency plans are included on the Guide CD-ROM.

The agencies in Figure 10 are considered key players in planning for and responding to WMD terrorism and other major emergencies.

3.13.1 Local Government

Local governments have primary responsibility in planning for and managing the consequences of a terrorist incident using available resources in the critical hours before state and federal assistance can

arrive. Public transportation systems coordinate their emergency response functions through integration into this local planning effort.

Though local planning guidelines will direct initial response to acts of terrorism and other major events, these guidelines reflect requirements specified by state and federal agencies for incorporating additional resources to manage major events.

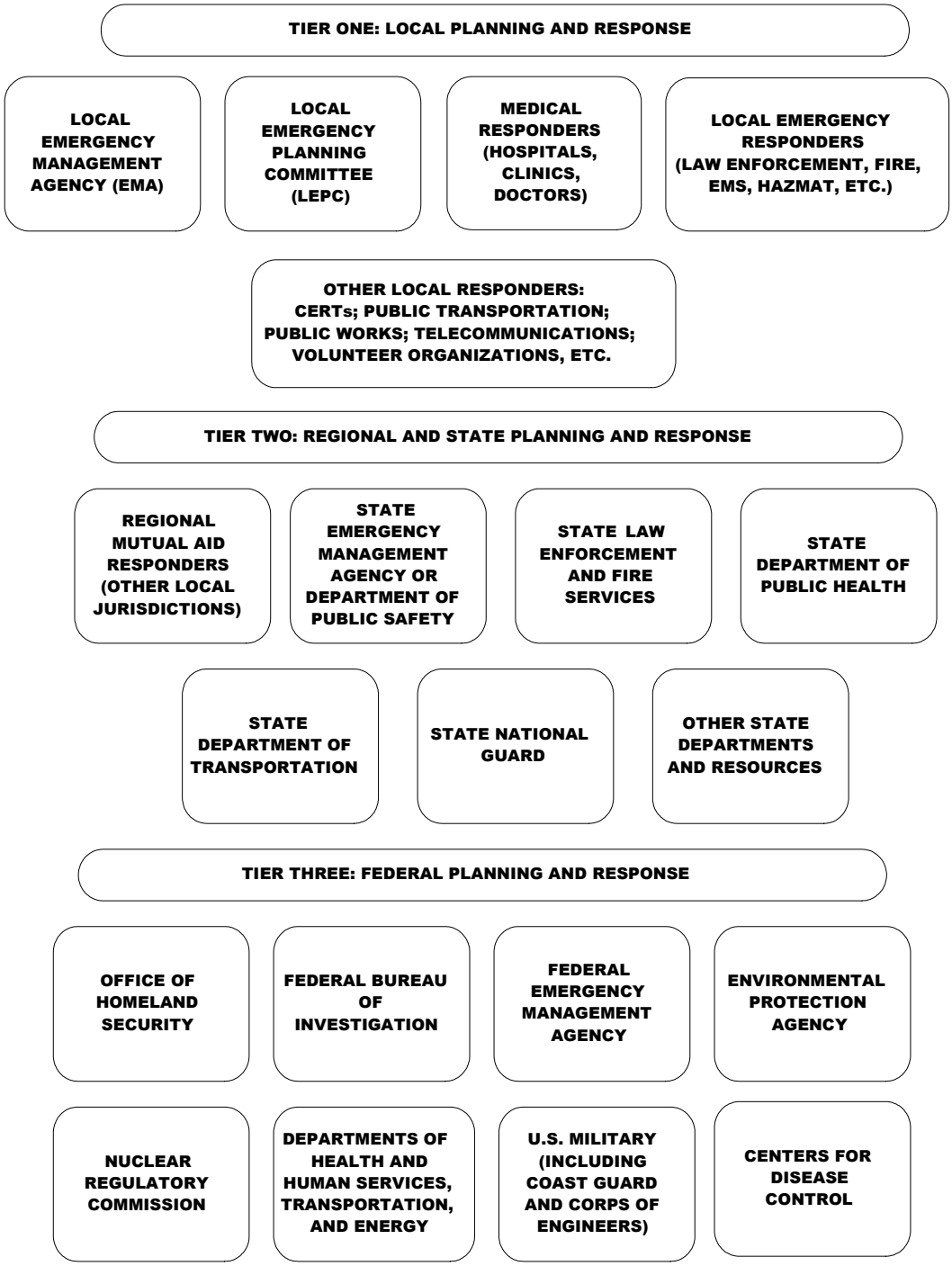


Figure 10: Agencies Involved in Planning

Federal departments and agencies have developed plans and capabilities for an integrated federal response to terrorist incidents and other major emergencies. This response network is detailed in the Federal Response Plan (FRP), including its Terrorism Incident Annex. The FRP is managed by the Federal Emergency Management Agency (FEMA), and addresses the following federal regulations:

⇒ US Public Law 920, as amended (US Civil Defense Act);
⇒ US Public Law 93-288, as amended (Robert T. Stafford Act);
⇒ US Public Law 99-499, as amended (Superfund Amendment and Reauthorization Act [SARA] of 1986);
⇒ Federal regulations 10 CFR 70, 10 CFR 71, 10 CFR 73, 44 CFR 350, 49 CFR 171, 49 CFR 172, 49 CFR 173, 49 CFR 177;
⇒ NUREG-0654/FEMA REP-1, Revision 1 and related Guidance Memoranda;
⇒ FEMA REP-5: Guidance for Developing State, Tribal, and Local Radiological Emergency Response Planning and Preparedness for Transportation Accidents;
⇒ Federal Response Plan (for Public Law 93-288, as amended);
⇒ Federal Radiological Emergency Response Plan (FRERP), as amended; and
⇒ National Guard Regulation (AR) 500-1/National Guard Regulation (AF) 55-5.

Through these requirements, federal agencies have identified specific responsibilities to be carried out or required by state departments and government. This combined system has generated three primary sets of guidelines for local governments, promulgated by state governments in response to federal requirements. Public transportation systems, in their programs for local emergency response planning, must work within this established framework.

3.13.2 State Government Emergency Planning Program

State government programs typically require county-level emergency management, administered by county emergency management agencies (EMAs) or equivalent organizations, and may require or recommend municipal programs for urbanized areas meeting specific requirements. These state regulations also typically specify conditions to be met for receipt of state funds and resources in the event of an incident that overwhelms local resources. State requirements are usually coordinated with US Public Law 93-288 (Robert T. Stafford Act) and overseen by FEMA as requisites for the receipt for funding in the event of presidential declarations of disaster.

State requirements for emergency planning are typically detailed in the state emergency operations plan (EOP) that addresses state-wide activities to be performed in the event of occurrences that exceed the capabilities of local and regional resources. For planning purposes, these

events typically include natural disasters, technological hazards, civil emergencies, and national security events.

Public transportation roles and responsibilities, typically identified in state EOPs and organized according to the ESF structure, appear in Figure 11.

TRANSPORTATION SERVICE	FRP ESFs	AGENCY
Community Evacuation & Shelter; Transport of Responders & Equipment	**ESF #1 Transportation**	Department of Transportation
Transport of Communications Equipment, Infrastructure, & Dispatchers	**ESF #2 Communications**	National Communication System
Damage Assessment, Emergency Repair, & Traffic Control	**ESF #3 Public Works/ Engineering**	Corps of Engineers
Transport of Equipment, Meals and the Provision of Shelter to Responders	**ESF #4 Firefighting**	Department of Agriculture/ Forest Service
Rosters of Mobility-impaired & Transit-dependent Residents, Public Information	**ESF #5 Information/Planning**	Federal Emergency Management Agency (FEMA)
First Aid Training, Vehicles to Support Victim Transport & Supplies, Managing School Children & Mobility-Impaired	**ESF #6 Mass Care**	American Red Cross
Vehicles; Towing Equipment; Generators and Other Essential Items	**ESF #7 Resource Support**	General Services Administration
N/A	**ESF #8 Health/Medical Services**	Health & Human Services and other Public Health Services
Metal Workers & Other Skilled or Specialized Labor or Equipment	**ESF #9 Urban Search & Rescue**	Federal Emergency Management Agency (FEMA)
Contractors for clean-up, Traffic Control	**ESF #10 Hazardous Materials**	Environmental Protection Agency
Vehicles for Transportation of Goods & Supplies	**ESF #11 Food**	Department of Agriculture
Fuel & Electricity	**ESF #12 Energy**	Department of Energy

Figure 11: Possible Transportation Responsibilities

Typical objectives for state EOPs include:

- ⇒ maximizing the protection of lives and property;
- ⇒ ensuring state and local capabilities are in place for emergencies;
- ⇒ ensuring that the government is able to survive and continue to provide essential services under adverse conditions;
- ⇒ supporting local units of government, as necessary;
- ⇒ describing standards regarding training and exercising activities, plan maintenance, and other preparedness activities; and
- ⇒ ensuring that all current state and federal government planning requirements are met, maintaining eligibility for receipt of federal funds and support.

Most state EOPs are divided into a basic plan and annexes. The basic plan focuses first and foremost on the assignment of emergency responsibilities and general operations policies. The annexes elaborate on the emergency responsibility assignments made in the basic plan and are of principal value to those within an agency or department who are responsible for carrying out such assignments. Annexes often mirror emergency support functions (ESFs) specified in the federal response plan.

3.13.3 Nuclear Regulatory Commission (NRC) Requirements

NRC requirements mandate a comprehensive emergency response and exercising program to protect public health and safety in communities that support nuclear reactors and commercial nuclear power plants. This program must address:

- ⇒ on-site emergency response and evacuation at the nuclear power plant; and
- ⇒ off-site response and evacuation for the community surrounding the nuclear power plant, including a plume emergency planning zone with a radius of 10 miles from the plant and an ingestion planning zone within a radius of 50 miles from the plant.

The Nuclear Regulatory Commission (NRC) approves on-site plans. Approval of off-site plans is coordinated between the NRC and FEMA. Both onsite and offsite plans must be approved for every nuclear plant to obtain and retain an operating license.

3.13.4 Emergency Planning and Community Right-to-Know Act (EPCRA)

The EPCRA is also known as Title III of the superfund amendments and reauthorization act (SARA) regulations that specify requirements for businesses and for federal, state, and local governments regarding emergency planning and community right-to-know (CRTK) reporting for hazardous chemicals. The CRTK provision in the EPCRA helped to increase awareness of chemicals in local communities and the releases of these toxins into the environment. Most State legislatures have also

enacted CRTK laws that are consistent with federal law. As a result, states and communities, working with the industry, are better able to protect public health and the environment. Congress enacted the EPCRA regulations to benefit communities. The main goals of the law are:

⇒ to provide a basis for each community to develop and tailor a chemical emergency planning and response program to suit the community's needs and
⇒ to provide the public with a right-to-know attitude to identify, quantify, locate, and determine the physical and chemical properties of hazardous substances in the community.

Under the federal EPCRA law, local emergency planning committees (LEPCs) must be established for each community. The LEPC must develop an emergency response plan and review it at least annually thereafter. Section 321 of EPCRA states that nothing in EPCRA will preempt any state or local law. Thus, existing state law governs local emergency management planning as long as it meets the requirements of EPCRA. Most states have determined that planning by local emergency management jurisdictions will meet the requirements of EPCRA, if it integrates EPCRA requirements into the existing multi-hazard functional plan. A basic emergency management plan that addresses the following functions normally will fulfill the requirement for local emergency planning under Section 303 of EPCRA:

⇒ warning;
⇒ shelter and mass care;
⇒ evacuation;
⇒ emergency public information;
⇒ resource management; and
⇒ hazardous materials response.

In most situations, the LEPC does not develop a separate plan, but assists local governments in carrying out emergency planning related to hazardous materials. In this capacity, the LEPC provides an important resource useful to all local responders, ensuring that each local emergency response plan:

⇒ identifies facilities and transportation routes of extremely hazardous substances;
⇒ describes emergency response procedures, (onsite and offsite) for facilities and operations that manage hazardous materials;
⇒ designates a community emergency coordinator and facility coordinator(s) to implement the plan;
⇒ describes methods for determining the occurrence of a release, the probable affected area, and population; and performing release notification
⇒ describes community and industry emergency equipment, facilities, and the identity of persons responsible for them; and

- ⇒ outlines evacuation plans;
- ⇒ describes a training program for emergency response personnel (including schedules); and
- ⇒ presents methods and schedules for exercising emergency response plans to emergency medical personnel, fire service, and law enforcement agencies.

3.13.5 Inter-organizational Emergency Memoranda of Understanding

Inter-organizational Memoranda of Understanding (MOUs) or Memoranda of Agreement (MOA) can serve as the basis of mutual acknowledgement of the local, state, region, and Federal resources that each organization may provide during emergency response and recovery efforts. MOUs can take many different forms including formal or written as well as oral agreements[6]. Public transportation systems developing or entering inter-organizational MOUs may choose to include the following elements:

- ⇒ A list of participating emergency response organizations, including contact information of approving officials
- ⇒ Definition of jurisdictional boundaries for primary responding organizations
- ⇒ Detailed definition of the chain of command and control, communication, and evacuation procedures and responsibilities to followed at the scene of the incident
- ⇒ A statement to address potential changes in protocols
- ⇒ Identification and description of equipment resources to be made available for incident response
- ⇒ Description of public transportation system personnel and their duties
- ⇒ Training and exercising responsibilities
- ⇒ Provisions for revision(s) to the MOU
- ⇒ Provision for the identification and documentation of costs to be tracked for potential reimbursement

[6] Appendix F provides a sample Memorandum of Understanding between a public transportation agency and a local public safety agency.

4 Capabilities Assessment

There is growing recognition that, in order to be truly effective in the new threat environment, transportation systems should commit to the first directive of system security, which is to prevent first, then be prepared to respond.

Capabilities assessment provides an opportunity for the transportation system to take a step back from day-to-day operations, and to identify its security and emergency preparedness activities as part of a comprehensive program. In this assessment, the transportation system evaluates its existing capability to:

⇒ reduce the threat of crime and other intentional acts;
⇒ recognize, mitigate, and resolve incidents that occur in service and on system property;
⇒ protect passengers, employees, emergency responders, and the environment during emergency operations; and
⇒ support community response to a major event.

This activity also contributes three key elements the SEPP program:

⇒ an inventory of resources available to support response to an emergency event (either on the transportation system or in the surrounding community);
⇒ a list of roles and responsibilities for the transportation system in managing incidents on its own property and in supporting community response; and
⇒ notebooks for all major facilities containing critical information for on-scene responders.

The results are documented in a checklist or report delivered to top management, and used to guide both the threat and vulnerability assessment (discussed in Section 5 of this Guide) and the preparation of recommendations for activities to be performed in the SEPP plan. Table 6, at the end of this section, contains a summary findings checklist, followed by a detailed worksheet that can be used to guide the capabilities assessment.

4.1 Establish the Team

The system's security manager, supported by system security and/or preparedness committees, a consultant, or an ad hoc planning team, initiates the assessment by assembling a multidisciplinary team with sufficient expertise in transportation operations, security, and emergency response to yield a comprehensive approach without draining scarce resources of the system.

To solicit support from local response and planning agencies, the security manager should also consider inviting participation from local public safety agencies. In addition, team members may use existing relationships to seek public safety personnel review of relevant planning areas, such as security procedures for managing bomb threats, unusual events reports, and abandoned items or suspicious substances. The security manager may also consider giving a presentation regarding the team's activities to local law enforcement, fire and medical services, and the local EMA or LEPC.

Capabilities assessments can demonstrate to the local community that transportation management is genuinely concerned about security, emergency preparedness, accountability, and has the best interests of the community in mind when managing facilities and continuing service.

4.2 Program Review

Depending on the system's current level of security and emergency preparedness, the team may conduct its initial activities by reviewing existing plans and procedures or by documenting existing practices that may not be formally committed to writing. Whatever the system's status, the team should consider emphasizing the areas illustrated in Figure 12.

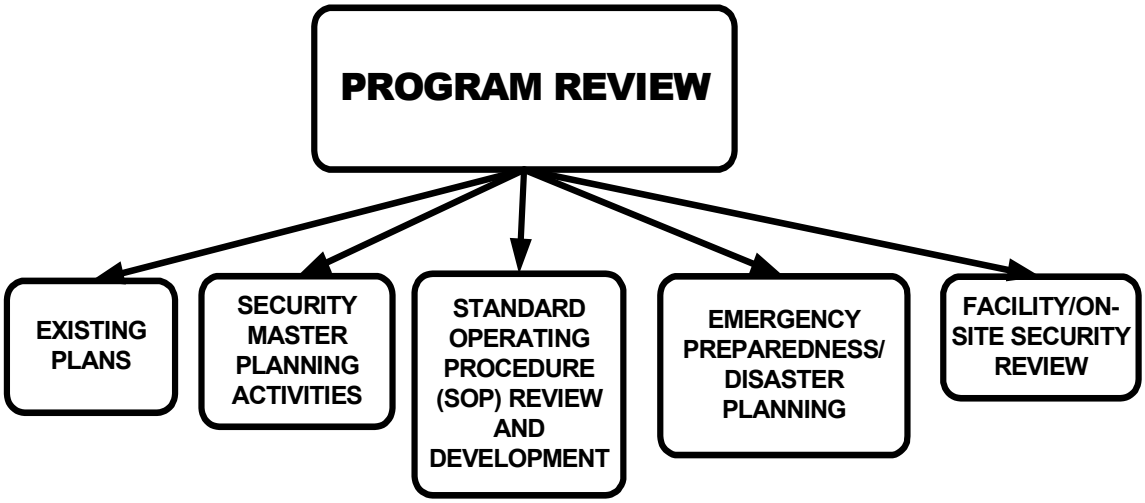


Figure 12: Capabilities Assessment Program Review

Once the team has been established, the real work of the assessment begins. This activity requires the team to:

⇒ identify all activities currently performed by the system to address security and emergency response issues and
⇒ display the system's physical security, management, training, and emergency response capabilities.

4.2.1 Existing Plans

The capabilities assessment typically begins by reviewing the system's existing plans for safety, security, and emergency response, if they are developed or available. These include:

⇒ System Safety Program Plan;
⇒ System Security Program Plan;
⇒ Safety and Security Certification Program Plan;
⇒ Emergency Operations Plan; and
⇒ Terrorism or Homeland Security Plan.

These plans should be reviewed for content addressing security and emergency preparedness activities. When conducting this assessment, the system may be in the process of developing its SEPP plan, so this activity provides an additional opportunity to review practices under consideration for the SEPP plan.

At the conclusion of this component of the assessment, the team should indicate in the assessment checklist the progress of the system's planning process, document the types of activities are documented in these plans, and clearly identify the system's planning assumptions regarding response to a major terrorist event on its property.

4.2.2 Security Master Planning

The program review generally considers the short and long term security design requirements currently in place, as they relate to facility infrastructure, policies and procedures, security operations, and existing security systems. These master planning elements typically include the following:

- ⇒ the system's physical security measures to delay and deter the potential offender and to ensure heightened awareness regarding potential threats and vulnerabilities;
- ⇒ the system's equipment and procedures in place to detect and assess unauthorized and/or unusual or unattended activities, packages, and substances;
- ⇒ the system's technology used for security systems management, operations, and response; and
- ⇒ the system's procedures essential for effective security system operation.

At the conclusion of this component of the assessment, the team should indicate in the assessment checklist what security equipment and procedures are currently in place at the system and general assessments regarding the level of procedural integration of this equipment into transportation operations.

4.2.3 Standard Operating Procedure (SOP) Review and Development

The program review also addresses the system's current process to ensure SOP development and documentation, including:

- ⇒ the system's policy regarding employee responsibilities for the identification and reporting of unusual conditions;
- ⇒ the provision of appropriate personnel and resources to ensure effective notification and management of these conditions, coordinating with local emergency responders as appropriate; and
- ⇒ the system's training, exercising, and assessment to initiate and maintain response capabilities and coordinate with local responders.

It is axiomatic in security that employees and contractors can serve as the eyes and ears of a system-wide security effort. Employees and contractors see much that occurs in and around the transportation operation and are in a good position to notice when something or someone seems out-of-place. Training and awareness measures can transform employees and contractors into a natural surveillance system.

Security managers may reinforce personnel training in security practices through bulletins, e-mailed security reminders, security tips posted on the system's intranet, advice and contact numbers in internal publications, and the distribution of security-related videos, pamphlets, wallet-cards, and posters. This activity should also be identified in the assessment.

Most transportation systems typically investigate unusual occurrences, reported incidents, and security breaches. Where appropriate, transportation management may refer such incidents to legal counsel for review. Any suspected illegal activity should be reported for referral to law enforcement. Criteria for these investigations should be identified in the assessment, and typically include:

- ⇒ doors not secured, holes in fence lines, indication of illegal entry;
- ⇒ unauthorized egress by personnel in restricted areas of the facility;
- ⇒ signs of vehicles in restricted areas along pipelines, fence lines, electrical substations, or remote plant security gates;
- ⇒ individual asking for technical information about the facility that could be used by an adversary to cause harm;
- ⇒ unexplained disruptions in service;
- ⇒ unexplained loss of parts and equipment;
- ⇒ unexplained illness of many transportation employees ; and
- ⇒ major cyber attack against internal process control systems.

At the conclusion of this component of the assessment, the team should indicate in the checklist whether policies and procedures have been developed to address particular security and preparedness topics and whether employees have received training on new procedures.

4.2.4 Emergency Preparedness and Disaster Planning

The program review also assesses system activity to review or develop response contingencies for security events that impact facility operations and personnel, resulting in emergencies. This activity also may address the review or development of procedures to protect life and assets, and to maintain continuity of business systems and operations in response to acts of terrorism and extreme violence. Efforts assessed might include developing contingency plans and procedures, creating comprehensive emergency plans, and providing training sessions to staff.

Emergency response and crisis management are natural functions that responsible security managers may perform for their systems. Proper crisis management may prevent an intrusion or attack from becoming a

major incident. In the transportation industry, emergency response and crisis management functions are especially complicated and may require specialized knowledge on the part of responders. A few measures that managers may currently perform include activities to:

- ⇒ implement an emergency response plan that fits system needs and resources;
- ⇒ Provide employees with information regarding the well-being of family members;
- ⇒ account for employees and visitors during emergencies;
- ⇒ attempt to preserve evidence for later investigations; and
- ⇒ manage a crisis communication system for key personnel and security staff so that they can:
  - o signal for help surreptitiously (with duress alarms, for example);
  - o keep a small incident from escalating into a large one; and
  - o easily contact other key staff members during a crisis (by any means, including intercoms, mobile and land-line telephones, e-mail, and two-way radios).

At the conclusion of this component of the assessment, the team should indicate emergency response and planning activities performed and identify, based on this activity, the likely roles and responsibilities assumed by the transportation system in supporting emergencies on its property and within the community.

A sample listing of activities that could be performed during emergencies includes:

- ⇒ emergency evacuation of citizens from affected area(s), coordinated with local law enforcement, the local Emergency Operations Center (EOC), the state Department of Transportation, and local highway, bridge and tunnel authorities;
- ⇒ identification and transportation of citizens with disabilities and those citizens dependent on public transportation who may be unable to reach an evacuation staging area;
- ⇒ evacuation of schools and day-care centers, and support for managing the reuniting of parents and children in the immediate aftermath of a major event;
- ⇒ temporary or in-place sheltering of evacuated citizens in air-conditioned or heated vehicles and stations;
- ⇒ transportation, in-facility transfer, or evacuation of hospitals, nursing homes, hospices, and other community and private facilities;
- ⇒ transportation of emergency workers and volunteers to and from an emergency staging site;
- ⇒ transportation of meals, goods, and supplies to an affected area for victims, emergency responders, or to support recovery operations;
- ⇒ provision of respite facilities and vehicles for emergency workers;

- ⇒ communications support for emergency responders (using hand-held and on-board vehicle radios, alpha-numeric pagers and Palm Pilots, cell phones, transportation dispatch facilities, and transportation communications infrastructure);
- ⇒ identification of routes and schedules to support the safe transportation of emergency responders, public utilities, support personnel, and other essential responders to an incident site or staging area;
- ⇒ provision of vehicles and equipment to support emergency operations and incident stabilization;
- ⇒ provision of estimates and information regarding the application of available resources to the movement of people or supplies;
- ⇒ provision of skilled craftsmen and heavy equipment to support initial debris removal during search and rescue operations;
- ⇒ provision of fuel, parts, supplies, and mechanics to support the maintenance of emergency vehicles;
- ⇒ provision of damage assessments and emergency repairs; and
- ⇒ provision of public information on agency websites and using public relations facilities and capabilities.

Untested response capabilities for weapons of mass destruction, explored by several communities over the last five years as part of the Nunn-Lugar-Domenici Domestic Preparedness Program, include the following:

- ⇒ use of transportation sprinkler systems and water supplies to support mass decontamination;
- ⇒ use of vehicle wash and maintenance facilities to decontaminate emergency vehicles and equipment;
- ⇒ provision of vehicle support for warm zone operations with trained bus operators using personal protective equipment (PPE);
- ⇒ use of vehicles or facilities as temporary morgues;
- ⇒ use of on-scene vehicles to provide barriers, shields, and shelter for contaminated, or potentially contaminated, victims who must disrobe;
- ⇒ use of in-place, transportation system contracts with hazardous waste management companies to support site clean-up and decontamination;
- ⇒ use of transportation personnel with basic first-aid training to support emergency or secondary triage and tagging of victims;
- ⇒ use of transportation vehicles for mobile command posts and secondary backup communications centers; and
- ⇒ integration of automated station and vehicle announcements and passenger information displays with local and regional ITS technology to support centralized management of passenger, pedestrian, and vehicle management from the community's emergency operations center (EOC).

At the conclusion of this component of the assessment, the transportation system should also complete the worksheet displayed in Figure 13

designed to communicate its response capabilities and resources to the local emergency planning community.

Facilities Provided by Transit System -- Please Check If Available:

- ❒ Communications center
- ❒ Evacuation shelter for _____persons
- ❒ Evacuation shelter for _____persons
- ❒ Evacuation shelter for _____persons
- ❒ Evacuation shelter for _____persons
- ❒ First aid and care center
- ❒ Goods and supplies storage center
- ❒ Other:

Services Provided by Transit System -- Please Check If Available:

- ❒ Surplus transportation for emergency response personnel
- ❒ Shelter or respite facilities for emergency response personnel
- ❒ Transport of emergency equipment and supplies
- ❒ Evacuation assistance
- ❒ Public information
- ❒ Transportation of "medically fragile" populations
- ❒ Communications support
- ❒ Traffic control/roadblocks/barriers
- ❒ Damage assessments and emergency repairs
- ❒ Other:_____
- ❒ Other:_____
- ❒ Other:_____

Vehicles Provided by Transit System -- Please Complete Information on Available Vehicles:

Vehicle Type	*Number*	*Size/Capacity*	*Lift-Equipped*	*Heating/Air Conditioned*
Buses				
Rail Cars				
Other Passenger				
Support Vehicles				

Equipment Provided by Transit System -- Please Check If Available:

Communications:

____2-way radios
____Hand-held radios
____Radio trunking capabilities
____Automated dispatch
____Alpha-numeric pagers
____Cellular Phones
____Palm pilots
____Internet-based
____Mobile data terminals
____Other

Other:

____Generators
____Metal working
____Fueling/maintenance facilities
____Towing Equipment
____Vehicle cleaning
____Other

Personnel Provided by Transit System -- Please Check If Available:

General

- ❒ Vehicle Operators
- ❒ System Police
- ❒ Non-sworn Security
- ❒ Dispatch
- ❒ Mechanics
- ❒ Administrative
- ❒ Other: _____

Specialized

- ❒ EMT or First Aid Trained
- ❒ Management of Medically Vulnerable Populations
- ❒ Damage assessment
- ❒ Construction management or engineering
- ❒ Other: _____

Information Provided by System -- Please Check If Available:

- ❒ Names and addresses of residents dependent upon public transportation services
- ❒ Names and addresses of residents with mobility impairments
- ❒ Names and addresses of school children routinely transported
- ❒ Other:_____
- ❒ Other:_____

Figure 13: Transportation System Resources

4.2.5 Facility or On-site Security Review

The program review concludes with an assessment of on-going activity to review the system's physical and procedural security systems and exposures. Findings from past and current threat and vulnerability assessment and design reviews may be of particular significance.

The conditions surrounding a security effort change constantly. Employees come and go, a facility's contents and layout may change, various threats wax and wane, and operations may vary. Even such mundane changes as significant growth of bushes or trees around a facility's exterior may affect the security plan (by shielding the view of any intruders). The assessment should document activities performed by managers to review their security measures periodically, as well as whenever facilities or other conditions change significantly. It may also be useful to system activity for the following:

- ⇒ update risk assessments and site surveys;
- ⇒ review the level of employee and contractor compliance with security procedures;
- ⇒ consider whether those procedures need modification; and
- ⇒ establish ongoing testing and maintenance of security systems (such as access control, intrusion detection, and video surveillance).

Figure 14 provides an example of the types of information typically collected during this phase of the assessment. This information can also support preparation of information folders or notebooks for each major facility. These materials can support emergency responders who may not be familiar with the site, and also enhance the system's capabilities to identify resources.

- ⇒ Location or address and nearby businesses and resources
- ⇒ Type of facility and typical uses by employees and passengers
- ⇒ Daytime or nighttime population
- ⇒ 24-hour points of contact
- ⇒ Voice, pager, beeper, and email information for facility
- ⇒ Unique hazards in facility (traction power, hazardous material storage, etc.)
- ⇒ Past threat history
- ⇒ Key dates for community
- ⇒ Floor plans and blue prints
- ⇒ Photos (ground level, aerial, key exits and entrances, proposed staging areas)
- ⇒ Heating, ventilation, air conditioning (HVAC) system characteristics
- ⇒ Blast analyses (if performed)
- ⇒ Procedures for controlling ventilation in response to toxic material release
- ⇒ Location of vents to street level and air out-take locations
- ⇒ Communications capabilities, accounting for radio dead spots and emergency phones
- ⇒ Location of equipment rooms and available power, water, and lighting (primary and backup)
- ⇒ Pre-designated emergency response support locations, including predetermined evacuation sites, command posts, and decontamination facilities
- ⇒ Evacuation plans

Figure 14: Characteristics of Transportation Sites

4.3 Documenting Results

At the completion of this assessment, the team should have an understanding of where the system is in terms of its current program. This understanding of the system's security and emergency preparedness capability can be documented in a memorandum, minutes from team meetings, or in a checklist, like the one provided in Table 6.

4.3.1 Note on Use

The checklist has been prepared to summarize issues for consideration by transportation personnel in reviewing the security and emergency preparedness of their current operations. Its objective is to help each system identify its current baseline regarding security and emergency preparedness activities. This checklist is generic and must be tailored by the system to its particular operation, facilities, personnel, and assessment of need. To support tailoring, this checklist provides four check boxes for responding to questions.

- ⇒ YES indicates the system performs the activity.

⇒ NO indicates the system does not perform the activity, but perhaps should consider it.
⇒ N/A indicates the activity is not applicable to the operation, size, mode of service, or management of the system.
⇒ COMMENT indicates that the transportation system has made an observation or finding regarding that specific activity. Comments should be attached to the checklist using additional sheets of paper.

A detailed worksheet is located in Appendix D that provides additional information to determine the applicability of a particular checklist item to a system's operation.

Table 6: Summary Findings – Capabilities Assessment

Section 1: Security Awareness & Threat Management
1. Does your system check the Homeland Security Advisory Threat Condition (http://www.whitehouse.gov/homeland/)? ☐ Yes ☐ No ☐ N/A ☐ Comment
2. Has your system performed a Terrorism Vulnerability Self-Assessment, as recommended by the Federal Bureau of Investigation (FBI), in cooperation with local law enforcement (see Appendix B)? ☐ Yes ☐ No ☐ N/A ☐ Comment
3. Does your system receive threat information and warnings from local law enforcement, state agencies, or other systems regarding local threat levels? ☐ Yes ☐ No ☐ N/A ☐ Comment
4. Do personnel at your system keep informed of major community activities and events? ☐ Yes ☐ No ☐ N/A ☐ Comment
5. Are personnel at your system aware of ongoing law enforcement concerns regarding specific communities or events that may be targeted for terrorist activity? ☐ Yes ☐ No ☐ N/A ☐ Comment
6. Have system personnel been trained to challenge people who do not appear to belong in restricted areas or who do not have the appropriate identification displayed? ☐ Yes ☐ No ☐ N/A ☐ Comment
7. Does the system have procedures in place for reporting these occurrences in a manner that supports appropriate evaluation and decision-making by supervisors and management? ☐ Yes ☐ No ☐ N/A ☐ Comment
8. Does the system have procedures in place for reporting these occurrences in a manner that supports appropriate evaluation and decision-making by supervisors and management? ☐ Yes ☐ No ☐ N/A ☐ Comment
9. Does your system have policies in place to ensure that security, operations or maintenance personnel routinely check unattended public or open areas, such as rest rooms, stairways, parking garages, and elevators for unusual, out-of-place, or abandoned items? ☐ Yes ☐ No ☐ N/A ☐ Comment

Table 6: Summary Findings – Capabilities Assessment

10. Has the system trained personnel on recognizing and reporting unusual, out-of-place, or unattended objects?

☐ Yes ☐ No ☐ N/A ☐ Comment

11. Has your system reviewed its policies for managing these objects (i.e., identifying lost-and-found items and reporting suspicious objects to management for further review)?

☐ Yes ☐ No ☐ N/A ☐ Comment

12. Has your system incorporated security checks into policies for pre-trip inspections, vehicle cleaning, and vehicle fueling?

☐ Yes ☐ No ☐ N/A ☐ Comment

13. Have appropriate personnel at your system received and reviewed security and emergency management materials from the FTA?

☐ Yes ☐ No ☐ N/A ☐ Comment

14. Have appropriate personnel at your system received security or emergency management training from the FTA or another source?

☐ Yes ☐ No ☐ N/A ☐ Comment

Section 2: Security & Preparedness Planning

1. Has management accepted responsibility for security vulnerabilities during the design, engineering, construction, testing, start-up, and operation of the transportation system related to rehabilitations, extensions, and modifications?

☐ Yes ☐ No ☐ N/A ☐ Comment

2. Has Executive Management endorsed a policy to ensure that security vulnerabilities are identified, communicated, and resolved through a process promoting accountability for decisions made?

☐ Yes ☐ No ☐ N/A ☐ Comment

3. Does your system have clear and unambiguous lines of authority and responsibility for ensuring that security is addressed at all organizational levels within the operation (including contractors)?

☐ Yes ☐ No ☐ N/A ☐ Comment

4. Does your system have access to personnel with security management experience, knowledge, skills, and abilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

5. Does your system ensure that resources are effectively allocated to address security considerations?

☐ Yes ☐ No ☐ N/A ☐ Comment

6. Is the protection of passengers, employees, contractors, emergency responders, and the general public a priority whenever activities are planned and performed at the system?

☐ Yes ☐ No ☐ N/A ☐ Comment

7. Wherever possible, does your system guide design, engineering, and procurement activity with an agreed-upon set of security standards and requirements (including design criteria manuals, vehicle specifications, and contracting guidelines)?

☐ Yes ☐ No ☐ N/A ☐ Comment

8. Does your system routinely evaluate its capabilities to provide adequate assurance that the public and employees are protected from adverse consequences?

☐ Yes ☐ No ☐ N/A ☐ Comment

9. Has your system committed to developing security mitigation measures to prevent and

Table 6: Summary Findings – Capabilities Assessment

manage security vulnerabilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

10. Has your system appropriately documented its security measures in plans, procedures, training, and in project requirements, specifications, and contracts?

☐ Yes ☐ No ☐ N/A ☐ Comment

11. Does your system have a formal system security program documented in a system security program plan?

☐ Yes ☐ No ☐ N/A ☐ Comment

12. If yes, is the security plan current, reflecting current security operations and system configuration?

☐ Yes ☐ No ☐ N/A ☐ Comment

13. If no, does your system have plans in place to develop a security plan?

☐ Yes ☐ No ☐ N/A ☐ Comment

14. If no, prepare a brief list of all activities performed at your system that address security and preparedness concerns. (Include procedures for handling difficult people, workplace violence program, bomb threat management plan, procedures for identifying and reporting unusual occurrences, facility and vehicle evacuation and search procedures, coordination with local law enforcement, etc.)

☐ Yes ☐ No ☐ N/A ☐ Comment

Section 3: Security & Preparedness Management

1. Does your system have a police or security department to implement the security program?

☐ Yes ☐ No ☐ N/A ☐ Comment

If yes, please describe organization and existing capabilities of this department?

Attach description.

2. If no, does your system use adjunct security personnel to support security for administrative and non-revenue facilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

1. If no, describe the activities performed by your system to coordinate security response with local law enforcement? Include MOUs and any reports that may be received regarding the occurrence of crime at the transportation system.

☐ Yes ☐ No ☐ N/A ☐ Comment

Attach description.

4. Does your system have specific plans for managing bomb threats, threats regarding the release chemical, biological or radioactive materials, and/or threats against specific individuals?

☐ Yes ☐ No ☐ N/A ☐ Comment

5. Does your system have specific plans to guide facility and vehicle evacuations and searches for unusual, out-of-place, or unattended packages?

☐ Yes ☐ No ☐ N/A ☐ Comment

6. Does your system coordinate with local law enforcement to ensure timely and effective response to identify a potential explosive device or other hazardous material?

☐ Yes ☐ No ☐ N/A ☐ Comment

7. Does your system coordinate its security activities with neighborhood watch programs,

Table 6: Summary Findings – Capabilities Assessment

other community and business security programs, and school safety programs to support integrated and coordinated approaches to shared problems?

☐ Yes ☐ No ☐ N/A ☐ Comment

8. Has your system reviewed its procedures for managing mail and deliveries to assess security considerations?

☐ Yes ☐ No ☐ N/A ☐ Comment

9. Are your employees trained to recognize and report threatening behavior and those activities that could be associated with the placement of an explosive device or the potential release of a hostile agent into the transportation environment?

☐ Yes ☐ No ☐ N/A ☐ Comment

10. Do your employees understand their roles and responsibilities for protecting passengers, other employees, and the general public from security threats?

☐ Yes ☐ No ☐ N/A ☐ Comment

11. Have your employees received security-related training for dispute resolution and conflict management?

☐ Yes ☐ No ☐ N/A ☐ Comment

12. Has your system developed a program to address workplace violence?

☐ Yes ☐ No ☐ N/A ☐ Comment

13. Has your system provided local law enforcement and public safety organizations with transportation awareness training?

☐ Yes ☐ No ☐ N/A ☐ Comment

Section 4: Threat & Vulnerability Assessment

1. Has your system ever conducted a formal threat and vulnerability assessment?

☐ Yes ☐ No ☐ N/A ☐ Comment

2. Does your system have a current listing of its critical assets?

☐ Yes ☐ No ☐ N/A ☐ Comment

3. Does your system have a current description of physical and procedural security measures in place to protect these assets?

4. Does your system have a current assessment of specific threats to its operation?

☐ Yes ☐ No ☐ N/A ☐ Comment

5. Has your system identified worst-case scenarios regarding security vulnerabilities to acts of terrorism and extreme violence?

☐ Yes ☐ No ☐ N/A ☐ Comment

6. Has your system ever assessed its capabilities to identify and manage those activities that may indicate the release of a hostile agent in the transportation environment or placement of an explosive device?

☐ Yes ☐ No ☐ N/A ☐ Comment

7. Does your system have a prioritized listing of current security vulnerabilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

8. Does your system have a current program in place to implement security measures that address these vulnerabilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

Section 5: Physical Security

Table 6: Summary Findings – Capabilities Assessment

1. Does your system provide access control systems to protect administrative and non-revenue facilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

2. Does your system require that employees wear badges or other forms of identification?

☐ Yes ☐ No ☐ N/A ☐ Comment

3. Does your system have procedures in place to verify access authorization for visitors, contractors, and delivery personnel?

☐ Yes ☐ No ☐ N/A ☐ Comment

4. Does your system have procedures to log non-routine entries (e.g., visitors, personnel during off-shift, and personnel not normally assigned) to administrative and non-revenue facilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

5. Does your system have procedures to verify the identity of a visitor before issuing a badge, pass, or credential?

☐ Yes ☐ No ☐ N/A ☐ Comment

6. Does your system have procedures to verify the access authorization of vehicles before they can be parked within 50 feet of administrative and non-revenue facilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

7. Does your system have inventory control procedures for access badges, uniforms, and equipment?

☐ Yes ☐ No ☐ N/A ☐ Comment

8. Does your system have procedures for reporting stolen badges, uniforms, or equipment?

☐ Yes ☐ No ☐ N/A ☐ Comment

9. Does your system issue advisories or bulletins regarding potential security threats?

☐ Yes ☐ No ☐ N/A ☐ Comment

10. Does your system screen personnel and packages before providing access to secure facilities (control center, revenue collection facilities, etc.)?

☐ Yes ☐ No ☐ N/A ☐ Comment

11. Does your system authorize the search of hand-carried items or packages entering or leaving a security area?

☐ Yes ☐ No ☐ N/A ☐ Comment

12. Does your system provide perimeter controls for administrative and non-revenue facilities, including fencing, gates, motion-detected lighting systems, etc.?

☐ Yes ☐ No ☐ N/A ☐ Comment

13. Does your system routinely patrol and/or inspect exterior security area perimeter barriers to verify integrity and detect unauthorized objects or conditions (e.g., excessive soil erosion under fence)?

☐ Yes ☐ No ☐ N/A ☐ Comment

14. Does your system follow pre-determined procedures to lock down and open administrative, non-revenue and passenger facilities each day?

☐ Yes ☐ No ☐ N/A ☐ Comment

15. Does your system have procedures to control the issuance of keys and combinations to locks and control panels?

☐ Yes ☐ No ☐ N/A ☐ Comment

16. Are your administrative and non-revenue facilities protected with intrusion detection alarm systems?

Table 6: Summary Findings – Capabilities Assessment

☐ Yes ☐ No ☐ N/A ☐ Comment

17. Are your administrative and non-revenue facilities covered by CCTV?

☐ Yes ☐ No ☐ N/A ☐ Comment

18. Identify other security systems in place to protect your system's administrative and non-revenue facilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

19. Does your system use security technology to support monitoring and management of passengers in stations, terminals, and on vehicles (examples include CCTV, emergency telephones, designated passenger waiting areas; emergency alarms on buses, alarms and intercoms on trains, and public address systems in stations)?

☐ Yes ☐ No ☐ N/A ☐ Comment

20. If yes, please describe this technology.

Attach description.

21. Has your system conducted blast hardening or mitigation as part of the station and administrative facility design or renovation process?

☐ Yes ☐ No ☐ N/A ☐ Comment

22. Do vehicle barriers, blast barriers, or other perimeter controls that limit or deny direct vehicle access to critical assets protect your facilities?

☐ Yes ☐ No ☐ N/A ☐ Comment

23. Please describe the security technology used by your police or security department (if applicable).

Attach description.

Section 6: Emergency Response Capabilities

1. Does your system have an emergency plan?

☐ Yes ☐ No ☐ N/A ☐ Comment

2. Does your system have emergency operating procedures?

☐ Yes ☐ No ☐ N/A ☐ Comment

3. Does your system have an incident response plan for terrorism, as an appendix to the emergency plan or as a separate plan?

☐ Yes ☐ No ☐ N/A ☐ Comment

4. Does your system coordinate with local public safety organizations on the development, implementation, and review of the emergency plan and procedures?

☐ Yes ☐ No ☐ N/A ☐ Comment

5. Does your emergency plan specify use of the incident command system?

☐ Yes ☐ No ☐ N/A ☐ Comment

6. Have your employees been trained in the emergency plan and procedures?

☐ Yes ☐ No ☐ N/A ☐ Comment

7. Does your system conduct routine simulation drills, tabletop exercises, and refresher training?

☐ Yes ☐ No ☐ N/A ☐ Comment

8. Does your system coordinate its drilling and training for emergency response with local public safety organizations?

☐ Yes ☐ No ☐ N/A ☐ Comment

9. Does your system conduct briefings of after-action reports to assess performance during the simulation drill or exercise and identify areas in need of improvement?

Table 6: Summary Findings – Capabilities Assessment

☐ Yes	☐ No	☐ N/A	☐ Comment
10. Have members of your system participated in domestic preparedness training programs sponsored by the federal government (FEMA, FBI, DOD, etc.)?			
☐ Yes	☐ No	☐ N/A	☐ Comment
11. Has your system participated in capabilities assessment readiness (CAR) exercise programs supported by the local EMA?			
☐ Yes	☐ No	☐ N/A	☐ Comment

Section 7: Previous Experience			
1. Has your system experienced an emergency in the last 12 months?			
☐ Yes	☐ No	☐ N/A	☐ Comment
2. If yes, were you satisfied with the system's level of response?			
☐ Yes	☐ No	☐ N/A	☐ Comment
3. Has your system received a bomb threat in the last 12 months?			
☐ Yes	☐ No	☐ N/A	☐ Comment
4. Has your system evacuated its facilities in the last 12 months as the result of a bomb threat?			
☐ Yes	☐ No	☐ N/A	☐ Comment
5. Has your system conducted a physical search of a facility in response to a bomb threat?			
☐ Yes	☐ No	☐ N/A	☐ Comment

5 Reducing Threat and Vulnerability

Threat and vulnerability assessment provides an analytical process to consider the likelihood that a specific threat will endanger the system. Using the results of the capabilities assessment (discussed in Section 4 of this Guide), the threat and vulnerability analysis can also identify activities to be performed to reduce risk of an attack and mitigate its consequences.

These assessments typically use a combination of quantitative and qualitative techniques to identify security requirements, including historical analysis of past events, intelligence assessments, physical surveys, and expert evaluation. When the risk of hostile acts is greater, these analysis methods may draw more heavily upon information from intelligence and law enforcement agencies regarding the capabilities and intentions of the aggressors. For example, recent experience with anthrax-tainted mail resulted in nation-wide dissemination of procedural changes for managing packages and letters, reflecting intelligence from the FBI and recommended practice from the Centers for Disease Control (CDC).

Effective threat and vulnerability assessments typically include five elements:

⇒ asset analysis;
⇒ target or threat identification;
⇒ vulnerability assessment;
⇒ consequence analysis (scenarios); and
⇒ countermeasure recommendation.

These elements and their inter-relationships are presented graphically in Figure 15.

5.1 Asset Analysis

In security terms, assets are broadly defined as people, information, and property. In public transportation, the people include passengers, employees, visitors, contractors, vendors, nearby community members, and others who come into contact with system. Information includes operating and maintenance procedures, vehicle control and power systems, employee information, computer network configurations and passwords, and other proprietary information. The range of property that a security effort might wish to protect is presented in Table 7.

In reviewing assets, the transportation system should prioritize which among them has the greatest consequences for people and the ability of the system to sustain service. These assets may require higher or special protection from an attack. In making this determination, the system may wish to consider:

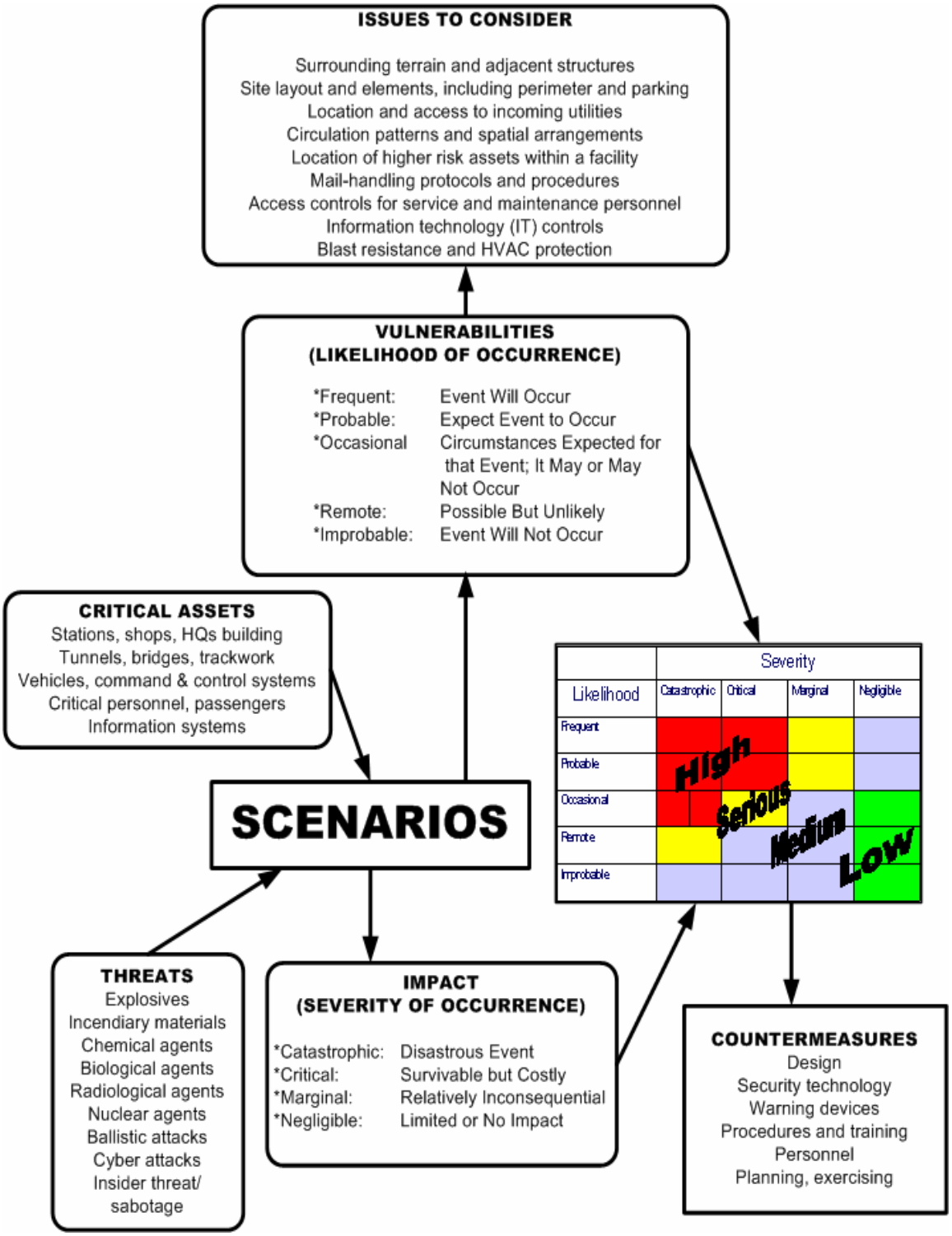


Figure 15: Threat and Vulnerability Process

Table 7: Transportation Assets

⇒ Passenger stations, stops and shelters ⇒ Tenant facilities in passenger stations ⇒ Passenger vehicles ⇒ Structures (underground, at-grade and elevated) ⇒ Passenger parking lots ⇒ Vehicle control systems ⇒ Communications systems ⇒ Heavy maintenance facilities ⇒ Service and inspection facilities ⇒ Maintenance vehicles and equipment ⇒ Backup power systems ⇒ Fuel farms and generators ⇒ Alternative fuel storage facilities	⇒ Switches, signals and interlockings ⇒ Grade crossings and automatic warning devices (gates, bells, flashers, and signs) ⇒ Electrification Systems (3rd rail, overhead catenaries) ⇒ Operations control centers ⇒ Revenue collection facilities ⇒ Vehicle storage facilities ⇒ Wayside support and maintenance facilities ⇒ Ancillary facilities and storage ⇒ Employee parking lots ⇒ Administrative facilities ⇒ Transportation police/security facilities and communications systems

⇒ the value of the asset, including current and replacement value;
⇒ the value of the asset to a potential adversary;
⇒ where the asset is located;
⇒ how, when, and by whom an asset is accessed and used; and
⇒ what is the impact, if these assets are lost, on passengers, employees, public safety organizations, the general public and the public transportation operation?

Based on current intelligence, the FBI urges transportation systems serving communities with the following characteristics to consider themselves at a higher level of risk:

⇒ availability of targets with symbolic meaning for the US government or the national culture and way of life;
⇒ availability of targets with precursor elements for major destruction (chemical, nuclear, or radiological material);
⇒ availability of targets whose destruction would provide the potential terrorist element (PTE) with visibility and prestige;
⇒ availability of targets with the potential to significantly impact not only a single community, but also a state and the nation;
⇒ availability of high-value targets (e.g., high replacement costs, high commercial impacts of delay and destruction, high loss on U.S. economy);
⇒ availability of major targets that provide relative ease of access (for ingress and egress with equipment and personnel required for attack); and
⇒ availability of targets that would produce mass casualties (in excess of 500 persons).

In a cooperative partnership with state and local law enforcement, the FBI has requested completion of vulnerability self-assessments, emphasizing the above characteristics for each community. Appendix B contains the full vulnerability

self-assessment supplied by the FBI, which is also included on the Guide CD-ROM.

Using this worksheet, transportation systems can identify which assets in their operations would produce the greatest losses to the system and the community. Based on the results of this assessment, the transportation organization may wish to share a copy with local law enforcement or to include a representative from law enforcement in the assessment process, to support their understanding of the transportation function and role in the community.

5.2 Threats, Vulnerabilities, and Consequences

Information regarding threats, vulnerabilities, and consequences is presented below.

5.2.1 Threats

A threat is any action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services. System facility threats include a number of hostile actions that can be perpetrated by criminals, disgruntled employees, terrorists, and others.

Threat analysis defines the level or degree of the threats against a facility by evaluating the intent, motivation, and possible tactics of those who may carry them out. The process involves gathering historical data about hostile events and evaluating which information is relevant in assessing the threats against the facility. Some of the questions to be answered in a threat analysis are displayed below.

⇒ What factors about the system invite potential hostility?
⇒ How conspicuous is the transportation facility or vehicle?
⇒ What political event(s) may generate new hostilities?
⇒ Have facilities like this been targets in the past?

Possible methods of carrying out hostile actions in the transportation environment are depicted in Table 8. Historical examples are provided for reference and consideration, as well as the types of weapons typically used in these attacks.

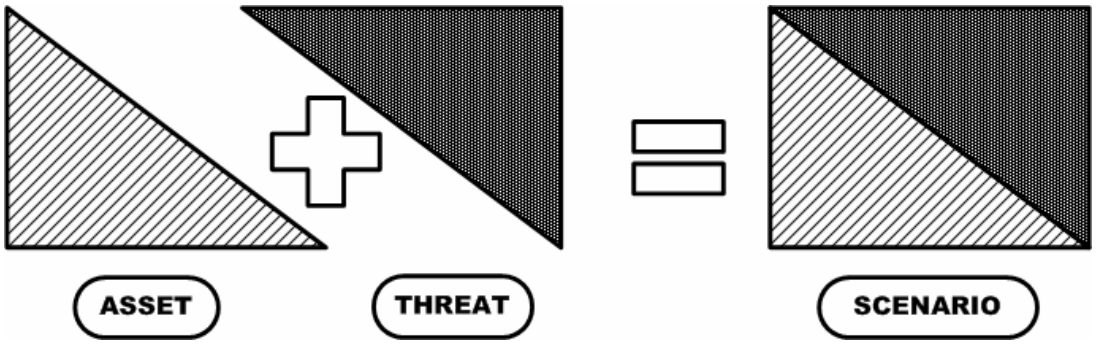
5.2.2 Vulnerabilities

A vulnerability is anything that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a facility, in its technological systems, and in the way a facility is operated (e.g., security procedures and practices or administrative and management controls). Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.

Table 8: Threats from Terrorism

Type of Attack	Historical Example	Type of Weapons
Explosive and Incendiary Devices	1995 GIA bombing of Paris Metro	Planted Devices
	HAMAS suicide bombs on Israeli buses (on-going)	Suicide Bombs
	1998 bombings of U.S. embassies in Tanzania and Kenya	Vehicle Bomb
	2001 World Trade Center; 1990s abortion clinic bombings in GA; 1995 Oklahoma City Bombing	Proximity Bombs; Incendiary Deices; Secondary Devices
Exterior Attacks	2001 militant assaults on Indian-held mosques in Kashmir	Rocks and Clubs; Improvised Devices; Molotov cocktails
Stand-off Attacks	Tamil Tiger's July 2001 mortar attack & bombing of Sri Lanka's National Airport	Anti-tank rockets; Mortars
Ballistics Attacks	Long Island Railroad Shootings; Columbine High School	Pistols; Handguns; Submachine guns; Shotguns
Networked/ Inside Access: - Forced Entry - Covert Entry - Insider Compromise - Visual Surveillance - Acoustic/ Electronic Surveillance	Amtrak *Sunset Limited* derailment 1996 Tupac Amaru Revolutionary Movement taking of Japanese Ambassador's resident and 500 guests in Peru (access through disguise as waiters at the party)	Hand, power and thermal tools; Explosives
		False credentials; Stolen uniforms and identification badges
		False pretenses, cell operations
		Binoculars; Photographic Devices
		Listening Devices; Electronic-emanation surveillance equip.
Cyber Attack	Code Red Worm (2002)	Worms, Viruses, Denial of Service Programs
Chemical, Biological, Radiological, & Nuclear (CBRN) Agent Release	1995 Aum Shinrikyo Sarin Gas Release in Tokyo Subway	Chemical, biological, or radiological or nuclear aerosolized

Vulnerabilities are commonly prioritized through the creation of scenarios that pair identified assets and threats. Using these scenarios, transportation agencies can evaluate the effectiveness of their current policies, procedures, and physical protection capabilities to address consequences.



5.2.3 Scenario Analysis

Scenario analysis requires an interpretive methodology that encourages role-playing by transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system. By matching threats to critical assets, transportation personnel can identify the capabilities required to support specific types of attacks. This activity promotes awareness and highlights those activities that can be preformed to recognize, prevent, and mitigate the consequences of attacks.

The FBI recommends that transportation systems focus on the top 10% of identified critical assets (at a minimum). Using these assets, transportation personnel should investigate the most likely threats, considering the range of attack objectives and methods that may be used (such as disruption of traffic, destruction of bridge or roadway, airborne contamination, hazardous materials accident, and threat or attack with explosives intended to disrupt or destroy). The system should also consider the range of perpetrators, such as political terrorists, radicals, right-wing extremists, disgruntled employees, disturbed copycats, and others.

When conducting the scenario analysis, the system may choose to create chronological scenarios (event horizons) that emphasize the worst credible scenario as opposed to the worse case scenario. Experienced transportation personnel, who have participated in transportation war-gaming, recommend the investigation of worst-case scenarios. Results from this analysis are far more likely to produce recommendations appropriate for the size and operation of the system. Based on this type of assessment, as indicated in Tables 9 and 10, the transportation system may determine certain scenarios as relevant to bus and rail service.

Table 9: Relevant Bus Scenarios

Bus Assets	Most Probable Threats
Bus stations and/or terminals	⇒ High-yield vehicle bomb near station ⇒ Lower-yield explosive device in station ⇒ Armed hijacking, hostage, or barricade situation in station ⇒ Chemical, biological, and nuclear release in station ⇒ Secondary explosive device directed at emergency responders
Bus vehicles	⇒ Explosives placed on or under bus ⇒ Improvised explosive device (pipe or fire bomb) on bus ⇒ Chemical, biological, or nuclear release on bus ⇒ Armed assault, hostage, or barricade situation on bus ⇒ Secondary explosive device directed at emergency responders
Fuel storage facilities	⇒ Explosives detonated in or near fuel facilities
Command Control Center	⇒ Physical or information attack on train control system ⇒ Physical or information attack dispatch system ⇒ Armed assault, hostage, or barricade situation ⇒ Explosive device near or in Center ⇒ Sabotage of train control system

Table 10: Relevant Rail Scenarios

Rail Assets	Most Probable Threats
Stations	⇒ High-yield vehicle bomb near stations ⇒ Lower-yield explosive device in station ⇒ Armed hijacking, hostage, or barricade situation in station ⇒ Chemical, biological, and nuclear release in station ⇒ Secondary explosive device directed at emergency responders
Track/signal	⇒ Explosive detonated on track ⇒ Chemical, biological, nuclear release on track ⇒ Signal and/or rail tampering
Rail cars	⇒ Explosives placed on or under rail car ⇒ Improvised explosive device (pipe/fire bomb) on rail car ⇒ Chemical, biological, nuclear release on rail car ⇒ Armed assault, hostage, or barricade situation on rail car ⇒ Secondary explosive device directed at emergency responders
Power substations	⇒ Explosive detonated in or near substation
Command Control Centers	⇒ Physical or information attack on train control system ⇒ Physical or information attack dispatch system ⇒ Armed assault, hostage, or barricade situation ⇒ Explosive device near or in Center ⇒ Sabotage of train control system

5.2.4 Consequences

For each scenario, the transportation system should attempt to identify the costs and impacts using a standard risk level matrix, which supports the organization of consequences into categories of high, serious, and low. Consequences are assessed both in terms of severity of impact and probability of loss for a given threat scenario, as presented in Figure 16.

	Vulnerability	Impact	
Very Easy	A	I	Loss of life
Relatively Easy	B	II	Serious injuries, major service impact, >$250k damage
Difficult	C	III	Minor injuries, minor service impact, <$250k damage
Very Difficult	D	IV	No injuries, no service impact
Too Difficult	E		

Criticality Matrix

	I	II	III	IV
A	H	H	S	S
B	H	H	S	L
C	H	S	L	L
D	S	L	L	L
E	S	L	L	L

- H = High
- S = Serious
- L = Low

Figure 16: Scenario Evaluation Criteria

Scenarios with vulnerabilities identified as high may require further investigation. Scenario-based analysis is not an exact science but rather an illustrative tool demonstrating potential consequences associated with low-probability to high-impact events. To determine the system's actual need for additional countermeasures, and to provide the rationale for allocating resources to these countermeasures, the system should use the scenarios to pinpoint the vulnerable elements of the critical assets and make evaluations concerning the adequacy of current levels of protection. Examples of vulnerabilities that may be identified from scenario-based analysis include the following:

⇒ accessibility of surrounding terrain and adjacent structures to unauthorized access (both human and vehicular);
⇒ site layout and elements, including perimeter and parking that discourage access control, support forced or covert entry, and support strategic placement of explosives for maximum damage;
⇒ location and access to incoming utilities (easy access for offenders);

- ⇒ building construction with respect to blast resistance (tendency toward progressive collapse, fragmentation, or no redundancy in load bearing);
- ⇒ sufficiency of lighting, locking controls, access controls, alarm systems, and venting systems to support facility control; and
- ⇒ information technology (IT) and network ease-of-penetration.

5.2.5 Prioritized Listing of Vulnerabilities

At the conclusion of the scenario-based analysis, the transportation system should have assembled a list of prioritized vulnerabilities for its top 10% critical assets. Typically, these vulnerabilities may be organized into the following categories:

- ⇒ lack of planning;
- ⇒ lack of coordination with local emergency responders;
- ⇒ lack of training and exercising; and
- ⇒ lack of physical security (access control, surveillance; blast mitigation, or chemical, biological, or radioactive agent protection).

These vulnerabilities should be documented in a confidential report or memorandum for the system's executive director.

5.2.6 Developing Countermeasures

Based on the results of the scenario analysis, the system can identify countermeasures to reduce vulnerabilities. Effective countermeasures typically integrate mutually supporting elements.

- ⇒ Physical protective measures designed to reduce system asset vulnerability to explosives, ballistics attacks, cyber attacks, and the release of chemical, biological, radiological, or nuclear (CBRN) agents.

- ⇒ Procedural security measures, including procedures to detect and mitigate an act of terrorism or extreme violence and those employed in response to an incident that does occur.

In identifying these measures, the system should be able to answer the following questions.

- ⇒ What different countermeasures are available to protect an asset?
- ⇒ What is the varying cost or effectiveness of alternative measures?

In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded.

5.2.7 Rings of Protection

As illustrated in Figure 17, security tends to emphasize rings of protection, meaning that the most important or most vulnerable assets should be placed in the center of concentric levels of increasingly stringent security measures. For example, a transportation system's control center should not be placed right next to the building's reception area, rather, it should be located deeper within the building so that, to reach the control center, an intruder would have to penetrate numerous rings of protection, such as a fence at the property line, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door to the control room.

Other prevention strategies involve cooperation with law enforcement agencies, security staff in other systems, and industry associations in order to share threat information. It is useful to know whether other transportation systems in an area have experienced threats, stolen uniforms or keys, or a particular type of criminal activity, in order to implement appropriate security measures. Table 11 provides a sample list of typical countermeasures from threat and vulnerability assessments.

In the assessment, the team may consider both passive and active strategies for identifying, managing, and resolving threats to the system's operation. Team members should provide appropriate expertise in both these strategies.

Passive strategies include all security and emergency response planning activity, outreach with local law enforcement, training, evacuation and business continuity and recovery plans, employee awareness, public information, and passenger training. Passive responses also include security design strategies, supported by crime prevention through environmental design (CPTED) and situational crime prevention (SCP) methods, such as landscaping, lighting, and physical barriers (planters or bollards).

Active strategies include security technology, such electronic access control, intrusion detection, closed circuit TV, digital recorders, emergency communications systems, and chemical agent or portable explosives detectors. Active systems also include personnel deployment. It is important to consider the entire lifecycle cost when evaluating security solutions. Technology options may require a substantial one-time investment, supported by fractional annual allocations for maintenance and vendor support contracts. Personnel solutions are generally more expensive. Figure 18 depicts active strategies in use on bus vehicles around the country.

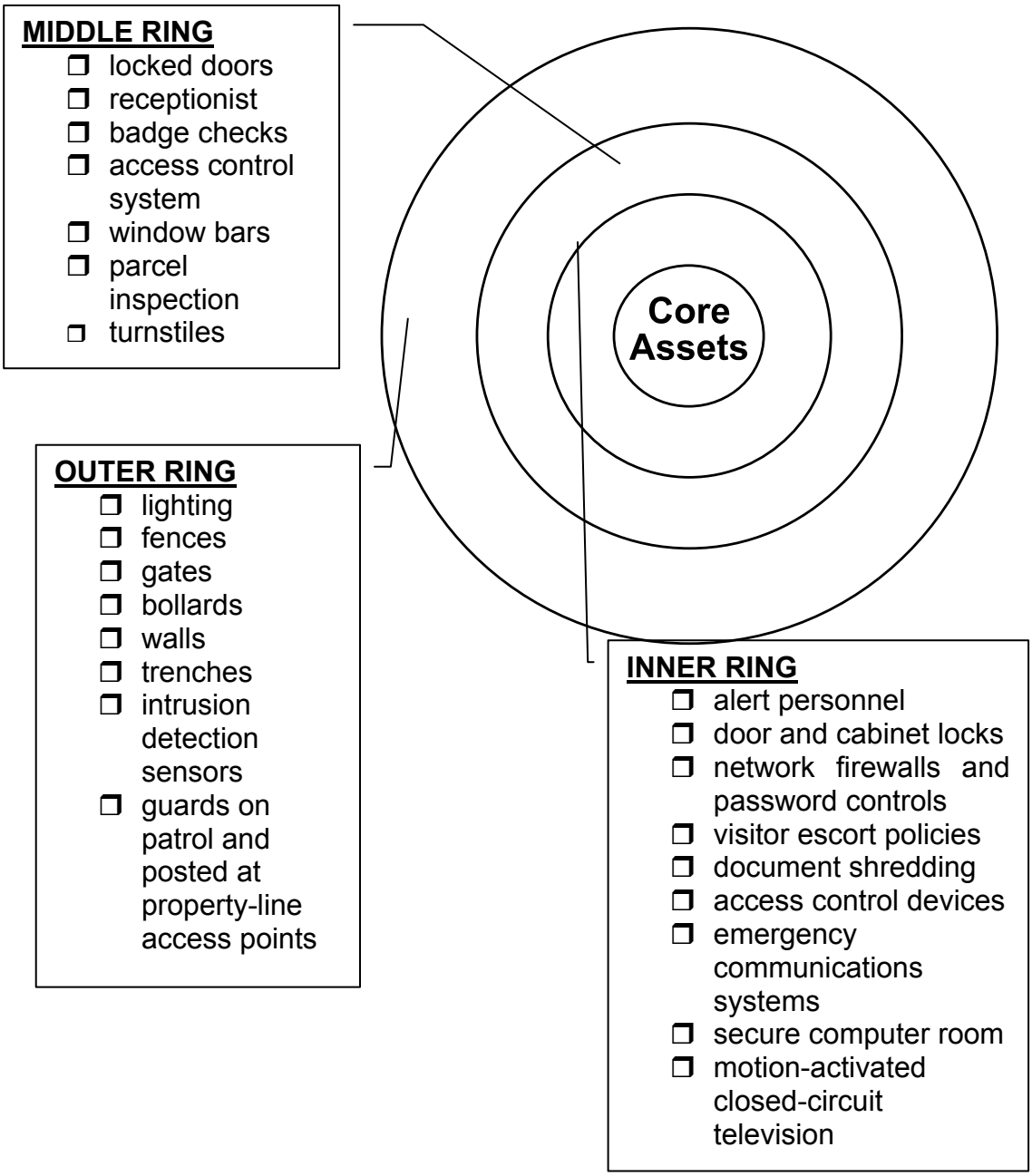


Figure 17: Sample Rings of Protection

Table 11: Public Transportation Countermeasures

COUNTERMEASURES	Planning	Coordination with Local Responders	Training and Exercising	Access Control	Surveillance	Blast Mitigation	WMD Agent Protection
				Physical Security			
Identifying Unusual or Out-of-Place Activity	X		X	X	X		X
Security Screening and Inspection Procedures	X	X	X		X	X	X
Enhancing Access Control for Stations/Vehicles	X	X	X	X	X	X	
Securing Perimeters for Non-revenue Areas	X			X	X		
Denying Access to Authorized-only Areas	X		X	X	X		
Securing Vulnerable Areas (target hardening)	X			X	X	X	
Removing Obstacles to Clear Line-of-Sight	X			X	X		
Protecting Parking Lots	X			X	X		
Enhanced Access Control for Control Center	X			X	X		
Securing Critical Functions and Back-ups	X			X	X		
Promoting Visibility of Uniformed Staff	X			X	X		
Removing Spaces that Permit Concealment	X			X	X		X
Reinforcing Natural Surveillance	X			X	X		
Procedures for Vehicle and Station Evacuations	X	X	X			X	X
Coordination with Community Planning Efforts	X	X	X				X
Backing up Critical Computer Systems	X		X				
Revising Lost-and-Found Policies	X		X				X
Securing Tunnels and Elevated Structures	X		X	X	X	X	X
Elevating/securing Fresh Air Intakes	X			X			X
Protecting Incoming Utilities	X			X	X	X	X
Establishing Mail-handling Procedures	X		X		X		X
Identifying Appropriate Personal Protective Equipment and Training	X	X	X				X
Preparing Response Folders and Notebooks for Facilities and Vehicles	X	X	X		X	X	X
Familiarization Training for Local Emergency Response Agencies	X	X					X
Planning for Scene Management and Emergency Response	X	X				X	X

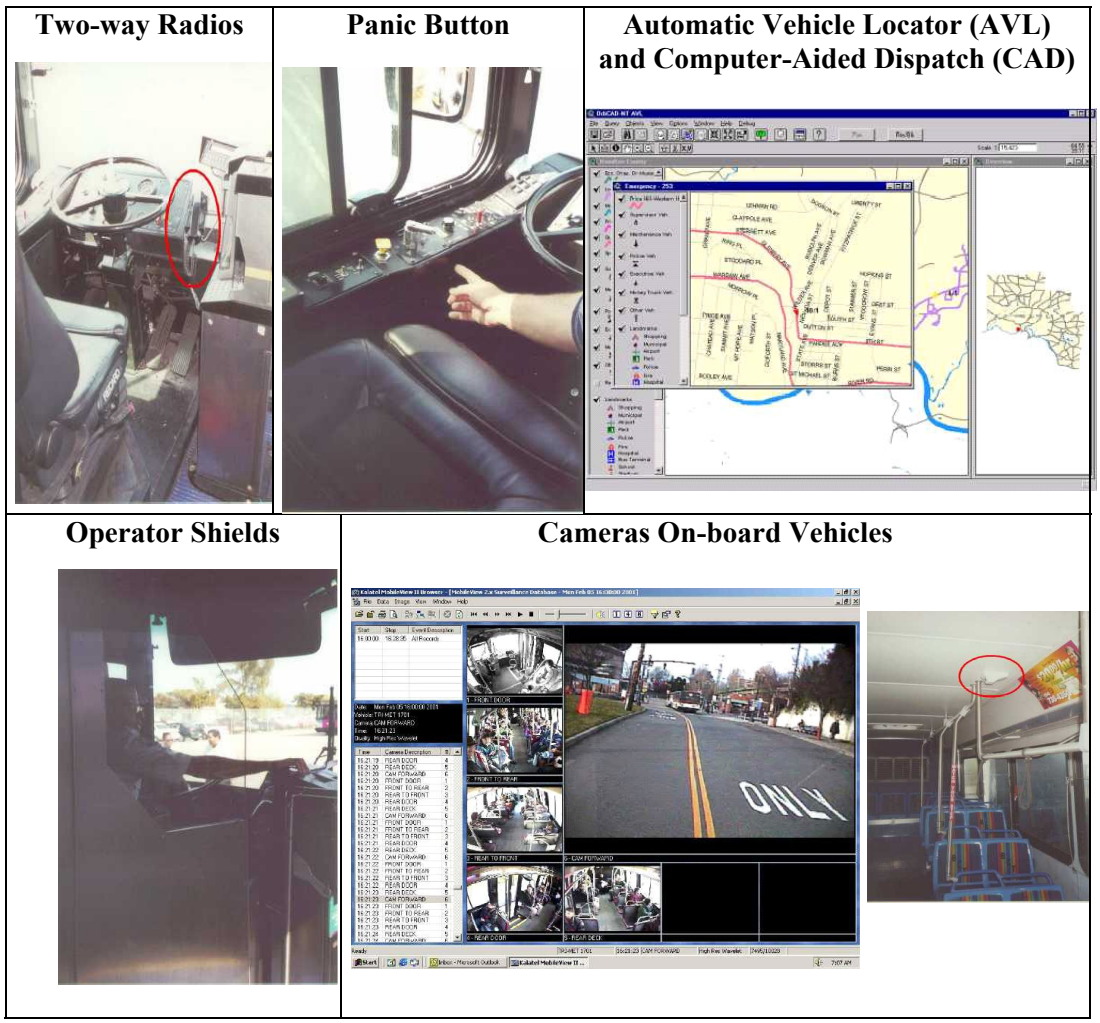


Figure 18: Active Security Strategies for Bus Vehicles

6 Procedures for New Threats

This section provides recommendations for procedures in the transportation industry to manage new and heightened threats. The four procedures discussed in this section are as follows:

⇒ sample bomb threat procedures;
⇒ managing hoaxes and unusual or out-of-place objects;
⇒ response to calls of reports suspecting a chemical agent release; and
⇒ release of sensitive information to the public.

6.1 Sample Bomb Threat Procedures

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

6.1.1 Threats by Phone

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

⇒ Stay calm, be courteous, and do not display fear.

⇒ Activate a telephone recording unit, if available.

⇒ Listen carefully during or immediately after the conversation. Take notes of the exact time the call was received, the exact words of the caller, and all details such as the sex of the caller, his/her accent or attitude, background noises, and motive. Use a bomb threat checklist to record the details of the call.

⇒ Explain consequences of an explosion. Advise the caller that the station, building or facility may be occupied and the explosion could result in death or serious injury to many innocent people.

⇒ Keep the caller talking. The more the caller says, the more helpful the information may be during the threat evaluation phase. If the caller does not indicate the location of the bomb or the time of detonation, ask him/her what time it is to go off and where it is located.

⇒ After the phone call, notify the appropriate supervisor. Do not discuss the call with anyone else unless authorized to do so or required by law. Follow proper procedures to "tag" call for further police investigation.

6.1.2 Threats by Mail

The following are instructions on how to handle bomb threats received by mail. The most likely recipients are mailroom personnel and administrative personnel.

⇒ Place all papers and envelopes associated with the threat in a bag or large envelope (clear plastic bag if possible). Pick up any bomb threat note only by the edge.

⇒ Do not handle the written threat any more than absolutely necessary.

⇒ Do not allow anyone else to touch the note unless specifically authorized by a security representative or senior management.

6.1.3 Manager's Responsibility

In the case of a bomb threat, the appropriate manager should assess the seriousness of the threat using the following bomb threat assessment and bomb threat response guidelines. He/she should also, if appropriate, notify law enforcement authorities.

BOMB THREAT ASSESSMENT	
Is the threat credible? Consider: ⇒ time of day and day of week; ⇒ mode, telephone or mail; ⇒ identity of caller, male/female, young/old, drunk, foul language, disgruntled employee or patron; ⇒ specificity of the threat, time, location, type of explosive device; and ⇒ possibility of access to allow placing of the device.	Does the threat contain positive target identifications (PTIs)? Did the caller identify: ⇒ time the bomb is to detonate; ⇒ target to be destroyed; ⇒ bomb's construction, shape, or description; ⇒ bomb's location; or ⇒ bomb threat response.

6.1.4 Executing the Response

⇒ Use a public service address announcement, telephone cascade, messenger, or other local notification plan.

⇒ Determine who is to search and in what area. In general, employees should search their own area to determine if there are any suspicious objects. Those who are most familiar with the common areas should search them. All search activity should be predetermined and voluntary.

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

⇒ Notify public law enforcement and emergency services as appropriate; notify immediately if an unusual or out-of-place object is found.

⇒ If appropriate, determine who is to be evacuated and to what location.

⇒ If evacuation is ordered before a search is done, determine for how long. Consider available options if the weather is inclement. Consider possible effect on operations if evacuation occurs at or near a shift change.

⇒ Ensure that procedures are in place to account for all persons ordered to evacuate and determine that they have in fact evacuated and there is an orderly shutdown of operations. Be sure to evaluate evacuation site for secondary devices.

⇒ Coordinate with local authorities to determine if the area needs to be searched and who will determine that operations can resume and people can return to their workstations.

6.1.5 Search Plans

A predetermined search should be organized. It is not effective to delegate the search to the police alone because they are unfamiliar with

the area and do not know which objects in the facility would look unusual or out of place. *The employees assisting in this search should be pre-designated volunteers and have had training in search techniques*.

The most effective search is possible when all employees are calmly told about the bomb threat and the reason for the search and are then asked to check their familiar areas for suspicious objects. Teams should be organized to search common areas. A search team leader should be designated and a notification protocol developed to report search results to the facilities manager. A plan should be developed to designate who is responsible for searching a specific area. For example, security personnel may search restrooms and outside areas, while maintenance staff may search LAN and electrical rooms.

The objective of the search activity is to search for and report unusual or out-of-place objects. There are several points to be stressed within search plans.

⇒ The search should be systematic (divide the facility into search areas), it should be thorough, and it should be done calmly. System personnel should also search on a voluntary basis. Identify the areas that are most accessible to outsiders and the areas that are most vulnerable. Search these first.

⇒ When searching a room, the room should first be searched from floor to waist height, then from waist height to eye level, and finally from eye level to ceiling. If the room has a false ceiling, the false ceiling should also be inspected.

⇒ No one should move, touch, or jar any unusual or out-of-place object or anything attached to it. The removal or disarming of a bomb must be left to law enforcement professionals.

6.1.5.1 No Bomb Found

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

6.1.5.2 Unusual or Out-of-Place Object Found

If an unusual or out-of-place object is found, the search team coordinator and the station manager should do the following.

⇒ Stress again to personnel not to touch or move the object.

⇒ Evacuate personnel from the surrounding area.

⇒ Prevent re-entering of the evacuated area.

⇒ Inform the police to take charge of getting the object deactivated or removed.

⇒ After the object has been removed, finish searching to ensure that no other bombs have been placed.

6.1.5.3 After-Action Plan

An after-action report, including incorporation of lessons learned, should be prepared immediately after resolution of the event. A formal debriefing of the event should occur with key management personnel.

6.2 Managing Hoaxes and Unusual or Out-of-place Objects

Figure 19 presents the scope of possible events that may occur on transportation property and in the community served by the system. These events range from threats and hoaxes to extended campaigns involving multiple attacks.

Analysis from the FBI indicates that the vast majority of threats and reported suspicious materials and packages will be revealed as common substances, lost or misplaced items, or normal occurrences in the transportation environment (train dust, cleanser residue, etc.). However, each of these events must be approached as a potential incident. Transportation personnel have a several possible actions available to them when responding to hoaxes and threats. Above all, the transportation system should invest in training personnel on the appropriate actions to take in these situations.

Safe investigation of reports and threats, proficient incident size-up, and effective communications and supervision will not only enhance the system's ability to recognize and manage an actual attack, but will also build confidence and provide an in-the-field training program. Debriefing of major threat report responses will further teach employees to proceed in a manner that best protects them, their fellow workers, and the system's passengers, facilities, and vehicles.

Transportation personnel should understand that, according to the FBI, hoaxes and threats should be expected to continue, and perhaps even escalate in frequency. The following guidelines may provide transportation personnel with useful advice when developing their programs, procedures, training, and exercise schedules.

⇒ Managing an actual hoax event should not be the first time a transportation employee is considering what should be done. Even obvious hoaxes relating to chemical, biological, radiological, and nuclear (CBRN) incidents have the potential to cause panic and generate negative publicity. These events require a much different response than bomb-threats, and only training, exercise, and technology can provide the necessary knowledge and awareness. Transportation systems should have plans and procedures in place for managing these events, so that employees will not be taken by surprise.

⇒ These events often take the form of written and phone threats; suspicious packages with signs and notes; suspicious powders and liquids left on turnstiles and public transportation vehicles, on station floors or in trash cans or restrooms; abandoned spray canisters, gloves, or masks; and the use of mace and machine oil to replicate chemical and biological agent characteristics.

⇒ Whenever possible, transportation personnel should remain sensitive to the reality that hoaxes deplete limited community resources and, in extreme periods, challenge the capabilities of local responders to provide basic services. Do not call local responders or hazardous materials units as a default position.

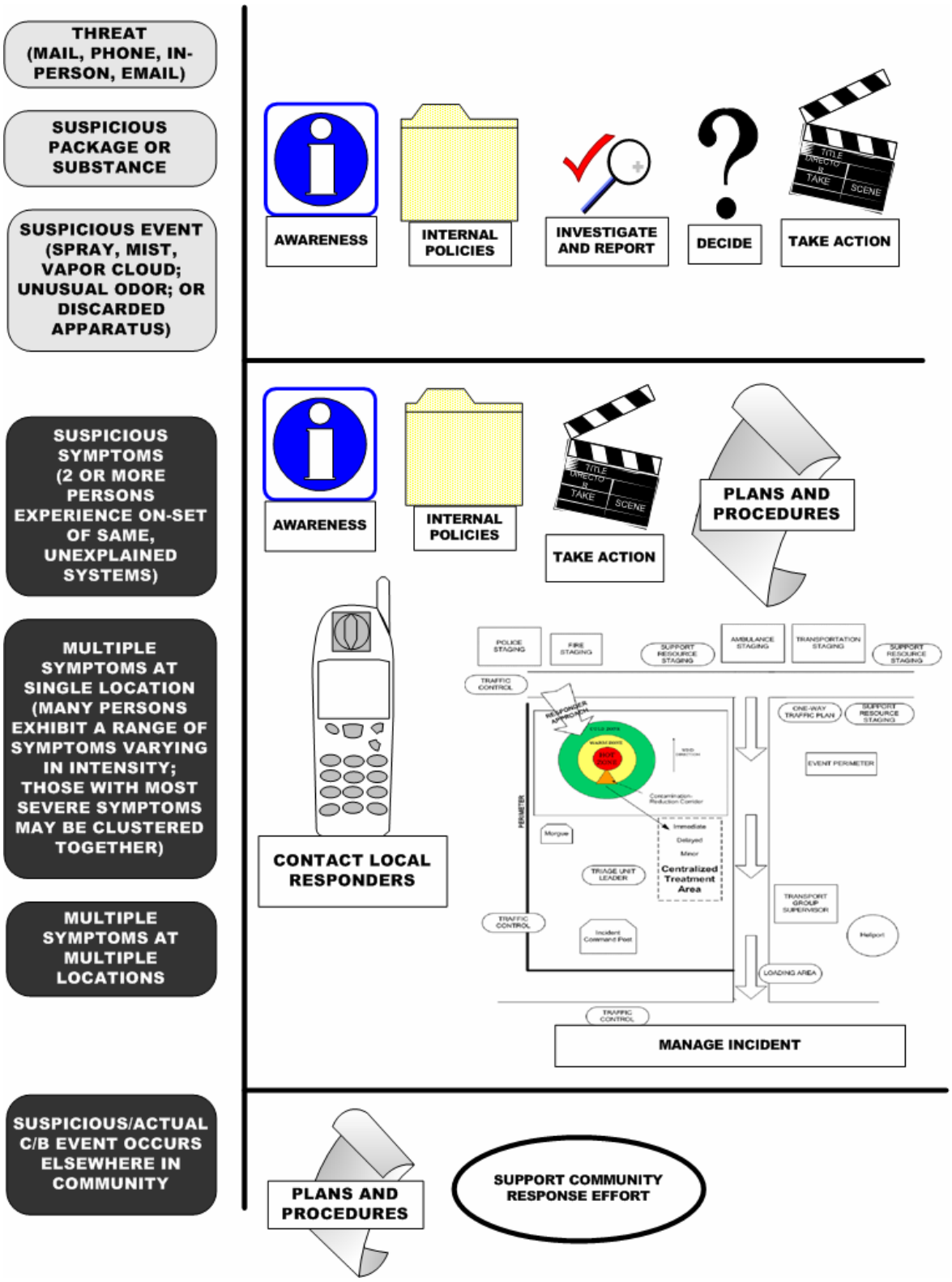


Figure 19: Response to Chemical and Biological Threats

⇒ Develop procedures for taking threat calls and reviewing suspicious letters and packages received in the mail (building on the bomb threat procedures outlined above).

⇒ Transportation employees and the riding public will be the source of most reported suspicious substances and packages. In managing these reports, transportation personnel will be expected to:

- receive news of a suspicious substance or package in a calm and reassuring manner; investigate the report using safe practices and from a safe vantage point; coordinate with transportation supervisory and dispatch personnel regarding appropriate action, maintenance clean-up or collection; hazardous materials clean-up; notification of local responders; notification of local hazardous materials response unit; evacuation; or other resolution;
- have equipment pre-staged to cordon off areas and to collect the names of potentially affected passengers and personnel;
- maintain a strict posture regarding investigation and prosecution of perpetrators of hoaxes and threats (the USA PATRIOT ACT makes special provisions for threats against public transportation, dramatically increasing the seriousness of this activity and its legal consequences);
- have and use internal procedures for managing hoaxes and threats, and distinguish escalating patterns of activity that may portent actual attacks; and
- coordinate closely with local, state, and federal law

USA PATRIOT ACT

The Act outlaws terrorist attacks and other actions of violence against mass transportation systems. Offenders may be imprisoned for life or any term of years, if the conveyance is occupied at the time of the offense, or imprisoned for not more than twenty years in other cases, section 801. Under its provisions, it is a crime to willfully:

- wreck, derail, burn, or disable mass transit;
- place a biological agent or destructive device on mass transit recklessly or with the intent to endanger;
- burn or place a biological agent or destructive device in or near a mass transit facility knowing a conveyance is likely to be disabled;
- impair a mass transit signal system;
- interfere with a mass transit dispatcher, operator, or maintenance personnel in the performance of their duties recklessly or with the intent to endanger;
- act with the intent to kill or seriously injure someone on mass transit property;
- convey a false alarm concerning violations of the section;
- attempt to violate the section;
- threaten or conspire to violate the section when the violation involves interstate travel, communication, or transportation of materials or that involves a carrier engaged in or affecting interstate or foreign commerce, 18 U.S.C. 1993.

enforcement officials to ensure that they remain in the loop regarding both emergency response planning and the identification of groups or individuals who are both motivated and capable of employing chemical or biological agents against civilians.

⇒ Both transportation and local response must have the capability to quickly and accurately determine the legitimacy of threats in order to dispel panic.

⇒ Hoaxes must be treated as actual events until proven otherwise, thus demanding the coordinated response of police, fire, and public health officials.

⇒ The incident command system (ICS) should to be utilized in handling hoax events. Without properly defined command structures in the highly stressful, emotional, and confusing scenario of a CBRN scare, conflicting orders can lead to a rapid breakdown in procedure.

⇒ Hoaxes require a response by many local agencies, and often various federal agencies including the FBI and EPA, thus the pre-establishment of interpersonal relationships is recommended. Efficient and compatible interagency communication systems must be developed to facilitate cooperation.

⇒ Public communication protocols and a local media partnership should be established prior to the onset of an event. A spokesperson, whose job is to facilitate constant contact with the public, should be designated.

⇒ In more serious hoaxes, it may be necessary to have a chief executive and key staff available to the media in order to inform and reassure the public with a clear, consistent message. These emergency management relationships with the media should be established well before an event arises so that mutual trust is ensured.

⇒ With simple awareness campaigns, the public can be educated to recognize the difference between an obvious hoax and a potential threat.

⇒ Hoaxes should be seen as opportunities for surprise exercise. The response community needs to expect that terrorism in all forms will aim to catch victims off guard, and the more they practice under these conditions, the better.

⇒ Standard procedure can be developed that allows for systems to continue with an event, once it has been determined that there exists no real threat, as if they were conducting an interagency exercise. This will allow for full analyses of readiness and further develop the working relationships required to respond to future hoaxes and actual events with increased efficiency.

⇒ All hoaxes should have after-action reports conducted to define areas for improvement.

6.3 Response to Calls of Reports Suspecting a Chemical Agent Release

Transportation systems must now be prepared to respond to investigate a suspected chemical, biological, radiological, or nuclear (CBRN) agent release or dispersal device. This threat co-exists with the industry's on-going concern regarding improvised explosive devices (IEDs), mass shootings, and flammable materials.

Until the CBRN event is confirmed, many dangers exist for those station managers, maintenance personnel, supervisors, transportation police, and other transportation employees who may be assigned to investigate an initial report. These personnel will already be stationed near but, not affected by, the scene.

In most cases, these incidents will involve an unknown substance, suspicious package, or report of a suspicious activity that can safely be investigated and resolved quickly, using elements specified in Procedure Two. However, it is possible that transportation personnel, approaching an incident site in a station or evacuation assembly area, may immediately be faced with mass casualties (e.g., trauma, chemically contaminated, and psychosomatic) as well as major scene control challenges.

Situational awareness, therefore, is critical to effective response. As transportation personnel near the scene, the extent of the incident should become apparent. The following actions should be used as a guide for approaching the scene of what appears to be a WMD event with multiple casualties.

⇒ Approach the scene from upwind and upgrade. Ensure other responders do the same. Upwind distance for a possible chemical incident is at least 300 to 1,000 feet for an explosives related incident.

⇒ Be aware of the need for protection from possible contamination. If personal protective equipment (PPE) is available, and if transportation personnel are appropriately trained, put it on. Otherwise, observe upwind distance parameters.

⇒ From a safe vantage point, attempt to determine the exact location(s) of agent dissemination. Observe patterns or clusters in the severity of symptoms demonstrated by victims, and also observe where the ambulatory victims have assembled.

⇒ From a safe vantage point, attempt to establish communications with transportation personnel in the scene. These personnel may be contaminated, incapacitated, or unable to support response action. Obtain their status and location.

⇒ Observe the scene and do not attempt rescue. Immediate and accurate field reports are the best way to help the victims and ensure the greatest good for the greatest number.

⇒ Look for the following:
- exact location of incident;
- nearest upwind street access;
- estimated number of casualties;
- signs and symptoms of casualties;
- the presence of oily liquids, vapors, clouds, and mists;
- unusual odors;
- weather conditions;
- other resources available to support immediate evacuation from the scene and initial decontamination (sprinkler system, nearby swimming pool or lake, dirt or sand, towels or cloth); and
- information available on possible perpetrators, including physical descriptions, make and/or model of vehicles, or other identifying characteristics.

⇒ Report incident to transportation dispatch, summarizing what was observed.

⇒ As appropriate to internal system procedures, establish (or support already established) command. Transportation personnel are the on-scene authority figures immediately following the incident and will be integrated into the ICS established by local responders upon their arrival.

⇒ Control the scene by:
- establishing an outer incident perimeter to provide safe ingress and egress for arriving responders;
- isolating the hazard area and controlling walking casualties (using voice, bull horn, or public address system) to direct them upwind and upgrade from the incident site, but away from the evacuation site;
- observing unusual activity (perpetrators may be nearby or could be among the injured); and
- anticipating the potential for multiple hazard locations that may require re-defining outer (and inner) operational perimeters.

⇒ Reassure walking casualties, discouraging self-evacuation from a safe distance. Tell them that help is on the way.

⇒ Be aware of site security and check for snipers, secondary devices, suspicious packages, or other threats.

⇒ Monitor weather and wind. Remain upwind of the scene release.

⇒ Identify water supply or other decontamination materials in vicinity (sprinkler system, pool, pond, dirt, clean fabric, etc.).

⇒ Identify staging areas:
- o if practical, position first arriving units and responders upwind and uphill;
- o direct other units to approach from upwind and uphill if possible;
- o avoid stacking units where they interfere with each other's evacuation route;
- o avoid line-of-sight staging with suspected explosive devices;
- o strictly enforce staging instructions;
- o consider having units back into position so that they can leave the scene efficiently, and
- o avoid vapor clouds, mist, and unknown liquids.

⇒ Maintain communications with dispatch. Notify dispatchers of any changes in weather conditions, available site resources, and condition of assembled victims.

⇒ Await other transportation personnel and first responders. Remember that the incident scene is also a crime scene and all precautions need to be taken to preserve evidence.

6.3.1 Responding to an Actual Chemical or Biological Agent Release

If investigation reveals a chemical or biological agent release in a transportation vehicle, station, or facility, the system requires a well-planned, integrated, and coordinated response. Some of the major issues that will require attention during management and control of a chemical terrorist incident include:

⇒ event recognition or agent detection;
⇒ reporting and notification;
⇒ isolation of agent release;
⇒ evacuation of scene (upwind, uphill, up-river) or shelter-in-place;
⇒ isolation of scene or perimeter control;
⇒ crowd control (near perimeter and at evacuation site);
⇒ status briefings and updates to arriving responders;
⇒ staging of emergency response vehicle to avoid contamination, yet hasten ability to reach evacuation site with hoses;
⇒ traffic rerouting, congestion, and control;
⇒ mass casualty decontamination, triage and medical management;
⇒ disposition of the deceased;
⇒ hospital casualty overload;
⇒ public fear;
⇒ public information dissemination;
⇒ spread of contamination;
⇒ safety and welfare of emergency responders;
⇒ evidence identification and preservation; and
⇒ suspect identification, arrest, and criminal prosecution.

To assure its capabilities to respond effectively under these highly adverse conditions, the transportation system should perform the following steps.

⇒ Review the lessons learned from the Tokyo Sarin gas release and its impacts on both emergency response and transportation operations.

⇒ Perform a threat and vulnerability assessment to identify likely targets and current preparedness capabilities (described in Section 5 of this Guide).

⇒ Complete the FBI's Vulnerability Self-Assessment, and share significant findings with local law enforcement (described in Section 5 and included in Appendix B of this Guide).

⇒ Review the system's capabilities and current level of preparedness for emergency response (Appendix D contains a detailed worksheet to support this assessment).

⇒ Invest in the Incident Command System (ICS). Know how this system would be applied in a minor and major incident, and work closely with local responders to improve capabilities through planning, training, and exercising (on this site).

⇒ Understand the Unified Command Structure and its benefits to multi-agency incident response. Unified command provides all agencies with responsibility for the incident with an understanding of one another's priorities and restrictions.

⇒ Develop and revise emergency plans and procedures to address chemical and biological events, emphasizing the specific facility's needs and resources; a system by which to account for employees during emergencies; and a crisis communication system for key personnel and security staff so that they can (1) signal for help surreptitiously when necessary (e.g., with duress alarms), (2) keep a small incident from escalating into a large one, and (3) contact other key staff easily during a crisis (by means of intercoms, mobile and land-line telephones, email, and two-way radios).

⇒ Develop training and exercises to direct and assess management of actual attacks that are small in scale and generally produce fewer casualties than conventional bombs or attacks involving firearms.

⇒ Use Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel Systems as a resource for developing operating policies.[7]

[7] Available from Argonne National Laboratory at 630-252-3235.

⇒ Use Emergency Preparedness for Transit Terrorism as a resource in developing policies, plans, and procedures for managing major incidents.[8]

⇒ Use guidelines prepared by the US Army Soldier and Biological Chemical Command (SBCCOM) for mass decontamination and mass casualty incident response.[9]

⇒ Understand the system's ventilation system, including the impacts of vehicle movement and vehicle HVAC systems on airflow.

⇒ Develop procedures for vehicle control, station ventilation, and station evacuation, ensuring that evacuation sites remain upwind from both the release site and the station ventilation system.

⇒ Understand public fear and how it can be assuaged both during response to an incident and in the aftermath of a successful attack or on-going campaign.

⇒ Understand that persons affected by a chemical release may attempt to self evacuate to area hospitals and medical facilities, thus requiring notification of these institutions of the possible contaminated victims en route.

6.3.2 Support Community Response

The transportation system should be prepared to support emergency response to a major chemical or biological release occurring within its service area. Integration into emergency response planning and coordination with local responders, all activities required for the management of incidents on transportation property, will also serve to enhance the capabilities of the transportation organization to support the community during a major crisis, especially one involving WMD agents.

A key goal of the Emergency Plan is to establish Unified Command with local responders. Unified Command allows all agencies with geographical, legal, or functional responsibility to establish a common set of incident objectives and strategies, and a single plan for action. Using the Unified Command, the public transportation system coordinates with local police, fire, and Emergency Medical Services (EMS) personnel to ensure that:

⇒ one set of objectives is developed for the entire incident,

⇒ a collective approach is used to develop strategies to achieve incident goals,

[8] Available at http://www4.trb.org/trb/homepage.nsf/web/security.
[9] Available for download at http://www2.sbccom.army.mil/hld.

- ⇒ information flow and coordination is improved between all jurisdictions and agencies involved in the incident,
- ⇒ all agencies with responsibility for the incident have an understanding of joint priorities and restrictions
- ⇒ each agency is fully aware of the plans, actions, and constraints of all others,
- ⇒ the combined efforts of all agencies are optimized, and
- ⇒ duplicate efforts are reduced or eliminated, thus reducing cost and chances for frustration and conflict.

6.4 Release of Sensitive Information to the Public

Publicly available information can appear in many forms, including annual reports, media releases, brochures and other promotional materials; Internet web sites and on-line documents; automated or personally-conveyed information; and public records.

The term sensitive information refers to any information that would allow a malicious actor to select, or gain information about, a target without the need to physically access it. The following questions will assist security professionals in reviewing sensitive information that has been, or could be, made publicly accessible.

- ⇒ Has the information been cleared and authorized for public release?
- ⇒ What impact could the information have if it was inadvertently transferred to an unintended audience?
- ⇒ Does the information provide details concerning security procedures and capabilities?
- ⇒ Does the information contain personnel information such as biographical data, addresses, etc.?
- ⇒ How could someone intent on causing harm misuse the information?
- ⇒ What instructions should be given to legitimate custodians of sensitive information with regard to disseminating the information to other parties, such as contractors?
- ⇒ Could this information be dangerous if it were used in conjunction with other publicly available information?

⇒ Could someone use the information to target personnel, facilities, or operations?

⇒ Could the same or similar information be found elsewhere?

⇒ Does the information increase the attractiveness of a target?

Knowledge concerning the threat environment will assist transportation operators in deciding on the level of vigilance with which they review sensitive information. Risk from the public availability of sensitive information comes from both determined and opportunistic threats.

Table 12 identifies generic categories of sensitive information that, if released to the public domain, could place transportation elements at greater risk from determined threats. Transportation operators are encouraged to use these categories when evaluating the dissemination of potentially sensitive information.

Table 12: Categories of Potentially Sensitive Information

TYPE OF INFORMATION	EXAMPLES
Locations & Functions	
Critical assets[10]	High capacity and redundant assets
Network topology maps	Intersections or congestion points
Exposed or unprotected assets	Bridge and over-surface assets
Unmanned assets	SCADA-controlled assets
Hazardous materials	Industrial chemicals or waste storage
Contingency gathering areas	Emergency meeting points and stations
Assessments	
Vulnerability or risk assessments	Security assessments
Hypothetical impact assessments	Environmental impact assessments
Assessments of drills or exercises	Contingency scenario debriefings
Facility limitations	Natural hazard high-risk limits
Facility capacities	Redundant capacities
Specific location or function ranked data	Quantitative comparisons of assets
Operations	
Physical and cyber security plans	Facility and IT security measures
Heightened risk operating procedures	Contingency protection measures

[10] This term refers to the data, communications, energy, and operational systems or structures necessary to sustain business continuity.

Table 12: Categories of Potentially Sensitive Information

TYPE OF INFORMATION	EXAMPLES
Hypothetical emergency scenarios	Operational stoppage scenarios
Emergency response procedures	Facility evacuation criteria
Business continuity plans	Details concerning shifts in production
High-risk operating procedures	Critical processes in production
Facility designs	Blueprints and photos
Operating manuals	Emergency power-down procedures
Meeting minutes	Highlights of recent security concerns
Interdependencies	
Personnel information	Addresses, contact information, etc.
Energy sources	Regular or backup energy sources
Communications assets and procedures	Repeating stations and radio protocols
Transportation methods	Routes use for hazmat transportation
Key suppliers	Safety equipment manufacturers
Key clients	Potential targets for disruption

7 Training and Exercising

This section outlines considerations for training and exercising programs to support core competencies in those areas essential for responsible decision-making and effective implementation of emergency response in the transportation environment.

Transit Safety & Security Program

The Federal Transit Administration and the Transportation Safety Institute's Safety and Security Division offer courses in Transit System Security, Effectively Managing Transit Emergencies, Transit Rail Incident Investigation, Response to Weapons of Mass Destruction, Threat Management & Response to Bus Hijacking, Emergency Response and Access to Alternative Fueled Vehicles, and Crime Prevention Through Environmental Design.

7.1 Principles of Training for Preparedness

When evaluating the transportation system's training and exercising needs, it is important to remember that:

⇒ training should reflect security and emergency plans and procedures; and
⇒ exercises are conducted to assess the quality of both the training and plans, and to provide valuable feedback in the planning process.

The purpose of training for security and emergency preparedness is to provide transportation system personnel with the specific knowledge necessary to perform the critical functions required in system plans and procedures. Training, in this regard, may be highly technical, geared specifically to the responsibilities of an individual employee to support the system during an emergency (e.g., procedures for powering up or down rail service, performing notification and incident reporting, or managing bus vehicle evacuations).

Other types of training may emphasize collaborative activities performed by transportation employees, in concert with local law enforcement, fire and emergency medical services, and other local agencies to support capabilities to accomplish group tasks. In emergency management, the goal of this type of training is to bring individuals, teams, and organizations to a state from which they can accomplish required activities quickly, efficiently, and effectively.

7.2 Existing Training Programs

Around the country, transportation systems of all sizes provide a wide range of training for their employees, contractors, and local public safety agencies. This training addresses many issues pivotal to effective security and preparedness, including basic awareness, reporting emergencies, managing conflicts, evacuating vehicles, and facilities and other safety and security activities.

In the transportation environment, training for safety, security, and emergency preparedness is performed to ensure that:

- ⇒ applicable management, operations, and maintenance rules, procedures, and plans are effectively documented and conveyed to those responsible for their implementation;
- ⇒ manuals showing how to administer, operate, and maintain the system's safety and security equipment and facilities are understood by those responsible for their use;
- ⇒ safety-related rules and procedures for management, operations, and maintenance personnel are documented and effectively implemented by all employees as required;
- ⇒ emergency procedures have been developed, documented and are successfully implemented by all personnel as required, including public safety personnel (if appropriate);
- ⇒ transportation personnel and local emergency responders understand the hazards of the transportation environment; and
- ⇒ an adequate level of preparation is maintained for a possible emergency.

Training typically addresses rules, policies, and procedures, as well as many of the hazards in the transportation environment (e.g., live power, track and roadway safety, hazardous materials and alternate fuels, medical emergencies or blood-borne pathogen awareness, personal safety, and injury prevention). Some transportation systems have established an emergency response agency familiarization program that provides orientation for local law enforcement, fire personnel, and medical services regarding the transportation environment and its vehicles.

National Transit Institute

In addition to its Train-the-Trainer program and its commitment to provide training, education and clearinghouse services in support of public transportation, NTI recently developed the System Security Awareness for Transit Employees and Security Incident Management for Transit Supervisors courses to address the heightened need for interactive training for front-line personnel and supervisors.

Many transportation systems have also initiated basic security awareness or first responder awareness training, which emphasizes topics, such as:

- ⇒ understanding the specific threats from explosives, incendiary devices, and toxic materials (chemical, biological, or radiological agents) and the risks associated with them in an incident;
- ⇒ understanding the potential outcomes associated with an emergency created when explosives, incendiary devices, or toxic materials are present;
- ⇒ the ability to recognize the presence of these devices and materials;
- ⇒ the ability to identify the classes of chemical agents, if possible, using signs and symptoms;
- ⇒ the ability to reference laminated cards and other automated and manual checklists to support initial response activities and incident reporting; and
- ⇒ proper use of personal protective equipment, such as escape hoods and gas masks.

Public transportation systems that routinely work with hazardous materials have certain advantages in this regard, as they are already familiar with EPA regulations

regarding hazardous materials spills, response plans, support training, and coordination programs with their local emergency planning committees (LEPCs) and state emergency response committees (SERCs).

In response to Occupational Safety and Health Administration (OSHA) or environmental requirements, transportation systems also have developed emergency plans for the evacuation of key infrastructure facilities and vehicles. These plans specify the recommended sequence of actions to be taken by transportation system personnel in the event of an emergency, including a security incident. Training provided for these plans may include recognition of the emergency, establishing proper notification procedures, and implementing an appropriate response to the emergency.

Many proactive transportation systems, deeply concerned by the Tokyo Sarin gas release, have supported the development of first response training for WMD incidents in their local communities and states, in partnership with other agencies (such as the International Association of Chiefs of Police), FTA's Transportation Safety Institute (TSI), the National Transit Institute (NTI) at Rutgers, and the Federal Law Enforcement Training Center (FLETC).

Federal Law Enforcement Training Center

FLETC's Security Specialties Division designs, develops and conducts training courses related to antiterrorism, bombs and explosives, counterterrorism, crisis management, patrol procedures, physical security, tactical applications and transportation security. The Division operates a specialized training facility to demonstrate and validate state-of-the-art hardware and procedures relating to antiterrorism and physical security.

Basic awareness and conflict management training, provided through the National Safety Council (NSC) and the Rural Transportation Assistance Program (RTAP), as well as partner programs in first aid and the management of passengers with disabilities and medically fragile passengers (with the American Red Cross, community groups and hospitals, and rider associations), have been developed to support a variety of transportation needs that also emphasize security and emergency preparedness capabilities in small and rural operations.

Transportation systems (particularly those without dedicated transportation police departments) may not yet have conducted formal needs assessments to identify training issues associated with terrorism and emergency preparedness, such as the following:

⇒ implementing the ICS in transportation emergencies;
⇒ coordinating incident command within an unified command structure;
⇒ critical incident protocols for joint partnership with local public safety agencies;
⇒ emergency planning for terrorism;
⇒ decontaminating passengers, employees, and equipment;

- ⇒ managing mass casualties (coordination with emergency responders and hospitals);
- ⇒ community evacuations (procedures and legal issues);
- ⇒ managing public information; and
- ⇒ managing victims, affected families, impacted employees, and community need for information.

Wherever the transportation system may be in its training program, Table 13 provides a useful tool to assess the extent to which current training addresses key security and emergency preparedness issues. Completion of this table will also help to identify opportunities for including or expanding training on these topics, particularly in areas related to WMD terrorism.

7.3 Exercising for Preparedness

Emergency preparedness is a continuous process with the three integral functions of planning, training, and exercising. Each function is dependent upon the other two functions and should not be viewed in isolation. Figure 20 illustrates this relationship.

Table 13: Preparedness Review of Training Programs

TYPE OF TRAINING	SECURITY AND EMERGENCY PREPAREDNESS CONSIDERATIONS															
	Awareness	Reporting an Incident	Coordination with Law Enforcement	Emergency & Security Procedures	Emergency First Aid	Station and Vehicle Evacuation	Managing Threats and Mail	Managing Suspicious Packages	WMD: Signs and Symptoms	Emergency Plan & EOC Activation	Threat & Vulnerability Assessment	Hazardous Materials Response	Evacuating the Medically Fragile	Protecting an Emergency Scene	Conflict Management	Debriefing
Initial																
Refresher																
Certification																
On-the-Road																
On-the-Rails																
Industrial Safety & Security																
Personal Emphasis Training (PET)																
Safety Meetings																
Safety Ride Checks																
Video & Interactive																
Familiarization																
Special Topic																
Safety/Security Committee																

✓ = Addresses Issue, Blank = Does Not Address Issue

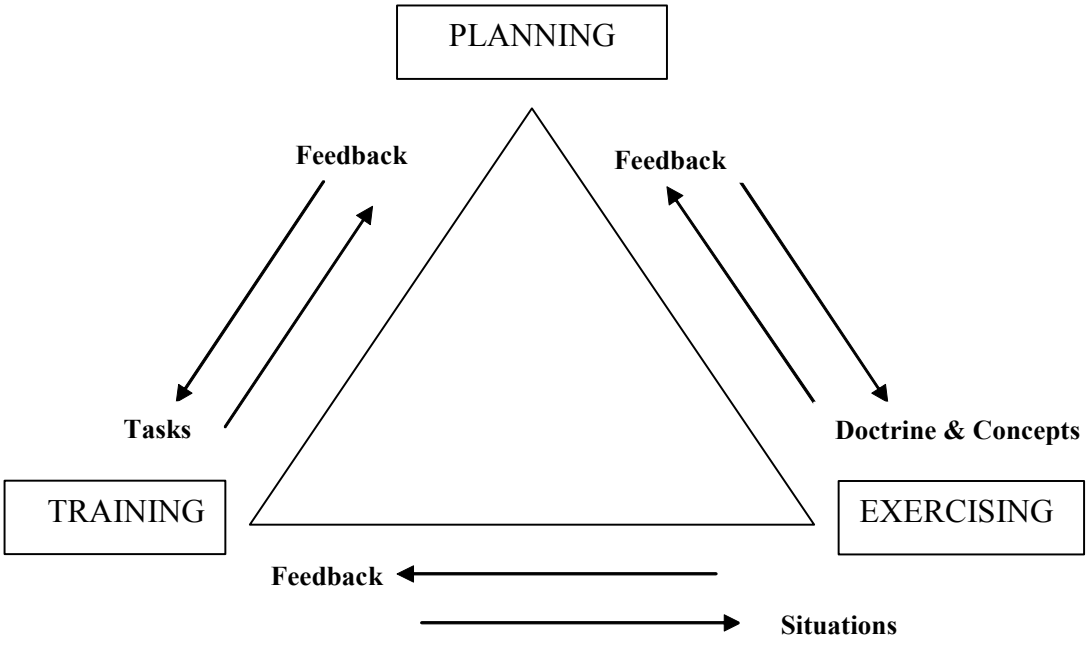


Figure 20: Planning, Training, and Exercising Inter-Relationships

Once plans and procedures have been developed and personnel have been trained to implement them, the transportation system is then ready to conduct an exercise to determine if the planning is adequate to satisfy anticipated needs and personnel are properly trained.

A comprehensive exercise program is one of the best means for assessing emergency plans and procedures, determining the readiness of emergency responders, resolving questions of coordination, clarifying roles and responsibilities and promoting awareness of potential threats and hazards. Exercises are the most practical, efficient, and cost effective method to prepare for disasters and crises. The aim for any transportation system 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 primary benefits of such a program. First, transportation system personnel practice their emergency operating procedure roles and gain proficiency. Second, the coordination among transportation systems and local emergency response agencies is dramatically improved. It is common for emergency preparedness forces to be unfamiliar with the vehicles and facilities operated and maintained by the local transportation system. Likewise it is common for transportation system professionals to be unfamiliar with the procedures and equipment used by local law enforcement and fire and emergency medical services. These mutual benefits arise from exercising, evaluating the exercise (debriefing), and acting upon those lessons learned. An exercise has immense value when it leads to individual and/or collective improvement.

7.4 Building a Progressive Exercise Program

A progressive exercise program requires commitments from the transportation system and community public response agencies to plan and conduct increasingly more challenging exercises over a period of time. Implementation of such a program allows the collective community to achieve and maintain competency in executing the transportation and local emergency response plans.

There are five major types of exercises that comprise this program, each with a different purpose and requirements.

⇒ An orientation seminar is an informal discussion designed to familiarize participants with roles, plans, procedures, and resolve questions of coordination and assignment of responsibilities.

⇒ A tabletop exercise simulates an emergency situation in an informal, stress-free environment. It is designed to elicit discussion as participants examine and resolve problems based on existing crisis management plans.

⇒ A drill is a set of supervised activities that test, develop, or maintain skills in a single response procedure (e.g., communications, notification, lockdown, and fire) and the possible or probable interaction with local government agency functions (e.g., incident command posts, rescue squad entry, and police perimeter control) that will involve actual field response. Drills help prepare for more complex exercises in which several functions are simultaneous coordinated and tested.

⇒ A functional exercise is a fully simulated interactive exercise that tests one or more functions in a time-pressured realistic situation that focuses on policies, procedures, roles, and responsibilities.

⇒ A full-scale exercise evaluates the operational capability of emergency response management systems in an interactive manner. It includes the mobilization of emergency personnel and the resources required to demonstrate coordination and response capability. A full-scale exercise tests total response capability in a manner as closely resembling a real emergency as is possible.

Many systems prefer to start out on a small scale and move toward more sophisticated exercises. This process builds experience, confidence and success for the program, within both the transportation system and the local response community. FEMA, the Department of Justice, Office of Domestic Preparedness, and the National Response Team[11] (NRT) all recommend that systems work their way through a consistent and dedicated program, building from orientation

[11] A group of 14 Federal agencies, including the US DOT, FEMA, and EPA, responsible for coordinating federal planning, preparedness, and response actions related to oil discharges and hazardous substance releases.

seminars and tabletops, to drills and functional exercises, and lastly, to full-scale exercises.

As part of its program for national preparedness and capabilities assessment, FEMA urges local communities to perform one full-scale exercise every three years, with tabletops and functional exercises conducted during off years. Most LEPCs perform one full-scale exercise every five years, though many are now working toward implementing a biennial exercise schedule.

Each transportation system should consider several factors in deciding the scope of its exercise program (particularly if initiating the first exercise).

⇒ How fixed are system emergency response plans and procedures? Have they ever been used in actual situations, or are they still in progress?

⇒ What is the nature and extent of risk posed by various threats located in or near the transportation system?

⇒ What are the existing response capabilities of the community?

⇒ What level of funding is available to support the exercise?

⇒ Is the system scheduled to participate in other exercises, tabletops, or drills within the next 6 to 12 months?

In answering these questions, the system can determine if it should take advantage of orientation seminars and tabletops to communicate emergency response concepts and planning principles to its personnel and familiarize local responders with the transportation environment; or if previous response experience and perceived need and opportunity suggest a more ambitious course.

7.5 Designing Exercises

The CD-ROM for this guide contains several references on developing exercises. Scenarios, which provide the overall outline of how an exercise will be conducted, typically include an event narrative (to get all participants on the same page and set conditions), a major and detailed sequence of events, problems or messages, and expected actions. Scenarios also contain objectives and evaluation criteria to be used by the system to evaluate its performance and support debriefing and critiques. Some key issues to consider when planning exercises are presented below.

⇒ What are the highest priority natural, technological, or man-made hazards or threats to the system?

⇒ What physical or geographical components of the transportation operation are most vulnerable to these threats?

⇒ What agencies and personnel need to participate in an exercise?

⇒ What preparedness functions are most in need of rehearsal?

A realistic exercise scenario provides the best opportunity for a response organization to evaluate its emergency plan, training, and overall preparedness to operate under emergency conditions. There are several ways to incorporate realism into an exercise scenario. Extensive information regarding scenario development is also provided on the guide CD-ROM. Table 14 provides some tips on how to develop an exercise.

Table 14: Exercise Development Checklist[12]

1. ASSESS TRAINING NEEDS
- ⇒ Analyze the threats and hazards
- ⇒ Determine suitable exercise types
- ⇒ Assess capability
- ⇒ Conduct pre-exercise drills or rehearsals

2. DEFINE THE SCOPE
- ⇒ Subject of exercise
- ⇒ Location of exercise
- ⇒ Participants in exercise
- ⇒ Functions to be tested

3. WRITE A STATEMENT OF PURPOSE
- ⇒ Prepare pre-exercise notification
- ⇒ Obtain support from project team
- ⇒ Coordinate with participating personnel and organizations
- ⇒ Schedule the exercise and develop planning milestones
- ⇒ Coordinate logistics, such as facilities, equipment, and support
- ⇒ Organize design and evaluation teams

4. DEFINE EXERCISE OBJECTIVES
- ⇒ Verify the ability to respond to an emergency situation
- ⇒ Validate train operator, controller, and field supervisor training

5. WRITE MAJOR DETAILED EVENTS
- ⇒ Plan exercise enhancements or props, maps, color cards, computers, radios, etc.
- ⇒ Prepare evaluation plan and checklists
- ⇒ Nominate an evaluation team to determine how objectives will be evaluated and how actions by participants will be monitored and measured against plans and procedures

6. IDENTIFY EXPECTED ACTIONS
- ⇒ Reference procedures, rules, plans, and training

7. PREPARE MESSAGES/PROBLEMS
- ⇒ Conduct pre-exercise briefings
- ⇒ Plan post exercise actions
- ⇒ Issue final exercise report or after-action report

8. TRACK EXERCISE-RELATED COSTS
- ⇒ Wages
- ⇒ Materials and supplies
- ⇒ Contractors
- ⇒ Emergency services

[12] In 2002, the Federal Transit Administration (FTA) began issuing and administering grants for the performance of Emergency Preparedness Drills for the top 100 transit agencies. In FTA's Grant Processing Guidelines, exercise goals and objectives, drill requirements, and eligible expenses were identified. The "Fact Sheet" for the guidelines is in Appendix E.

7.6 Exercise Evaluation

The extent and depth of the evaluation should be based on the transportation system's internal objectives, the participating agencies' needs and resources, and any state and federal technical assistance that may be available. State guidelines for CAR reviews, several of which are included on the Guide CD-ROM, provide useful checklists for consideration. FEMA and EPA both have evaluation guides, also presented on the CD-ROM, to support this effort. A sample evaluation checklist for the exercise program is provided in Table 15.

Table 15: Checklist for Evaluating the Transportation Emergency Exercise Program

Attribute 1: The System Has Established an Emergency Management Exercises Program	
1.1	Designated responsibility is identified to coordinate the development and implementation of emergency management exercises.
1.2	The designated staff with responsibility for coordinating the system's Emergency Management Exercise Program has adequate access to top management and to required resources to conduct or participate in the exercises.
1.3	The designated staff coordinates closely with the local emergency planning community (EMA, LEPC) and local law enforcement to remain apprised of community exercises and to encourage system participation in those exercises.
1.4	The system seeks out technical assistance from various levels of government and private entities during the exercise planning.
1.5	Actual disaster or emergency operations experience is factored into exercise planning.
1.6	Results from the system's capabilities assessment, vulnerability self-assessment, and on-going threat and vulnerability assessment are factored into the exercise planning.
1.7	Identified corrective actions, lessons learned, and new technology and/or procedures are factored into exercise planning.
Attribute 2: The System Exercises its Emergency Plan and Procedures on an Annual Basis	
2.1	The system sponsors and conducts a functional, full-scale, or tabletop exercise annually.
2.2	The system participates in one or more functional, full-scale, or tabletop exercise sponsored by Federal, State or local government department/agency annually.
Attribute 3: A multi-year exercise schedule is published and maintained.	
3.1	The system incorporates regulatory required local, state, and federal-sponsored exercises into its schedule.
3.2	The schedule is updated and published at least semiannually.
3.3	The schedule is developed in consultation with local and state agencies.
Attribute 4: Exercises for System Support to Hazard-Specific Programs Comply With Necessary Regulatory Requirements	
4.1	Radiological emergency preparedness (REP) exercises are conducted (if transportation support is provided).
4.2	Chemical stockpile emergency preparedness program (CSEPP) exercises are conducted (if transportation support is provided).

Table 15: Checklist for Evaluating the Transportation Emergency Exercise Program

4.3	Dam emergency action plan (EAP) exercises are conducted as required by the Federal Energy Regulatory Commission (FERC).
4.4	SARA Title III exercises are conducted (if transportation support is provided).
Attribute 5: The System Has Exercised its Emergency Plan and Supporting Procedures Using A WMD Terrorism Response Scenario in the Past Two Years	
5.1	The system has conducted or participated in a tabletop or functional exercise using a WMD terrorism scenario.
5.2	The system has conducted or participated in a full-scale exercise using a WMD terrorism scenario.
5.3	The system has participated in a state or federal tabletop or functional exercise using a WMD terrorism scenario.
5.4	The system has participated in a state or federal full-scale exercise using a WMD terrorism scenario within the past two years.
Attribute 6: The System's Emergency Management Exercise Program Contains an Evaluation Component	
6.1	The system's exercise evaluation methodology is based on clearly delineated evaluation principles.
6.2	The evaluation principles are formally documented, designed for easy use and implementation, and reviewed to ensure their ongoing validity.
Attribute 7: The System Utilizes A Corrective Action Program or Lessons Learned to Strengthen its Emergency Management Program	
7.1	The system has developed corrective action guidance documents.
7.2	Corrective action guidance is applicable to local agencies with emergency management responsibility.
7.3	The corrective action program uses the lessons learned from exercises and actual disasters to modify the EOP and associated SOPs, checklists, field operating guides, and training manuals.

For systems initiating this process, it may be useful to designate an experienced local responder or contractor as the exercise evaluator. This individual can review plans and procedures, support development of exercise objectives, and provide both a third-party assessment of performance and facilitate the group debriefing.

There are several key issues to consider when developing and evaluating exercises.

⇒ With regard to internal alerting, the system should demonstrate its capabilities to receive and process emergency calls and initiate emergency action. Twenty-four hour emergency contact information should be available for all key personnel. Sufficient personnel redundancy should be exercised to evaluate the agency's capabilities around-the-clock operations for the duration of an emergency when warranted.

⇒ In respect to the appraisal of a situation, decision-makers need to know the date, time and location of the incident. They also will want information about

injuries, signs and symptoms (if appropriate), weather conditions, terrain, and names of on-site personnel. A pre-printed response form should be used to assemble information to help determine the most appropriate action. System personnel should demonstrate their capability to perform an effective incident size-up and to define the critical issues of the incidents.

⇒ Transportation procedures should be sufficient to ensure identification of the person in charge, the chain of command, the on-scene authority, and any technical, maintenance or media-relations personnel requirements. Transportation personnel should demonstrate the capability to bring these resources to the scene, to determine who will seek further help, if required, and how these personnel will communication with emergency responders (mobile telephone, radio, walkie-talkie, etc.).

⇒ With respect to the use of on-scene tools, flow charts and checklists are valuable decision-making tools for condensing information. They should contain sufficient detail to ensure that all critical activities are covered. Letters of agreement and emergency response contracts should also be included. Transportation personnel should demonstrate their proficiency in using these materials.

⇒ In regard to external alerting, the system should demonstrate its capability to notify fire and local law enforcement departments, emergency organizations, federal and state authorities, news media, and volunteer or off-duty workers.

⇒ Concerning lead local responder's, the system should also identify its capabilities to recognize the agency that will lead in responding to an emergency and to integrate it into the ICS established by this agency.

⇒ With contact lists, the system should demonstrate that it has an accurate, up-to-date telephone roster for emergencies that may include individuals within the organization, regulatory contacts, containment and cleanup equipment contractors, technical specialists, public health and environmental authorities, and the news media. For telephones not staffed 24 hours a day, the times they will be answered should be included.

⇒ Concerning communications, the system should demonstrate the effective operation of the communications network to be used to support response, including operational procedures for the use of pagers, telephones and cell phones, public annunciation systems, and radios and the different frequencies used by various response organizations. System personnel should identify radio links among those performing similar functions and specify those who are allowed to use radios or telephones. Some equipment must be spark-free to avoid explosion and fire hazards.

⇒ With respect to logistics, system personnel should demonstrate their capabilities to get people and equipment to the site, including the procedures to be followed to ensure sufficient support during the crisis and how crews will be supplied for the duration of the incident.

⇒ In relation to equipment and materials, the transportation system should have an equipment inventory identifying resources available to support emergency response. During exercises, transportation personnel should demonstrate their capabilities to identify and marshal appropriate resources based on the type of incident, the climate, scene access considerations, the speed of local law enforcement and fire services response, the availability of specialized contractors and prior agreements or contracts for services. Outside expertise, contractors, staff and equipment should be evaluated in advance. As appropriate, transportation personnel should know the calibrations and limitations of instruments used to identify and monitor substances.

⇒ When dealing with issues around protective equipment, transportation systems should have a clear policy on its use. Transportation personnel trained to use this equipment should demonstrate their capabilities to consider the circumstances at the scene including climate, season, visual conditions, restriction of movement, and need for decontamination to ensure that protective equipment will not hinder performance.

⇒ Transportation personnel should demonstrate their capabilities to establish their response organization, recognize roles of key personnel, and ensure the assignment of personnel with appropriate qualifications to appropriate duties at the scene.

⇒ If the system has a formal written, mutual aid agreement with another agency, then personnel should demonstrate their capabilities to notify and request this support. The extent of the assistance agreed to will be considered in the overall evaluation of participation in the exercise.

⇒ When coordinating with the news media, the transportation system should demonstrate its capabilities to support effective media relations and to coordinate with the media regarding the dissemination of information to help ensure public safety.

8 Design and Technology Review

This section provides an overview of security design and technology solutions and mitigation measures available to support improved transportation security and preparedness in the operational environment. The CD-ROM for this section provides an inventory of design and technology alternatives for consideration by transportation personnel.

Enhancing physical security in the transportation environment involves a unique combination of requirements driven by the identification of threats, the system's expectation for passenger protection and security, the opportunities for integration of design and technology measures, the financial and physical constraints of the facility, vehicle and operation, and the technology available for a specific security function.

Public transportation cannot be protected like commercial aviation. Trains, buses, and paratransit vehicles must remain readily accessible, convenient, and inexpensive for users. Passenger profiling (including the deployment of computer databases and networks), metal detectors, X-ray machines, explosive sniffers, hand searches, and armed guards, having become features of the landscape at airports, cannot be transferred easily to subway stations, bus stops, paratransit vehicles, automated guideway systems, ferries, and other surface transportation modes. The delays would be enormous, the costs prohibitive, and passengers would seek alternative transport options.

This does not mean that nothing can be done. On the contrary, transportation operators and security officials, in areas more susceptible to terrorist attacks, have developed some effective security countermeasures. Although no one can entirely prevent terrorist attacks, good security measures can make terrorist operations more difficult, increase terrorist detection and identification, keep casualties and disruptions to a minimum, reduce panic, and reassure alarmed passengers in a crisis. Good security measures also assure employees and passengers on a daily basis that the system is safe and secure.

8.1 Security by Design

When designing facilities and procuring vehicles, transportation systems address a multitude of considerations, including security. In today's environment, however, security has taken on new requirements that require facility design (architects) and transportation (planners and engineers) professionals to consider an enhanced range of threats, vulnerabilities, and countermeasures. Balanced assessments of physical design and technology support the development of facilities and transportation services that effectively address needs for accessibility, mobility, security, and emergency preparedness.

Physical design and security technology measures typically involve the use of barriers, ranging from fences and walls to electronic surveillance and intrusion detection devices, to prevent attacks on individuals and facilities and the theft or destruction of valuable items. Police and security personnel may be used to

monitor the barriers and control access to the facility through the barriers. Design, technology, and personnel security solutions can be integrated to deny terrorists what they seek. For terrorist organizations, attacks on protected facilities may generally:

⇒ require more personnel than attacks on less secure facilities;
⇒ require more sophisticated weaponry and tactics; and
⇒ result in more casualties (e.g., killed, wounded, or taken hostage).

Physical security measures may also have a positive psychological affect on personnel within the secure area, because the threat of violence is reduced, and the system's commitment to security is visibly demonstrated. Of course, security design and technology have impacts on the transportation organization in terms of the costs to design, install, and maintain these measures. The costs must be weighed against expected benefits and available resources.

8.2 Crime Prevention Through Environmental Design and Situational Crime Prevention

Situational Crime Prevention strategies have as their basic premise that the physical environment can be changed or managed to produce behavioral effects that will reduce the incidence and fear of crime – and the perceptions of fear – thereby improving in the quality of life, and enhancing profitability for patronage.

Like all situational crime prevention strategies, Crime Prevention Through Environmental Design (CPTED) has as one of its primary aims to reduce the opportunity for specific crimes to occur. Where CPTED differs from traditional target hardening strategies is that CPTED traditionally focuses on design techniques and use of a particular space. Its main goal is to create an environment that does not tolerate crime.

Situational Crime Prevention (SCP) strategies use CPTED design solutions and integrate them with management policy and legal or prosecution measures. For example, to resolve pay phone fraud at a major transportation terminal, an SCP solution would involve both surveillance and environmental controls, and the provision of "call trace" facilities to private telephone subscribers.

Both CPTED and SCP create physical and social conditions through environmental design in selected environments aimed at reducing both crime and the fear of crime. SCP typically addresses physical measures, modifies existing operating procedures, and addresses the specific nature of crime.

While CPTED is invaluable in the initial design of the transportation system environment, SCP offers many advantages during the operational life cycle of the system. As opposed to other methods of crime prevention strategies that may require many years to produce a reduction in crime (e.g., Operation Head Start that intervenes in lives of three- to four-year-olds), SCP efforts reduce crime relatively quickly after intervention. These preventive measures are focused on reducing opportunities for specific forms of crime. Solutions for a particular crime in a

particular situation, however, will not necessarily work in other situations for other types of crime. Therefore, identifying and designing appropriate measures based on an accurate understanding of the success of offenders is essential.

CPTED and SCP techniques stress the importance of including operations, maintenance, and security representatives during the design and procurement stages to aid in the specification, selection, installation, and acceptance of system components. The National Crime Prevention Institute, the American Society of Industrial Security, and the American Institute of Architects teach both strategies, emphasizing the designation, definition, and design of human space.

⇒ Designation – the purpose or intention of the space

⇒ Definition – the social, cultural, legal, and psychological ways that the space is defined

⇒ Design – the prescribed or intended behaviors of the space

Some major CPTED/SCP strategies are listed below.

⇒ Provide clear border definition of controlled space. The borders of the space can be defined by using physical objects, like fences, signs, symbols, distinctive wall colors, or pictures.

⇒ Provide clearly marked transition zones. Transition zones let people know when they are moving into the controlled space.

⇒ Relocation of gathering areas. Gathering places can be placed where they are easy to monitor and where access can be controlled.

⇒ Place safe activities in unsafe locations. Safe activities attract users and the system can monitor undesirable users. In essence, the activities will attract enough people, assuring that no undesirable behavior occurs without being seen.

⇒ Place unsafe activities in safe locations. Unsafe activities can be placed in locations that permit public view and access control.

⇒ Redesign the use of space to provide natural barriers. Conflicting activities can be located far apart, separated by a wall, building, or other activities.

⇒ Improve scheduling of space. Activities can be scheduled to reduce the likelihood of conflicts and to make it easier to control behaviors.

⇒ Redesign or revamp space to increase the perception of natural surveillance. The placement of windows, lines-of-sight, and walkways can increase the feeling of security by increasing the likelihood of surveillance, even without security cameras and other electronic monitoring devices.

⇒ Overcome distance and isolation. Natural surveillance can be facilitated. For example, communications equipment, such as payphones, provide access to assistance. The placement of restrooms near entrances facilitates surveillance of people entering and exiting buildings.

Some CPTED/SCP planning principles and accompanying design strategies most often used in the transportation environment are listed below.

⇒ Plan for concentric security zones and space transitions. Site selection, building clusters, individual building placement and internal configuration of buildings should incorporate the principle of concentric circles of increasing security and overt transitioning between spaces. The outermost ring or perimeter should be the first line of defense and should contain the public activities. Continuing inward, greater security measures should be incorporated as one approaches private or high-risk areas. Prominent use of signage, architectural elements, and natural or human made barriers should be utilized to signify the transition from public to semi-private to private space. Clear border definition should be provided for the controlled space.

⇒ Implement natural surveillance. Legitimate users of the space, observers, or visitors to an area, and persons performing security functions for a space, should observe activities in their environment. Abnormal users should have the perception or reality that their behavior will be observed, while legitimate users feel secure knowing others are present. The prudent use of landscape materials should ensure clear sight lines at grade level and should not create areas of concealment or provide a climbing path to the upper levels of buildings. The use of glazing, the placement of amenities, the style of fencing materials and architectural elements should foster an open environment and eliminate areas of concealment.

⇒ Provide natural access control. Legitimate users of the space should be made to feel welcome and secure, while discouraging the entry of undesirable users. Access to the site, parking areas, and accompanying structures should be well defined and incorporate a welcome or sense of arrival. The main entrance to a site, parking area, or structure should be sufficiently sized to accommodate the normally expected ingress and egress demands. Supplemental entry and exit ways should be securable or have the ability to be closed off. Signage and natural barriers should inform legitimate users of the space of appropriate directions and the rules pertaining to the areas, eliminating excuses for a user's unacceptable behavior.

⇒ Dictate territorial behavior strategies. Utilize the physical design, signage, or other elements to reinforce the sense of proprietorship within an area. The design of a space should reflect the designated purpose and function of the space. Clearly defined defensible space will enhance the users' sense of ownership, while denying criminals the anonymity they seek. Physical design should support the activities of the legitimate users of the space. Design of architectural elements and amenities should not attract undesirable

behaviors, such as loitering. Consider the potential for conflicting activities in a space. Provide natural barriers for these conflicting activities.

⇒ Provide good lighting. Desired users of the space should encounter consistent, well-lit, clean spaces to enhance their feeling of safety. The designated purpose of lighting must be properly identified. If the purpose of lighting is to enhance the security of an area, it should be sufficient to support the principles of natural surveillance. The application of lighting should be uniform, consistent and contain overlapping zones of coverage. Special situations (e.g., CCTV surveillance, parking garages) will require further lighting analysis.

SCP techniques can be implemented during system design, renovation, and/or response to specific crimes. The following two tables are examples of SCP technique utilization by the Washington Metropolitan Area Transit Authority (WMATA) and New York City Transit.

WMATA designed its system for an open environment, optimizing employee and natural surveillance capabilities. The following table describes these features.

Table 16: Security by Design - WMATA

Area Addressed	Preventative Efforts
Supporting Columns	• Decreased number to reduce cover for criminals
Entrances, Exits, and Pathways	• Designed long and straight pathways, stairways, and escalators • Eliminated corners to reduce shadows and decrease transient occupation
Lighting and Maintenance	• Used recessed lighting to reduce shadows and enhance the environment • Excluded public bathrooms in design to eliminate undesirable activity • Recessed walls and bars installed in front to discourage graffiti • Placed litter bins on platforms • Implemented policy directing the cleaning of graffiti and repairing of vandalism within 24 hours of incident
Security Devices	• Installed CCTVs on the end of each platform, deterring criminals • Installed kiosks at entrances to platforms • Installed passenger-to-operator intercoms • Installed blue light boxes with emergency phones every 600 feet
WMATA Transit Police and Personnel	• Added formal surveillance of facility • Required to enforce all facility rules • Trained to report all maintenance problems

As a result of SCP's flexibility, techniques of implementation are also effective in response to specific crimes. Target hardening at NYCT stations in the 1980s provides an example of the many SCP techniques employed in response to specific crimes. Select NYCT stations were experiencing the following fare evasion problems:

⇒ Walking through unmanned "slam" gates to enter the paid-fare area;

⇒ "Backcocking," or turning back the arms of the turnstile, and squeezing through;

⇒ Vaulting over waist-high turnstiles or low fence railings; and

⇒ Using slugs at stations with antiquated mechanical turnstiles.

The following table describes the changes implemented at the 110th Street and Lexington Avenue station in the Harlem District of upper Manhattan.

Changes at NYCT 110th Street and Lexington Avenue Station
To reduce fare evasion, NYCT implemented the following changes: • Installed floor-to-ceiling railings, • Replaced older token devices with modern electronic models, and • Installed clerk-controlled "high wheel" turnstiles.

8.3 Security Technology

Once it is decided to use security technology to enhance surveillance and access control, technology systems must be considered part of a total security system and design approach. Each mechanical technique has distinct technological and operational characteristics and environmental reactions, along with differing requirements for installation and maintenance. To determine which security technology is the most cost effective and appropriate, each transportation system should consider the following questions.

⇒ How will the system be used? Is the system designed to prevent unauthorized access or intrusion, or to provide support for investigation and apprehension of criminals? What are the protocols for responding to alarms? What resources are available to manage false alarms? What priorities are placed on the system as a deterrent to crime versus functionality as a vital, day-to-day component of the security program? Can multiple users benefit from the system? Can CCTV deployed on platforms support operations and dispatch, as well as the transportation security function? Each security situation is unique, which means that there are no packaged solutions.

⇒ What are the operational aspects of a required security system, and what is their priority? Clear identification and prioritization of need is an important first step when investigating security technology. Does the CCTV system need to record camera feeds? Does the system need to be monitored? How fast and clear must images be transmitted from a transportation station or parking lot to a centralized location? Transmission systems may be expensive or limit system functionality and capabilities. They should be thoroughly investigated. What are the requirements for backup systems in power and hardware? How are the alarms assessed for effectiveness (e.g., with CCTV, lights, horns, bells, or printed records)? Does the system have tamper alarms, self-tests, or lightning protection? Each security system requires careful forethought for implementation and operation.

⇒ What are the environmental impacts that affect the security system? Examples of such conditions are weather, water or moisture, vegetation, and corrosion from dust, acid rain, and/or salt. The transportation environment can be challenging for electronic equipment. Housings, accessories, protective cabinets, and shielding should be considered to extend performance and reduce maintenance requirements.

8.4 Considerations from the Department of Justice

As a consequence of the Murrah Federal Building bombing in Oklahoma City during April 1995, the US Department of Justice (DOJ) assessed the vulnerability of federal facilities across the country and issued a report recommending minimum standards for building security. The DOJ's recommendations included standards based upon risk levels for specific buildings determined on the basis of such criteria as daily population and amount of public contact and assessments by building security committees with representatives from each of the agencies in the building.

The following is a list of the risk levels determined using DOJ criteria.

⇒ Level V – Buildings with mission functions critical to national security (e.g., the Pentagon and the CIA Headquarters in Langley, VA). Tenant agencies secure the building according to their own security requirements.

⇒ Level IV – Buildings with 451 or more federal employees, high level of contact with the public, more than 150,000 square feet of space, and high-risk tenant agencies with highly sensitive records.

⇒ Level III – Buildings with 151 to 450 federal employees, moderate to high level of contact with the public, 80,000 to 150,000 square feet of space, and tenants that might include law enforcement agencies, government records.

⇒ Level II – Buildings with 11 to 150 Federal employees, moderate levels of public contact, 2,500 to 80,000 square feet of space, and tenants that have routine missions.

⇒ Level I – Buildings with 10 or fewer federal employees, low levels of public contact or contact with only a small segment of the population, and 2,500 square feet of space or less.

Public transportation systems with multiple facilities of various types may want to evaluate them using a similar method to ensure that strategic and critical facilities are protected to the highest cost-effective level and others, at the other end of the spectrum, are accepted as they are and not protected.

For all levels of facilities, DOJ recommended that 52 minimum security standards, including:

⇒ perimeter security, such as the control of parking facilities, identification systems for parking, closed circuit television monitoring, lighting with power backup, and physical barriers;
⇒ entry security, such as adequate shipping and receiving procedures, access control (including security guard patrols and intrusion detection systems with central monitoring), and screening and monitoring at entrances and exits;
⇒ interior security, such as employee or visitor identification, access control of utility areas, emergency plans, and relocation of daycare centers;
⇒ security planning, such as intelligence sharing among law enforcement and security agencies, adequate training and standards for security guards (including qualifications for unarmed and armed guards), grouping agencies with similar security requirements and risk levels, administrative procedures to minimize risk of crime to employees; and
⇒ construction or renovation to reduce risks, such as installing Mylar film on exterior windows to prevent shattering, attention to blast standards, adequate construction standards, and street setbacks for new facilities.

Based upon the DOJ standards, a building rated Level V (the highest risk) should have:

⇒ a controlled parking facility with adequate lighting and all unauthorized vehicles parked in the facility being towed;
⇒ CCTV camera surveillance with time lapse recording;
⇒ lighting with emergency backup;
⇒ adequate procedures for shipping and receiving;
⇒ intrusion detection systems with central monitoring;
⇒ life safety, e.g., fire detection and suppression systems that satisfy current standards;
⇒ x-ray and magnetometer devices at public entrances and x-raying of all mail and packages;
⇒ high security locks;
⇒ photo identification for personnel;
⇒ visitor control and screening;
⇒ visitor identification accountability system;
⇒ personal identification issuing authority;

- ⇒ controlled access to utility areas and emergency power for critical security systems;
- ⇒ adequate occupant emergency plans, updated annually, and tested periodically;
- ⇒ adequate intelligence sharing and control and common threat nomenclature;
- ⇒ adequate training of security personnel, including guards;
- ⇒ background security checks and/or security control procedures for service contract personnel; and
- ⇒ Mylar film on exterior windows with standards for new construction that include blast resistance and setbacks from the street.

By contrast, the standards for Level I (the lowest risk) facilities include:

- ⇒ adequate exterior lighting with power backup;
- ⇒ review of shipping and receiving procedures to determine vulnerabilities;
- ⇒ upgraded life safety systems;
- ⇒ high security locks;
- ⇒ emergency power for critical security systems;
- ⇒ occupant emergency plans and training;
- ⇒ intelligence sharing and control and common threat nomenclature;
- ⇒ security training for personnel and security guards;
- ⇒ background checks and/or security control procedures for contract personnel; and
- ⇒ review of current projects for blast standards and uniform standards for construction.

Specific DOJ recommendations are excerpted below for each facility risk level. "M" indicates that the minimum standard should be applied, as specified in guidelines maintained by the General Services Administration (GSA). "F" indicates that the standard should be established based on facility-specific evaluation. "G" indicates that the standard is desirable (though not required), and "N/A" indicates that the standard is "not applicable."

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
PERIMETER SECURITY	**I**	**II**	**III**	**IV**	**V**
Parking					
Control of facility parking	G	G	M	M	M
Control of adjacent parking	G	G	G	F	F
Avoid leases in which parking cannot be controlled	G	G	G	G	G
Leases should provide security control for adjacent parking	G	G	G	G	G
Post signs and arrange for towing unauthorized vehicles	F	F	M	M	M
ID system and procedures for authorized parking (placard, decal, card key, etc.)	G	G	M	M	M
Adequate lighting for parking areas	G	G	M	M	M
Closed circuit television (CCTV) monitoring					
CCTV surveillance cameras with time lapse video recording	G	F	F	M	M

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
Post signs advising of 24 hour video surveillance	G	F	F	M	M
Lighting					
Lighting with emergency power backup	M	M	M	M	M
Physical barriers					
Extend physical perimeter with concrete and/or steel barriers	N/A	N/A	G	F	F
Parking barriers	N/A	N/A	G	F	F

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
ENTRY SECURITY	**I**	**II**	**III**	**IV**	**V**
Receiving/Shipping					
Review receiving/shipping procedures (current)	M	M	M	M	M
Implement receiving/shipping procedures (modified)	G	F	M	M	M
Access control					
Evaluate facility for security guard requirements	G	F	M	M	M
Security guard patrol	G	G	F	F	F
Intrusion detection system with central monitoring capability	G	F	M	M	M
Upgrade to current life safety standards (fire detection, fire suppression systems, etc.)	M	M	M	M	M
Entrances/Exits					
X-ray and magnetometer at public entrances	N/A	G	F	F	M
Require x-ray screening of all mail/packages	N/A	G	F	M	M
Peepholes	F	F	N/A	N/A	N/A
Intercom	F	F	N/A	N/A	N/A
Entry control with CCTV and door strikes	G	F	N/A	N/A	N/A
High security locks	M	M	M	M	M

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
INTERIOR SECURITY	**I**	**II**	**III**	**IV**	**V**
Employee/Visitor identification					
Agency photo ID for all personnel displayed at all times	N/A	G	F	M	M
Visitor control/screening system	G	M	M	M	M
Visitor identification accountability system	N/A	G	F	M	M
Establish ID issuing authority	F	F	F	M	M
Utilities					
Prevent unauthorized access to utility areas	F	F	M	M	M
Provide emergency power to critical systems (alarm systems, radio communications, computer facilities, etc.)	M	M	M	M	M
Occupant emergency plans					
Examine occupant emergency plans (OEP) and contingency procedures based on threats	M	M	M	M	M
OEPs in place, updated annually, periodic testing exercise	M	M	M	M	M
Assign & train OEP officials (assignment based on largest tenant in facility)	M	M	M	M	M
Annual tenant training	M	M	M	M	M

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
Daycare centers					
Evaluate whether to locate daycare facilities in buildings with high threat activities	N/A	M	M	M	M
Compare feasibility of locating daycare in facilities outside locations	N/A	M	M	M	M

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
SECURITY PLANNING	**I**	**II**	**III**	**IV**	**V**
Intelligence Sharing					
Establish law enforcement agency/security liaisons	M	M	M	M	M
Review/establish procedure for intelligence receipt and dissemination	M	M	M	M	M
Establish uniform security/threat nomenclature	M	M	M	M	M
Training					
Conduct annual security awareness training	M	M	M	M	M
Establish standardized unarmed guard qualifications/training requirements	M	M	M	M	M
Establish standardized armed guard qualifications/training requirements	M	M	M	M	M
Tenant assignment					
Co-locate agencies with similar security needs	G	G	G	G	G
Do not co-locate high/low risk agencies	G	G	G	G	G
Administrative procedures					
Establish flexible work schedule in high threat/high risk areas to minimize employee vulnerability to criminal activity	F	F	G	G	G
Arrange for employee parking in/near building after normal work hours	F	F	F	F	F
Conduct background security checks and/or establish security control procedures for service contract personnel	M	M	M	M	M

DOJ RECOMMENDATIONS	LEVEL OF SECURITY				
CONSTRUCTION/RENOVATION	**I**	**II**	**III**	**IV**	**V**
Install Mylar film on all exterior windows (shatter protection)	G	G	F	M	M
Review current projects for blast standards	M	M	M	M	M
Review/establish uniform standards for construction	M	M	M	M	M
Review/establish new design standards for blast resistance	F	F	M	M	M
Establish street setback for new construction	G	G	F	M	M

A full description of these standards is available in Vulnerability Assessment of Federal Facilities, Department of Justice, Washington, D.C., June 28, 1995.

8.5 Assessing Technology Options

Successful implementation of security technologies in the public transportation environment requires a process that addresses three key elements:

1. Needs assessment
2. Performance and cost evaluation
3. Training and maintenance considerations

Public transportation agency decision-makers responsible for security technology procurement and deployment – whether it is a single individual or a committee – should use a systems approach to technology selection no matter how simple or complex the process. The analysis of needs, performance, cost, training, and maintenance should consider all phases of project development, integration and testing when possible.

Using the goals and objectives developed through the application of Section 3 preparedness principles, the capability assessment in Section 4 and the assessment of threats and vulnerabilities based on strategies referenced in Sections 5 and 6, the public transit system should have a strong sense of its security technology needs. These activities will provide the public transportation system clear purposes for security technology deployment. The next step is to evaluate current technology performance and cost within the public transportation system's security need framework.

In response to the events of September 11, counter-terrorism technology is being developed at a pace that makes it difficult to assess the ability of new technologies to function as advertised and determine the relative value of different technologies. The absence of an independent testing organization for transportation systems (and others who must secure publicly accessible infrastructure) is a problem left unresolved by the President's Commission on Critical Infrastructure Protection (PCCIP) and successor organizations in the federal government.

Budgetary decisions by federal, state, and local governments to make capital funds available for security technology enhance this problem, since no strategic plans have been developed to ensure that transportation operators are getting the best tools they need for their resources. The DOJ guidelines described above remain the only widely accepted set of objectives for security planning. While extremely useful, these guidelines address federal buildings, and are not generally applicable to the deployment of security technology in the transportation environment.

8.5.1 Available Technologies

Many families of technologies are now being offered to support homeland security and emergency management.

⇒ Devices for gaining access control are primary devices for physical security, such as electronic access control systems, card reader technology, proximity technology, fingerprint systems, keyless

entry systems, telephone or key pad entry systems, and traditional lock-and-key technology. For non-revenue facilities, emphasis in this area generally focuses on integrating employee identification badges with parking lot and facility access control systems. For revenue areas, this technology strengthens the capability to protect restricted areas and deny access to those who do not belong. Biometric technologies (e.g., facial recognition devices) are rapidly advancing and now offer a number of devices that scan faces, fingerprints, retinas or other unique human identification characteristics. When integrated with CCTV, intrusion detection and facility management systems, biometric technology supports the smart monitoring of alarms and systems, reducing personnel costs and perhaps increasing overall system performance.

⇒ Intrusion detection sensors (IDS) are customarily used to detect an intruder crossing the boundary of a protected area. They can be deployed on the interior or exterior of a building and are designed to operate in a variety of harsh environmental conditions compatible with the transportation environment. The detection function must be performed with a minimum of unwanted alarms, such as those caused by wind, rain, ice, standing water, blowing debris, animals, and other sources.

⇒ CCTV surveillance establishes surveillance or visibility to enhance monitoring of areas, facilities, and transportation vehicles. Whether the CCTV system is being utilized for mobile surveillance or facility surveillance, many of the system components are similar (e.g., cameras, recording medium, etc.). The most obvious exception is the transmission medium, with the exception of wireless technology. Public transportation systems implement formal surveillance through CCTV to support efforts to deter those with criminal intent, reassure passengers that the area or vehicle is supervised, and identify offenders to help secure their conviction. The installation of passenger communication systems can extend the effectiveness of CCTV and of transportation personnel in responding to calls for advice or assistance. CCTV surveillance, whether on-board a transportation vehicle or at a system facility, can support implementation in a manner that creates a networked digital video system that simultaneously records digital video and indexes the date, time, and event effectively for archival storage.

⇒ Automatic vehicle location (AVL) systems determine the real-time positions of transportation vehicles using onboard computers, electronic tags, and a positioning system (e.g., global, sign post, or dead-reckoning). This information is then relayed to a central location. Public transportation systems around the country are currently using AVL as the basis for advanced two-way communication, including mobile data terminal systems.

⇒ Mobile data terminal systems take AVL a step further and move the dispatcher and driver relationship into the digital age. Instead of just reporting the vehicle's position, mobile data terminal systems allow for real-time communication between the dispatcher and driver while allowing the driver to operate the vehicle. Currently, this equipment is being utilized primarily by the paratransit industry.

⇒ Silent alarm and emergency signals are key tools in protecting the safety of the bus driver and passengers, especially with today's heightened security needs. When integrated with a mobile data terminal and activated by the operator, the transportation or paratransit vehicle immediately transmits the emergency alert to the central dispatch center along with a current vehicle location derived from the on-board Global Positioning Satellite (GPS) system. Dispatch center personnel then pass this alert on to local law enforcement personnel, who can send the closest unit to the vehicle's location. This type of system often has special applicability for rural environments, where transportation vehicles may typically have long runs in secluded and sparsely populated areas.

⇒ Intelligent Transportation Systems (ITS) apply advanced communication, information and electronics technology to solve existing transportation problems. In its simplest form, ITS is a data and information sharing mechanism. Where feasible, ITS programs take a building block approach to technology. Using computer, telecommunication, aerospace, defense sensors, and other smart technologies, upgradeable, stand-alone systems can be deployed to provide near-term benefits. Integrating these building blocks will facilitate more comprehensive and effective systems in the future.

⇒ Scanner, sniffer, and sensor devices detect chemical and biological agents, nuclear materials, or even the presence of humans in a particular location. They also track the movement of people or things.

⇒ Data mining and related database information technology is used to compile, correlate and analyze existing or developed information to look for patterns and clues.

⇒ Information security technology is designed to support voice and data transmissions, networks, and electronic infrastructure to ensure that transportation systems are protected. Only authorized individuals are given access to critical facilities or areas of operations.

8.5.1.1 Considerations for Technology Evaluation

Experienced transportation system authorities have identified several critical elements in successfully evaluating and selecting security technology. The more approaches considered, the more successful a transportation system may become in acquiring both the type and amount of technology to make a difference.

Security budgets are always considerations, therefore decision-makers must be diligent in measuring the performance and cost of potential technology against the agency's needs. The considerations identified below can be included in the decision-makers strategy for technology assessment and address the final two elements in security technology evaluation and deployment.

⇒ Technology decisions should be made in the context of an overall strategic plan. Ideally, this should be the transportation system's strategic plan, integrated with the community's overall jurisdictional threat assessment and preparedness planning objectives for major facilities (if available and applicable). If such local plans do not exist, then the transportation system should consider creating a strategic plan to provide a context and framework against which to judge technology acquisitions. Veteran transportation managers recommend that, if there is no strategic plan for security technology, do not make any purchases. The negative consequences of poorly designed and ill-suited technology programs, which fall into disrepair, outweigh the potential for getting lucky. Failed technology purchases will become liabilities associated with the security program in future budget negotiations and will be difficult to overcome in the long term.

⇒ Develop a project budget that includes hardware and software estimates, as well as estimates for testing and integration of the technology, training staff, administering or contracting for maintenance, and upgrades. Without proper and extensive cost analysis, technology may present numerous "hidden" costs. Finally, costs for the ongoing use of the technology (i.e., staffing to support CCTV monitoring, or intrusion detection alarm response) should be considered.

⇒ When looking at a particular technology, evaluate multiple vendors. In the case of some technologies, there are relatively few vendors. In others, vendors are plentiful. Take the time to get to know a broad range of vendors and establish relationships with several of them. The development of vendor selection criteria can be useful and can be accomplished by contacting other transportation systems. The goal of developing the selection criteria is to assist in the evaluation of vendor bids.

⇒ Perform rigorous field-testing and observe demonstrations. Vendors make lots of claims about their products. However, each transportation system should test the technology against real-world applications. Experienced transportation system managers recommend field-testing several competing products in a formal evaluation to see which works the best. This process can be supplemented with recommendations from peers and agencies such as APTA and the Community Transportation Association of America (CTAA), which may have made similar acquisitions, and may be willing to share whatever research, literature and information about the product or technology used to support decisions.

⇒ If practical, ensure inter-operability with emergency communications channels and equipment. This is not always easy or even possible, but it does make response and day-to-day working relationships easier in the long run. The best case is to coordinate strategic plans and technology acquisitions with local public safety agencies in the transportation system's service area. Joint purchases of communications equipment and infrastructure should also be considered, as these may provide the most cost-effective and practical way to ensure interoperability.

⇒ Buy smart. Wherever possible, acquire technology that is scalable, upgradeable, expandable, flexible, and versatile. Seek to acquire products that can grow along with the transportation program without the need to be re-engineered to accommodate new tactics or even additional new technology.

⇒ Develop technology skills. Informed professionals make the best technology decisions. With technology permeating almost every area of transportation operations and security and emergency management, it is necessary to acquire some basic familiarity and skill. Experienced transportation system managers emphasize that, if those procuring security technology do not develop technology skills and expertise, they may be unable to effectively procure, develop, sustain, and implement security technology programs.

⇒ Create a trusted agent. Given that it would be virtually impossible for any single transportation operator to effectively test much of the sophisticated technologies that are newly available, consideration should be given to the creation of a trusted agent that is neutral and skilled. Various laboratories and engineering firms offer services to assess technology and support technology acquisitions.

⇒ Establish protocols and procedures for the performance of background investigations for contractors and to secure sensitive

documents such as blueprints, security systems and technology information. Special care should be taken to ensure that confidential and secure information is not easily accessed through the development of user-access level protocols.

Appendix A: Glossary of Terms

Security and Emergency Preparedness Terms

Assets: People, information, and property for which the public transportation system is responsible as legal owner, employer, or service provider.

Assets (Critical): A sub-category of assets whose loss has the greatest consequences for people and the ability of the system to sustain service. These assets may require higher or special protection.

Capabilities Assessment: A formal evaluation, conducted by the public transportation system, to identify the status of its security and emergency preparedness activities. This activity enables the system to determine its existing capacity to:

- ⇒ Reduce the threat of crime and other intentional acts
- ⇒ Recognize, mitigate, and resolve incidents that occur in service and on system property
- ⇒ Protect passengers, employees, emergency responders, and the environment during emergency operations
- ⇒ Support community response to a major event.

Consequences: The severity of impact and probability of loss for a given threat scenario. Consequences may be measured in qualitative or quantitative terms.

Countermeasures: Those activities taken to reduce the likelihood that a specific threat will result in harm. Countermeasures typically include the deployment and training of personnel, the implementation of procedures, the design or retrofit of facilities and vehicles; the use of specialized equipment, the installation of alarms/warning devices and supporting monitoring systems; and communications systems and protocols.

Crime Prevention: The systematic study of the interrelationships among those who commit crime, the location where crime occurs, and the victims of crime to identify patterns, and develop operational and design/engineering strategies to reduce the likelihood of crime and public fear. Two central elements of crime prevention include:

- ⇒ Crime Prevention through Environmental Design (CPTED): Set of design principles used by law public safety professionals, architects and engineers, to limit the ability of the physical environment to support criminal activity and public fear.

- ⇒ Situational crime prevention (SCP): A set of management, policy, and legal/ prosecution measures applied within a physical space to address specific categories of criminal occurrences. SCP is often described as the operational equivalent of CPTED design principles.

Disaster: An event, incident, or combination of incidents, not necessarily related to transit operations, that causes multiple injuries or wide-spread property damage on the system or in the public transportation system's service area.

Emergency: A situation which is life threatening to passengers, employees, or other citizens, or which causes significant damage to any transit vehicle or facility that require assessment and repair, or which reduces the ability of the system to fulfill its mission within its service area.

Emergency Operations Center (EOC): Special policy and incident management area, activated under certain conditions and staffed by representatives from the transit system, including top management, to serve as an information coordination point during special events or emergencies, and to authorize decisions that require/affect the legal authority of the system.

Emergency Operating Procedure (EOP): Any transportation system procedure that details activities to be performed by transit employees when normal operations are not possible.

Emergency Preparedness: a uniform basis for operating policies and procedures for mobilizing public transportation system and other public safety resources to assure rapid, controlled, and predictable responses to various types of transportation and community emergencies.

Evacuation of Passengers: The controlled removal of passengers from a bus, train or other transit vehicle during an emergency situation.

Incident Command System (ICS): A standardized on-scene incident management concept designed specifically to allow responders to adopt an integrated organizational structure equal to the complexity and demands of any single incident or multiple incidents without being hindered by jurisdictional boundaries. Key terms include the following:

⇒ **Command/Incident Commander:** The Command Function of an Incident Command System (ICS) is responsible for directing and/or controlling resources by virtue of explicit legal, agency, or delegated authority. The individual responsible for the overall management of the response is called the Incident Commander. The Command Function sets objectives and priorities and defines the ICS organization for the particular response. Even if other positions are not assigned, the Incident Commander will always be designated.

⇒ **Command** Post: A location at the site of an incident designated as the place from which the incident will be managed and through which all activities and communications will be coordinated.

⇒ **Command Staff:** The IC may appoint a person or persons to be in charge of specific staff functions including the Public Information, Safety, and Liaison functions. The members of the Command Staff report directly to the Incident Commander and will support, advise, and keep the other key functional managers informed. The Incident Commander may appoint functional managers responsible for specific tasks (operations, planning, logistics, and finance and administration). These tasks remain the responsibility of the

Incident Commander unless they are delegated to someone else. The tasks are as follows**:**

- Operations: Operations Staff direct tactical actions to meet incident objectives, administer staging areas, and identify and utilize resources.

- Planning: Planning Staff collect, evaluate, and display incident information; prepare an incident action plan; evaluate options; plan for demobilization; and maintain documentation.

- Logistics: Logistics Staff provide adequate service and support to meet incident or event needs, including supplies, first aid, food, communications, transportation, and vehicle maintenance.

- Finance/Administration: Finance and Administration Staff track incident costs, personnel and equipment records, claims, and procurement contracts; and provide legal expertise.

⇒ **General Staff:** The group of incident management personnel comprised of: the Incident Commander or Unified Command, the Operations Section Chief, the Planning Section Chief, the Logistics Section Chief, and the Finance/Administration Section Chief.

⇒ **Incident Action Plan (IAP):** Contains objectives reflecting the overall incident strategy and specific tactical actions and supporting information for the next operational period. The Plan may have a number of forms as attachments (e.g., safety plan).

⇒ **Operational Period:** The period of time scheduled for execution of a given set of operation actions as specified in the IAP. Operational Periods can be various lengths, usually not over 24 hours. The Operational Period coincides with the completion of one planning cycle.

⇒ **Unified Command:** A unified team that manages an incident by establishing a common set of incident objectives and strategies. This is accomplished without loss or abdication of agency or organizational authority, responsibility, or accountability.

Local Emergency Operations Plan: Plan developed by designated local emergency planning agencies to comply with State and/or local requirements. EOPs typically follow the general format specified by the Federal Emergency Management Agency (FEMA) in the Federal Response Plan, and often include a Basic Plan and supporting Annexes.

Local Emergency Planning Agencies: Includes those agencies of local government with authority to plan for, and manage the consequences of, a major emergency within their jurisdictional boundaries. The agencies vary by community, and often include: local Emergency Management Agencies (EMAs); Local Emergency Planning Committees (LEPCs); municipal Offices of Emergency Management (OEMs) and local Departments of Public Safety (DPS).

Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA): A formal written agreement between the public transportation system and a participating agency, or among multiple agencies and the transit system, which defines respective roles during emergency situations

Notification: The formal advising, by voice or in writing, of specific information about an incident by the process described in the emergency response procedure governing the incident.

Participating Agency: Any fire, law enforcement, medical, governmental, or humanitarian agency that participates in any portion of a public transportation system's emergency response.

Progressive Exercise Program: Comprised of five categories of activities for testing and evaluating the capabilities of transportation personnel to manage emergency situations using existing plans, procedures and equipment. The categories in a progressive exercise program build on each other, in both complexity and level of assessment provided for transportation management. They include:

- ⇒ An orientation seminar is an informal discussion designed to familiarize participants with roles, plans, procedures, and resolve questions of coordination and assignment of responsibilities.

- ⇒ A tabletop exercise simulates an emergency situation in an informal, stress-free environment. It is designed to elicit discussion as participants examine and resolve problems based on existing crisis management plans.

- ⇒ A drill is a set of supervised activities that test, develop, or maintain skills in a single response procedure (e.g., communications, notification, lockdown, and fire) and the possible or probable interaction with local government agency functions (e.g., incident command posts, rescue squad entry, and police perimeter control) that will involve actual field response. Drills help prepare for more complex exercises in which several functions are simultaneous coordinated and tested.

- ⇒ A functional exercise is a fully simulated interactive exercise that tests one or more functions in a time-pressured realistic situation that focuses on policies, procedures, roles, and responsibilities.

- ⇒ A full-scale exercise evaluates the operational capability of emergency response management systems in an interactive manner. It includes the mobilization of emergency personnel and the resources required to demonstrate coordination and response capability. A full-scale exercise tests total response capability in a manner as closely resembling a real emergency as is possible.

Safety: Freedom from danger.

Security: Freedom from intentional danger.

Security Breach: An unforeseen event or occurrence which endangers life or property and may result in the loss of services or system equipment.

Security Incident: An unforeseen event or occurrence which does not necessarily result in death, injury, or significant property damage but may result in minor loss of revenue.

Security and Emergency Preparedness Plan: The formal plan that documents the transportation's system security program and also addressed the elements of that program which affect emergency preparedness for events resulting from intentional acts.

Security Threat: Any intentional action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services.

System: A composite of people (employees, passengers, others), property (facilities and equipment), environment (physical, social, institutional), and procedures (standard operating, emergency operating, and training) which are integrated to perform a specific operational function in a specific environment.

System Security: The application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.

System Security Management: An element of management that defines the system security requirements and ensures the planning, implementation, and accomplishments of system security tasks and activities.

System Security Program: The combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of a system life cycle.

Threat and Vulnerability Assessment: An evaluation performed to consider the likelihood that a specific threat will endanger the system, and to prepare recommendations for the elimination or mitigation of all threats with attendant vulnerabilities that meet pre-determined thresholds. These assessments typically include both revenue and non-revenue operations. Critical elements of these assessments include:

⇒ Threat Analysis**:** Defines the level or degree of the threats against a specific facility by evaluating the intent, motivation, and possible tactics of those who may carry them out.

⇒ Threat Probability: The probability a threat will occur at a specific facility during its life cycle (typically quantified as 25 years). Threat probability may be expressed in quantitative or qualitative terms. An example of a qualitative threat-probability ranking system is as follows:

- Frequent: Event will occur will occur within the system's lifecycle (25 years)
- Probable: Expect event to occur within the system's lifecycle (25 years)
- Occasional: Circumstances expected for that event; it may or may not occur within the system's lifecycle (25 years)
- Remote: Possible but unlikely to occur within the system's lifecycle (25 years)
- Improbable: Event will not occur within the system's lifecycle (25 years)

⇒ Threat Severity: A qualitative measure of the worst possible consequences of a specific threat in a specific facility:

- Category 1 - Catastrophic. May cause death or loss of a significant component of the transit system, or significant financial loss.
- Category 2 - Critical. May cause severe injury, severe illness, major transit system damage, or major financial loss.
- Category 3 - Marginal. May cause minor injury or transit system damage, or financial loss.
- Category 4 - Negligible. Will not result in injury, system damage, or financial loss.

⇒ Threat Resolution: The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.

⇒ Scenario analysis: An interpretive methodology that encourages role-playing by transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system. This analysis uses the results of threat analysis, paired with the system's list of critical assets. Transportation personnel use this analysis to identify the capabilities required to support specific types of attacks. This activity promotes awareness and highlights those activities that can be preformed to recognize, prevent, and mitigate the consequences of attacks.

⇒ Vulnerability Analysis: The systematic identification of physical, operational and structural components within transportation facilities and vehicles that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a given transit facility or vehicle, in its technological systems, and in the way it is operated (e.g., security procedures and practices or administrative and management controls). Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.

Unsafe Condition or Act: Any condition or act which endangers life or property.

Public Transportation Terms

Public Transportation: Transportation by bus, or rail, or other conveyance, either publicly or privately owned, providing to the public general or special service (but not including school buses or charter or sightseeing service) on a regular and continuing basis. This term is also known as "mass transit," "public transit," and "transit."

Public Transportation System: A public entity responsible for administering and managing transit activities and services. Public transportation systems can directly operate transit service or contract out for all or part of the total service provided. Also known as "transit systems" and "public transit systems."

Other important terms include:

Fixed-Route: Service provided on a repetitive, fixed-schedule basis along a specific route with vehicles stopping to pick up and deliver passengers to specific locations; each fixed-route trip serves the same origins and destinations, unlike demand response. Includes route deviation service, where revenue vehicles deviate from fixed routes on a discretionary basis.

Intermodal: Those issues or activities which involve or affect more than one mode of transportation, including transportation connections, choices, cooperation and coordination of various modes. Also known as "multimodal."

Mode of Service: A system for carrying transit passengers described by specific right-of-way, technology and operational features. Typically includes the following:

- ⇒ Aerial Tramway: An electric system of aerial cables with suspended powerless passenger vehicles. The vehicles are propelled by separate cables attached to the vehicle suspension system and powered by engines or motors at a central location not on board the vehicle.

- ⇒ Automated Guideway: An electric railway (single or multi-car trains) comprised of guided transit vehicles that operate without transit personnel on-board. Service may be on a fixed schedule or in response to a passenger activated call button. Automated guideway transit includes personal rapid transit, group rapid transit and people mover systems.

- ⇒ Bus: A transit mode comprised of rubber tired passenger vehicles operating on fixed routes and schedules over roadways. Vehicles are powered by diesel, gasoline, battery or alternative fuel engines contained within the vehicle.

- ⇒ Bus Rapid Transit: A type of bus service that operates on exclusive transitways, HOV lanes, expressways, or ordinary streets. A BRT system combines intelligent transportation systems technology, priority for transit, rapid and convenient fare collection, and integration with land use policy in order to substantially upgrade bus system performance.

⇒ Cable Car: An electric railway with individually controlled transit vehicles attached to a moving cable located below the street surface and powered by engines or motors at a central location not on board the vehicle.

⇒ Commuter Rail: A transit mode that is an electric or diesel propelled railway for urban passenger train service consisting of local short distance travel operating between a central city and adjacent suburbs. Service must be operated on a regular basis by, or under contract with, a transit operator for the purpose of transporting passengers within urbanized areas, or between urbanized areas and outlying areas. Such rail service, using either locomotive hauled or self propelled railroad passenger cars, is generally characterized by multi-trip tickets, specific station to station fares, railroad employment practices and usually only one or two stations in the central business district.

⇒ Demand Response: A transit mode comprised of passenger cars, vans or Class C buses operating in response to calls from passengers or their agents to the transit operator, who then dispatches a vehicle to pick up the passengers and transport them to their destinations. A demand response operation is characterized by the following: (a) The vehicles do not operate over a fixed route or on a fixed schedule except, perhaps, on a temporary basis to satisfy a special need; and (b) typically, the vehicle may be dispatched to pick up several passengers at different pick-up points before taking them to their respective destinations and may even be interrupted en route to these destinations to pick up other passengers. The following types of operations fall under the above definitions provided they are not on a scheduled fixed route basis: many origins-many destinations, many origins-one destination, one origin-many destinations, and one origin-one destination. “Paratransit” is another name for "Demand Response" service.

⇒ Ferryboat: A transit mode comprised of vessels carrying passengers and/or vehicles over a body of water, and that are generally steam or diesel-powered.

⇒ Heavy Rail: A transit mode that is an electric railway with the capacity for a heavy volume of traffic. It is characterized by high speed and rapid acceleration passenger rail cars operating singly or in multi-car trains on fixed rails; separate rights-of-way from which all other vehicular and foot traffic are excluded; sophisticated signaling, and high platform loading.

⇒ Inclined Plane: A transit mode that is a railway operating over exclusive right-of-way on steep grades (slopes) with powerless vehicles propelled by moving cables attached to the vehicles and powered by engines or motors at a central location not on board the vehicle. Special tramway t vehicles have passenger seats that remain horizontal while the undercarriage (truck) is angled parallel to the slope.

⇒ Jitney: A transit mode comprised of passenger cars or vans operating on fixed routes (sometimes with minor deviations) as demand warrants without fixed schedules or fixed stops.

⇒ Light Rail: Lightweight passenger rail cars operating singly (or in short, usually two-car, trains) on fixed rails in right-of-way that is not separated from other traffic for much of the way. Light rail vehicles are driven electrically with power being drawn from an overhead electric line via a trolley or a pantograph. Also known as "streetcar," "tramway," or "trolley car."

⇒ Monorail: A transit mode that is an electric railway of guided transit vehicles operating singly or in multi-car trains. The vehicles are suspended from or straddle a guideway formed by a single beam, rail, or tube.

⇒ Trolleybus: Electric rubber tired passenger vehicles, manually steered and operating singly on city streets. Vehicles are propelled by a motor drawing current through overhead wires via trolleys, from a central power source not on board the vehicle.

Public Transportation Infrastructure: All vehicles, equipment, right-of-way, routes, support equipment and facilities, and buildings and real estate belonging to or operated by the public transportation authority.

Public Transportation Operations Control Center: A public transportation system's central control and communications facility for dispatching operations. Separate control centers are typically be used for different modes (i.e., bus, rail and paratransit/demand-response operations). A few transit systems have co-located modal dispatching functions within a single control center.

Service Area: The geographic boundaries which define the legal and/or management commitment of a public transportation system to provide service to passengers.

Transit Operator: A transportation system employee who is certified by the system to drive or operate a transit vehicle in passenger service, and who must comply with the procedures and rules specified by the system.

Transit Supervisor: A transportation system manager who has specific responsibilities in an emergency situation. The term supervisor typically refers to either a Line Supervisor (Rail) or a Street Supervisor (Bus), defined by the emergency response procedure governing a specific incident.

Appendix B: Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment

This vulnerability self-assessment is intended to help the transportation organization determine its vulnerability to terrorism and to assist local law enforcement in assessing the overall vulnerability of the community. It provides a worksheet that can be customized to the transportation-specific organization. The worksheet is intended to be a general guide. It may not include all issues that would be considered in every specific operation. Therefore, it is imperative to consider the unique character of the transportation organization: its functions, its general public image, and its overall public visibility. Consider both who may work in the organization and what the organization does. Assess the symbolic value of the organization to the public.

Each worksheet section is ranked on a 20-point scale. Answering this self-assessment is a subjective process. The person that best knows the physical security and community value of the transportation organization should complete the worksheet.

There are no firm guidelines on how to score a category. The person selected to complete the self-assessment, based on the uniqueness of the transportation organization, can best determine the score. Since the questions are subjective, give a best estimate when scoring each question.

It is important to remember that the most important threat reduction measure is vigilance on the part of the transportation organization's staff, their awareness of anything out of the ordinary and their prompt communication of that information to the organization's security team or management.

This assessment follows exactly the same format as the community assessment performed by local law enforcement to assist in preventing criminal acts committed by terrorists. Based on the results of this assessment, the transportation organization may wish to share a copy with law enforcement, or to include their representative in the assessment process, to support their understanding of the transportation function and its role in the community.

This assessment should be conducted at least annually, and within the year if there is an increased threat of a terrorist event or whenever there is a significant change to the organization's facilities or activities.

Upon receipt of a high risk assessment, each law enforcement agency sheriff, chief of police, head, or his/her designated representative may forward that assessment, or other threat report, to the state Emergency Management Agency (or equivalent), to state law enforcement, or to the local FBI office.

The Assessment

To complete the assessment, circle the evaluated score on each scale for each question. Then total the scores and enter the total on the last page. Based on the total, use the score guide to assign an overall ranking to the transportation organization.

POTENTIAL TERRORIST INTENTIONS

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Are you aware of any terrorist threat to your organization?
- ⇒ Are you aware of a history of terrorist activity in your area or your specialty?
- ⇒ Are you aware of the level of capability of any suspected terrorist that you believe poses a threat to your organization?

SPECIFIC TARGETING

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Have you obtained current information from law enforcement or other sources that your organization has been targeted by terrorists?
- ⇒ What is the reliability of these information sources?
- ⇒ What is your organization's public visibility?
- ⇒ Does the nature of your organization's activity lead you to think it may be targeted?
- ⇒ Are there activities that indicate possible terrorist preparations in your area or specialty?

VISIBILITY OF YOUR FACILITY OR ACTIVITY WITHIN THE COMMUNITY

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Is your organization well known in the community?
- ⇒ Do you regularly receive media attention?
- ⇒ Is your organization nationally prominent in your field or industry?
- ⇒ Is your location and the nature of your activity known generally to the public?
- ⇒ Have you ever had an event or accident with potential health risks that attracted public attention to your facility?

ON-SITE HAZARDS

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Are hazardous materials, explosives or other dangerous items on your site?
- ⇒ Do you store or use biologic or chemical materials that have the potential to be used as a threat or weapon?
- ⇒ Do you store or use radioactive material at your site?
- ⇒ Do you have a system to control access to hazardous materials, explosives or any other dangerous materials at your site?
- ⇒ Can any products stored or used on your site be used as, or in the manufacture of a mass casualty weapon?
- ⇒ Can any products stored or used on your site cause extensive environmental damage?

POPULATION OF SITE, FACILITY, OR ACTIVITY

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Do you have more than 250 people normally present at your site?
- ⇒ Do you have more than 1,000 people normally present at your site?
- ⇒ Do you have more than 5,000 people normally present at your site?
- ⇒ Do you hold events at your site that attracts large crowds?

POTENTIAL FOR MASS CASUALTIES

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Do materials stored or used at your site have the potential to create mass casualties on-site?
- ⇒ Do materials stored or used at your site have the potential to create mass casualties within 1 mile of your site?
- ⇒ How many people live or work within one mile of your site? 500? 1,000? 2,000? 5,000? More than 5,000?

SECURITY ENVIRONMENT AND OVERALL VULNERABILITY TO AN ATTACK

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Does your organization have effective internal security procedures?
- ⇒ What is the law enforcement presence in your area?
- ⇒ What is the hardness, level of blast protection, etc. of your facilities?
- ⇒ How accessible (security presence, access control, id badges, metal detection buffer zones, fences, etc.) is your facility?
- ⇒ Are your assets and/or its potential recognized as a symbol?
- ⇒ What level of public access is necessary for you to function?
- ⇒ Can you control high-speed vehicle approaches to your facility?
- ⇒ Do you have access control to your parking area?
- ⇒ Do you conduct vehicle searches when entering facility grounds or parking areas?
- ⇒ Do you employ detection/monitoring systems (video surveillance, intrusion detection systems, etc.)?
- ⇒ Is your parking delivery area adjacent to or near your facility?
- ⇒ Is your delivery area supervised during hours of normal business?
- ⇒ Is your delivery area access blocked during hours that your business is closed?
- ⇒ Do you have an on-site food service facility for employees and visitors?
- ⇒ Is access to the water supply for your facility protected?
- ⇒ Is access to the ventilation system for your facility protected?
- ⇒ Do you have a way to quickly shut down the water supply or ventilation system for your facility?

CRITICAL PRODUCTS OF SERVICES

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ What is the importance of your organization to the community?
- ⇒ Is your organization critical to the local population, economy or government?
- ⇒ Is your organization critical to the continuity of basic services?
- ⇒ Is your organization critical to state or national commerce?
- ⇒ What would be the social, economic or psychological ramifications of a terrorist attack against your organization?
- ⇒ What is the nature of your assets: hazardous materials, uniqueness, potential danger to others, etc?
- ⇒ How long would it take to restore your critical services/functions?

HIGH RISK PERSONNEL

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Do you have personnel that are critical to the continuing function of state or local government, basic services, utilities infrastructure, the community, the economy, or of inherent value to your business or agency?
- ⇒ Do you have personnel that are critical for responding to a terrorist act?
- ⇒ What would be the effect of a terrorist act against these high risk personnel?

ORGANIZATION COMMUNICATIONS

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

- ⇒ The following are issues to be considered in selecting your score.
- ⇒
- ⇒ Do you have a mass notification system (public address system, intercoms, alarms)?
- ⇒ Do you have a secure communications network that can be relied upon during a crisis?
- ⇒ Do you have a crisis response team?
- ⇒ Is your crisis response team trained?
- ⇒ Do you conduct regular exercises?
- ⇒ Do local/regional emergency responders participate in your exercises?
- ⇒ Does your Crisis Response Team have its own portable communications system?
- ⇒ Can your Crisis Response Team communicate directly with emergency responders?
- ⇒ Do you have an emergency law enforcement notification system such as a hot line, panic button or something similar?
- ⇒ Is your alarm system tied into the local law enforcement department or do you have an alarm service?
- ⇒ Are your systems tested regularly?

SECURITY AND RESPONSE

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Are your security forces' staffing and training levels adequate?
- ⇒ Do you have the capability to maintain a security presence in a high threat situation?
- ⇒ Are additional security personnel available if requested?
- ⇒ Are there affiliated agency/industry/organization support services available?
- ⇒ Do you have trained disaster response teams within the organization?

- ⇒ Do you have necessary specialty detection, monitoring, hazard assessment devices on hand and are they functional?
- ⇒ Are local/regional law enforcement forces adequate and can they respond rapidly?
- ⇒ Are local emergency responders familiar with your facility and its contents?
- ⇒ Do you keep records on who visits your facility and where they go within the facility?

POLICIES, PROCEDURES, AND PLANS

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Do you have a current crisis response/disaster plan?
- ⇒ Does your plan include the types of crises you are most likely to encounter (e.g., fire, explosion, chemical release)?
- ⇒ Are your employees familiar with the plan?
- ⇒ Have you conducted crisis response and disaster drills and were they effective?
- ⇒ Have you identified the critical functions of your workplace and do you have a plan for continuation of operation during an emergency?

SECURITY EQUIPMENT

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Do you have a security system and is it current technology?
- ⇒ Do you have an intrusion monitoring motion detector or an alarm system?
- ⇒ Do your systems have back-up if power is cut or fails?
- ⇒ Do you have security equipment that would detect leaks or ruptures of potentially hazardous materials?
- ⇒ Do you have personnel protective equipment for your emergency response team appropriate for the hazardous materials at your facility?
- ⇒ Is such equipment in working order and has it been inspected recently?

COMPUTER SECURITY, CYBER-CRIME, AND CYBER-TERRORISM

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Is your site dependent on information technology such as computers and networks to accomplish its daily business activities?
- ⇒ Is the information stored in your computer systems valuable?
- ⇒ Do you have back-up power available for your computer systems?
- ⇒ Do you make back-up copies of your data?
- ⇒ Is your back-up data securely stored?
- ⇒ Does your site have computers or networks connected to the Internet?
- ⇒ Have you experienced problems with computer security incidents, such as computer viruses, worms, web-site defacements and/or denial of service attacks in the past?
- ⇒ Do you have staff in place who are adequately trained and are available to monitor security warnings and take protective measures, such as loading system patches?
- ⇒ Do you have technology security tools in place such as firewalls, intrusion detection systems or anti-virus software to protect your computer systems?
- ⇒ Do you have a computer security policy, plan and procedure that includes a computer security incident response team?

SUSPICIOUS MAIL AND PACKAGES

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Is the mail for your facility opened in a secured area or an area isolated from the majority of personnel?
- ⇒ Have the personnel who open mail received training on the recognition of suspicious mail and/or packages?
- ⇒ Do you have specific procedures on how to handle suspicious mail and/or packages, including possible facility evacuation?
- ⇒ Do you have a secure and contained location where any unusual or suspect deliveries or mail can be stored until proper authorities can evaluate the suspect items?

TELEPHONE, BOMB, AND OTHER TYPES OF THREATS

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Has your staff received training on how to handle bomb and other threat calls?
- ⇒ Does your staff have a checklist of questions to ask the caller in case of a bomb or other threatening call?
- ⇒ Does your facility have a plan on how to handle bomb and other threatening calls?

- ⇒ Does your bomb threat plan include a system whereby your personnel would search your facility to identify suspicious objects to point out to emergency response personnel?
- ⇒ Does your plan include a decision making process on whether to evacuate the facility?
- ⇒ Are personnel familiar with the plan? Have evacuation drills been conducted?
- ⇒ Is your plan coordinated with local law enforcement and the local phone company?

EMPLOYEE HEALTH AND THE POTENTIAL FOR BIO-TERRORISM

Low Vulnerability																			**High Vulnerability**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

The following are issues to be considered in selecting your score.

- ⇒ Do you have an occupational health safety program in place?
- ⇒ Do you have a health professional working at your facility?
- ⇒ Do you have a procedure in place to track the health of each employee and know if more than one employee has the same symptoms?
- ⇒ Do you monitor the health status of employees on sick status or absent otherwise?
- ⇒ Are employees encouraged to keep supervisors informed on any unusual health related event or condition?
- ⇒ Are employees required to report any unusual conditions or substances encountered in the course of their normal duties, such as strange substances or odors from packaging or mail?
- ⇒ Do employees know the proper procedures for emergency operation or shut-off of air handler, air circulating or ventilation systems?
- ⇒ Do you keep a current list of employees, home addresses and emergency contact information?
- ⇒ Do you have an emergency notification plan for employees (e.g. calling tree)?

TOTAL SCORE: _____

SELF-ASSESSMENT EVALUATION

20	**LOW RISK**	**85**
86	**LOW CAUTION**	**170**
171	**HIGH CAUTION**	**255**
256	**HIGH RISK**	**340**

If the total score for the transportation organization exceeds 256, and if local law enforcement has not been involved in the assessment, then the transportation system should notify them at once, including a copy of the assessment worksheet.

Remarks and Unusual or Significant Issues

Please list any important remarks that should be made concerning the self-assessment. Also, please list any unusual or significant findings that developed during your self-assessment. List significant hazardous materials that might be used as a terrorist weapon or any significant impact a terrorist act against your site may cause to the community.

_____

_____

_____

_____

_____

_____

_____

_____

Please attach an additional sheet if necessary.

Appendix C: Security Contacts at the Top 35 Largest Public Transportation Systems

Metropolitan Transportation Authority

MTA New York City Transit
370 Jay Street
Brooklyn, NY 11201-3878
John Jimerson
(718) 243-4158
jojimer@nyct.com

MTA Long Island Rail Road
Jamaica Station Building
93-02 Sutphin Blvd.
Jamaica, NY 11435
James O'Donnell
(212) 878-1146
jodonnel@mtahq.org

MTA Metro-North Commuter Railroad
347 Madison Avenue
New York, NY 10017-3706
Mark Campbell
(212) 340-4913
campbell@mnr.org

MTA Long Island Bus
700 Commercial Avenue
Garden City, NY 11530
Barry Depperman
(516) 542-0100
bdepper@libus.org

MTA Staten Island Railway
60 Bay St. 5th Floor
Staten Island, NY 10301
Thomas Odessa
(718) 876-8271
sirtpd@mail.con2.com

Regional Transportation Authority

Chicago Transit Authority (CTA)
Merchandise Mart Plaza, P.O. Box 3555
Chicago, IL 60654-0555
Beatrice Cuello
(312) 432-8001
bcuello@transitchicago.com

Northeast Illinois Regional Commuter Railroad Corporation
547 West Jackson Boulevard
Chicago, IL 60669
Frederick Leonard
(312) 322-8911
fleonard@metrarr.com

Pace Suburban Bus
550 West Algonquin Road
Arlington Heights, IL 60005-4412
Melinda Metzger
(847) 228-2302
melinda.metzger@pacebus.com

Los Angeles County Metropolitan Transportation Authority (LACMTA)
One Gateway Plaza
Los Angeles, CA 90012-2934
Dan Cowden
(213) 922-3643
cowdend@mta.net

Massachusetts Bay Transportation Authority
10 Park Plaza
Boston, MA 02116
William Fleming
(617) 222-1100
wfleming@mbta.com

Washington Metropolitan Area Transit Authority
600 - 5th Street, N.W.
Washington, DC 20005
Polly Hanson
(202) 962-2150
Phanson@wmata.com

Southeastern Pennsylvania Transportation Authority
1234 Market Street
Philadelphia, PA 19107-3780
Richard Evans
(215) 580-3640
revans@septa.org

San Francisco Municipal Railway
401 Van Ness Avenue, Suite 334
San Francisco, CA 94102
Robert Hertan
(415) 554-7115
robert_hertan@ci.sf.ca.us

New Jersey Transit Corporation

NJ Newark Subway
One Penn Plaza East
Newark, NJ 07105-2248
Joseph Bober
(973) 378-6807
jobber@njtransit.com

NJ Hudson-Bergen
One Penn Plaza East
Newark, NJ 07105-2248
James Decataldo
(201) 209-2405
James.Decataldo@wgint.com

NJ Bus
One Penn Plaza East
Newark, NJ 07105-2248
Joseph Bober
(973) 378-6807
jobber@njtransit.com

NJ Commuter Rail
One Penn Plaza East
Newark, NJ 07105-2248
Joseph Bober
(973) 378-6807
jobber@njtransit.com

Metropolitan Atlanta Rapid Transit Authority
2424 Piedmont Road, N.E.
Atlanta, GA 30324-3324
Gene Wilson
(404) 848-4900
gwilson@itsmarta.com

New York City Department of Transportation
40 Worth Street, Room 1005
New York, NY 10013
Eduardo Cousillas
(718) 391-2809
ecousillas@nyct.com

Mass Transit Administration of Maryland
6 St. Paul Street
Baltimore, MD 21202-1614
Douglas DeLeaver

(410) 454-7736
Ddeleaver@mdot.state.md.us

King County Department of Transportation
201 South Jackson Street, KSC-TR-0415
Seattle, WA 98104-3856
Carol Cummings
(206) 684-2760
carol.cummings@metrokc.gov

Metropolitan Transit Authority of Harris County, Texas
1201 Louisiana Avenue
Houston, TX 77208-1429
Tom Lambert
(713) 615-6409
tl02@ridemetro.org

Bay Area Rapid Transit District
800 Madison Street
Oakland, CA 94607-2688
Gary Gee
(510) 464-7022
ggee@bart.gov

Tri-County Metropolitan Transportation Dist. of Oregon
4012 Southeast 17th Street
Portland, OR 97202
Bob Nelson
(503) 962-4955
nelsonb@tri-met.org

Miami-Dade Transit Agency
111 N.W. 1st Street, 9th Floor
Miami, FL 33128-1999
Bonnie Todd
(305) 375-4240
btodd@co.miami-dade.fl.us

San Diego Metropolitan Transit Development Board

San Diego Trolley
1255 Imperial Avenue, Suite 900
San Diego, CA 92101-7492
Bill Burke
(619) 595-4947
bburke@sdti.sdmts.com

San Diego Transit Corporation (SDTC)
PO Box 122511

100 16th Street
San Diego, CA 92112
Steve Blackwood
(619) 238-0100
steve.blackwood@sdmts.com

Port Authority of New York and New Jersey
1 PATH Plaza
6th Floor
Jersey City, NJ 07306
Martha Gulick
(201) 216-6258
mgulick@panynj.gov

Port Authority of Allegheny County
345 - 6th Avenue, 3rd Floor
Pittsburgh, PA 15222-2527
Bill McArdle
(412) 255-1350
wmcardle@portauthority.org

Regional Transportation District
1600 Blake Street
Denver, CO 80202-1399
David Genova
(303) 299-4038
david.genova@rtd-denver.com

Metropolitan Council – Metro Transit
560 - 6th Avenue North
Minneapolis, MN 55411-4398
Jack Nelson
(612) 349-7201
jack.nelson@metc.state.mn.us

Milwaukee County Transit System
1942 North 17th Street
Milwaukee, WI 53205
Ronald Bollhoffer
(414) 343-1772
wackenhut@mcts.org

Dallas Area Rapid Transit Authority
1401 Pacific Avenue
Dallas, TX 75266-0163
Juan Rodriguez
(214) 749-5901
juanr@dart.org

Alameda-Contra Costa Transit District
1600 Franklin Street
Oakland, CA 94612
Bob Hughes
(510) 891-4811
bhughes@actransit.org

Department of Transportation Services
711 Kapiolani Boulevard, Suite 1200
Honolulu, HI 96813
Roger Morton
(808) 848-4508
rmorton@thebus.org

Greater Cleveland Regional Transit Authority
1240 W. 6th Street
Cleveland, OH 44113
John Joyce
(216) 771-4953
jjoyce@gcrta.org

Orange County Transportation Authority
550 South Main Street
Orange, CA 92863-1584
Dan Jarvis
(714) 265-4346
djarvis@octa.net

Santa Clara Valley Transportation Authority
3331 North 1st Street, Building C
San Jose, CA 95134-1906
Raymond Frank
(408) 321-7175
raymond.frank@vta.org

Regional Transit Authority
6700 Plaza Drive
New Orleans, LA 70127-2677
Ruben Stephens
(504) 827-7920
rstephens@norta.com

Bi-State Development Agency
707 North First Street
St. Louis, MO 63102-2595
Willie McCuller
(314) 982-1507
wmcculler@bsda-transit.org

Regional Transportation Commission of Washoe County
2050 Villanova Drive
Po Box 30002
Reno, NV 89520-3002
David Jickling
(775) 335-1902
djickling@rtcwashoe.com

Via Metropolitan Transit
800 West Myrtle Street
P.O. Box 12489
San Antonio, TX 78212
David Martinez
(210) 362-2430
david.martinez@viainfo.net

Detroit Department of Transportation – People Mover
1301 East Warren Avenue
Detroit, MI 48207
Jerry Jones
(313) 833-7111
jerjon@ddot.ci.detroit.mi.us

Capital Metropolitan Transportation Authority
2910 East Fifth Street
Austin, TX 78702
Pamela Rivera
(512) 389-7471
pam.rivera@capmetro.org

Connecticut Department of Transportation
2800 Berlin Turnpike
PO Box 317546
Newington, CT 06131-7546
Michael Morrison
(860) 594-3053
michael.morrison@po.state.ct.us

Other Contacts

Port Authority Transit Corporation
PA and NJ Administrative and Maintenance Facility
Lindenwold, NJ 08021
Thomas Biehler
(856) 963-7988
TBiehler@drpa.org

Niagara Frontier Transit Metro System, Inc.
181 Elicott Street

Buffalo, NY 14205
Joseph Riga
(716) 855-7666
joseph_riga@nfta.com

Northern Indiana Commuter Transportation District
33 East U. S. Highway 12
Chesterton, IN 46304-3514
Robert Byrd
(219) 926-5744
robert.byrd@nictd.com

San Mateo County Transit District
1250 San Carlos Avenue, P.O. Box 3006
San Mateo, CA 94070-1306
Steven Frew
(650) 508-7743
frews@samtrans.com

Southwest Ohio Regional Transit Authority
414 Walnut Street, Suite 408
Cincinnati, OH 45202-3913
William Desmond
(513) 632-7604
bdesmond@queencitymetro.com

Appendix D: Detailed Capabilities Assessment Worksheet

Prevention

⇒ Does the system check the Homeland Security Advisory Threat Condition every day (http://www.whitehouse.gov/homeland/)?

⇒ Does the system receive threat information and warnings from local law enforcement, state agencies, or other transportation systems regarding threat levels?

⇒ Do appropriate personnel at the system keep informed of major community activities and events?

⇒ Are appropriate personnel at the system aware of ongoing law enforcement concerns regarding specific communities or events that may be targeted for terrorist activity?

⇒ Does anyone representing the transportation system participate in the local or regional terrorism working group or other similar organization?

⇒ Has anyone at the transportation system established a direct relationship with the FBI field office and the FEMA regional office with jurisdiction for the system's service area?

Federal Transit Administration Threat Levels

FTA is supporting the development of transit system protective measures to promote a consistent and effective transit industry response to threat conditions defined by the Department of Homeland Security (DHS). The FTA response model supplements the HSAS model with Black and Purple designations for further refine transit industry activities when an event is in progress and during the post-event recovery of transit services and facilities. The guidance document outlines protective measures in relation to the direction provided by DHS.

Awareness

⇒ Have system personnel been trained to challenge people who appear not to belong in restricted areas or who are not displaying the appropriate identification?

⇒ Have system personnel been trained to recognize unusual, out-of-place, or unattended objects and to report them in a manner that supports appropriate evaluation and decision-making by supervisors and management?

⇒ Does your system have policies in place to ensure that security, operations, or maintenance personnel routinely check unattended public or open areas, such as rest rooms, stairways, parking garages, and elevators for unattended objects?

⇒ Has your system incorporated security checks into policies for pre-trip inspections, vehicle cleaning, and vehicle fueling?

⇒ Has your system reviewed its policies for lost and found items in light of the changing threat environment?

⇒ Has your system developed a customer outreach program to provide passengers with instructions for reporting unusual, out-of-place activity or items?

⇒ Have personnel in your system been trained to:
- identify characteristics of weapons of mass destruction (WMD) use in the transportation environment;
- recognize specific signs and symptoms related to WMD agent release; and
- conduct incident size-up to ensure that appropriate information is reported from the scene to dispatch?

Threat and Vulnerability Assessment

⇒ Has the system considered the potential for terrorist acts against its facilities and personnel?

⇒ Has the system identified the most likely locations for such acts?

⇒ Does the system have a prioritized listing of current security vulnerabilities?

⇒ Does the system have a current program in place to implement security and emergency preparedness measures that address these vulnerabilities?

⇒ Has the system conducted a formal assessment to identify and resolve major vulnerabilities, including the following:
- accessibility of surrounding terrain and adjacent structures to unauthorized access (both human and vehicular);
- site layout and elements, including perimeter and parking, that discourage access control, support forced or covert entry, or support strategic placement of explosives for maximum damage;
- location of incoming utilities and air intake vents (easy access for offenders);
- building construction with respect to blast resistance (tendency toward progressive collapse, fragmentation, and no redundancy in load bearing);
- sufficiency of lighting, locking controls, access controls, alarm systems, and venting systems to support facility control;

- availability of locations for hiding or planting devices or packages on platforms, in tunnels, near fueling, at off-hour vehicle storage facilities, and on passenger vehicles; and
- information technology (IT) and network ease-of-penetration.

⇒ Has the system participated in local law enforcement jurisdictional threat and vulnerability assessments?

⇒ Has the system coordinated its threat and vulnerability assessment activities with local neighborhood watch programs?

⇒ Do businesses and vendors in or near the transportation system coordinate programs?

⇒ Have schools, hospitals, and other public service developed programs to support awareness? Do these programs extend to the transportation system?

Security and Emergency Preparedness Planning

⇒ Has the system reviewed its standard operating procedures (SOPs) for managing both internal emergencies and responding to community emergencies?

⇒ Has the transportation system committed to using the incident command system (ICS) to integrate its response activity into the larger community effort?

⇒ Has the transportation system committed to working with local and state public safety organizations to understand relevant terrorism response plans, SOPs, and the transportation system's role in them?

⇒ Has the system considered its role in community evacuation and in-place sheltering?

⇒ Has the system worked with the local emergency planning community to pre-determine evacuation routes and the transportation role in supporting evacuation or in-place sheltering?

⇒ Has the system made certain that its equipment and capabilities for supporting community response to a terrorist incident are accurately represented in community plans and resource inventory documentation?

⇒ Has the system initiated or completed internal planning efforts to ensure that:
- an emergency contact list is developed and current, and the responsibility for call-outs is clearly identified;
- employees have been issued quick reference guidelines for reporting and managing emergency situations on the system;
- pre-determined guidelines have been developed for managing threats against the system, including procedures for receiving and evaluating

telephonic and written threats, conducting searches, evacuating facilities, and initiating partial or full-service shut-downs;

- pre-determined staging areas have been identified for major sites served by the transportation system and identified as the most vulnerable to attack;
- security and emergency response planning, coordination, and training is formalized and documented;
- security and emergency response plans identify responsibilities of employees by function, employees are proficient in their responsibilities, and have received the appropriate training and exercising to carry out these responsibilities;
- security and emergency response planning includes preparedness for multiple, concurrent events;
- a system-wide service continuation, restoration, and recovery plan is in place, with responsibilities clearly identified;
- revisions to standard operating procedures (SOPs), new SOPs and updates (based on security and emergency response planning activities) have been developed for signatures and distribution to be incorporated into training;
- emergency drills and tabletop exercises are scheduled on a regular basis;
- coordination and training with outside agencies is occurring on a regular basis and the system is effectively integrated into the community's emergency management plans and activities;
- media relations and system information control procedures and policies are established (both internal and external to system);
- documentation of drills is maintained; drill critiques held; and recommendations are recorded and addressed with appropriate with follow-up;
- emergency procedures are reviewed by the transportation system on a regular basis and updated as needed;
- regular assessments of employee proficiency are conducted;
- procedures exist for an alternate operations control center in the event of the evacuation of a primary facility;
- support systems developed to provide post-incident support to customers and employees;
- regular functional testing and inspection of emergency support equipment and systems (e.g., emergency phones, CCTV, alarms, onboard and in-vehicle equipment, two-way radios, fans, pumps, generators, etc.) is performed;
- SOPs for HVAC operations in various emergency conditions have been reviewed;
- contingency plans for loss of electrical power and radio or phone communications have been developed; and
- pre-determined public address announcements for station platforms and on-board vehicles have been developed.

Incident Command System

⇒ Do transportation personnel understand the special tensions between crisis and consequence management during a security incident and recognize that the ICS provides an on-going tool for managing this tension and establishing joint priorities?

ICS provides an important framework from which all responding agencies can work together. In any major incident, many local, state, and federal agencies may become involved. The challenge is to get the various agencies to work together in the most efficient and effective manner. The principles of ICS will enable state and local emergency response agencies to utilize common terminology, span of control, organizational flexibility, personnel accountability, comprehensive resource management, unified command, and incident action plans.

The transportation system should use ICS in order to support the system's ability to integrate with response activities.

⇒ Key definitions, terms, acronyms, roles, functions, and responsibilities used by the local community to describe ICS and its application to manage local response, and to integrate this response with state and federal assets as they arrive on the scene of a major threat or actual event.

⇒ Leadership and authority roles for crisis and consequence management at the local, state, and federal level, and how the transportation system remains aware of these different response levels and functions.

⇒ Key elements of the transportation system's situation and assumptions regarding its capabilities to identify, report, and manage a WMD incident on its property or to support response to an incident in the community (includes what resources, skills, and proficiencies transportation personnel do and do not have regarding WMD incidents, and what specialized functions must be provided by local, state, and federal agencies).

⇒ Key elements of the transportation system's situation and assumptions regarding its capabilities to recover from a WMD incident on its property or in the community, including expectations regarding the role of local, state, and federal resources to support recovery of costs incurred for personnel, equipment, damaged property, decontamination, structural damage, and other activities associated with both response and long term service restoration.

⇒ The community's approach to managing a major incident is often termed the concept of operations, which describes activities to support crisis and consequence management, and typically addresses many different areas of interest.

- If there is a local incident site, an incident command post (ICP) will be established to manage emergency operations at that incident site. The local system with primary jurisdictional authority will designate the

incident commander. The incident commander will direct and control responding resources and designate emergency operating areas.

- The crime scene boundary defines the crime scene. The crime scene may include the area referred to in technical operations as the red zone or working point. State, federal, or local law enforcement personnel may restrict access to the crime scene. Response activities within the crime scene may require special care in order to protect evidence.

- The hazmat boundary defines the hazmat site, which is referred to in hazmat operations as the hot zone and may be termed the isolation area or exclusion zone by other responders, and may include the hazmat upwind warm zone, utilized for contamination control and rescue staging. Depending on the spread of contaminants, the hazmat site may include some or the entire crime scene. Entry into the hazmat boundary is normally restricted to response personnel equipped with personal protective equipment and using decontamination procedures.

- The incident boundary includes the crime scene, the hazmat area, the cool zone or support zone used for incident support operations, such as resource staging or casualty collection, and areas where protective actions, such as shelter-in-place or evacuation, may be recommended or mandatory measures, such as a quarantine become imposed. Access to this area is normally controlled; if quarantine is implemented, egress may also be restricted.

- The incident commander and the community EOC have typically established a division of responsibilities. The incident commander will normally manage field operations at the incident site and in adjacent areas. The EOC will normally mobilize and provide local resources, disseminate emergency public information, organize and implement large-scale evacuation, coordinate care for casualties, coordinate shelter and mass care for evacuees, arrange mortuary support, and, if local resources are insufficient or inappropriate, request assistance from other jurisdictions of the state. Does the transportation system understand how its field and EOC operations will coordinate with the community response?

- As state and federal responders arrive, the response will transition from an incident command operation to a unified command arrangement. Does the transportation system understand its role in unified command?

- If there is no local incident site, which may be the case in incidents involving biological agents, consequence management activities will generally be directed and controlled from the local EOC. An incident commander may be designated. When state and federal response forces arrive, the EOC may be used as a unified command operations

center. Is the transportation system prepared to coordinate with and support this type of response effort?

Figure 21 displays a sample decontamination scene staging area schematic. Notice how the contamination reduction corridor is a limited access point to the hot zone. This is where emergency responders must remain extra careful to protect themselves and evidence from becoming contaminated.

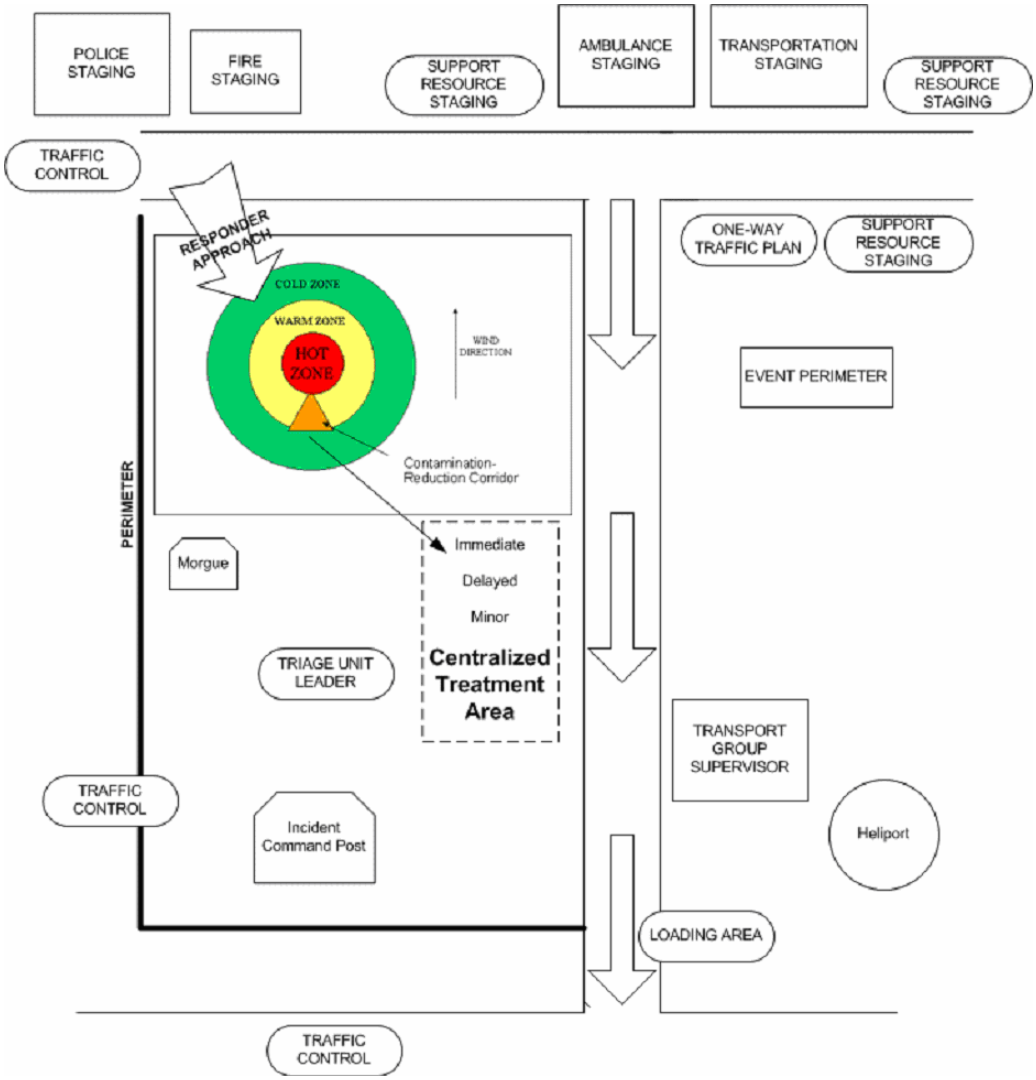


Figure 21: Sample Decontamination Scene Staging Area Schematic

Elements of Notification and Response

⇒ Has the system reviewed its current emergency procedures to:
- ensure that notification procedures support dispatch of the correct responders with the appropriate equipment and that all responders are aware of potential hazards (structural issues, electrical issues, suspected chemical or toxic agent) prior to his/her arrival at the scene;
- ensure timely activation of the transportation system emergency operations center (EOC) or other specially-equipped facility from which transportation management can exercise direction and control, coordinating necessary resources in an emergency situation;
- identify roles and responsibilities for transportation personnel conducting field operations at the scene in specific terms, so that operators and supervisors understand the limits of their responsibilities, particularly in hazardous conditions;
- use escape hoods or pre-staged gas masks to support facility evacuation (requires training and exercising for all personnel involved in the program);
- revise evacuation and shutdown procedures to consider secondary attacks and other environmental hazards;
- manage information requests from victims, families, and relatives (applying the NTSB guidelines for airplane crashes may be appropriate);
- evaluate activities to ensure ongoing liaisons with local emergency responders;
- ensure the safety and security of passengers after the incident;
- manage medically vulnerable passengers in community and vehicle evacuations;
- prioritize decision-making regarding the need for medication, treatment, and hospitalization;
- restore service or create alternatives with heightened security or road, bridge, and tunnel restrictions; and
- issue public information.

Other Considerations

Other considerations for planning are listed in the following outline.

⇒ Strategies and programs for initiating sustained relationships with local emergency planning organizations, ensuring that transportation systems are aware of the emergency management process in all phases.

- Local communities must understand the resources and capabilities of transportation systems to support preparedness and response, as well as the hazards involved in operations based in the transportation environment.

- Local responders must also recognize the ways in which community traffic management decisions may affect transportation operations, providing additional response challenges.

- Public transportation systems must learn what roles they can or are expected to play in the community response effort and must ensure that their employees are trained to proficiency and ready to provide this service safely and effectively.

- Enforcement issues must all be resolved. For example, the issuance of evacuation orders, the management of children and those with serious medical conditions, the support of people of age and those with mobility, sensory and/or cognitive disabilities, the institution of in-place sheltering in transportation facilities (in response to a hazardous materials or CBRN incident at the transportation system), and the use of transportation facilities as mass care shelters.

⇒ Strategies for overcoming friction and resistance from local public safety organizations, thus ensuring that transportation responders are not marginalized.

- Public transportation concerns regarding incident staging, traffic control, managing passenger and employee safety, and restoration of service must be acknowledged in the local response effort and addressed in the response.

- The jurisdictional authority and safety concerns of the transportation system must be addressed in all emergency response and management activities.

⇒ Tools and techniques for supporting effective integration of the transportation system into new models and emerging structures for incident management at the local and state level.

⇒ Strategies for ensuring that local responders are aware of unique hazards associated with the transportation environment, transportation equipment, and alternative fuel vehicles;

⇒ Tools and systems to support strategic deployment of resources at the scene (to ensure availability, yet manage convergence and avoid premature commitment);

- Scene management techniques to resolve inherent conflicts among competing priorities and practical approaches for promoting life safety priorities while preserving (as much as possible) evidence at any scene that may have criminal origins.

- Tools for tracking resource and personnel expenditures devoted to emergency response, in keeping with requirements necessary for

reimbursement from FEMA, state and local agencies, FTA or other organizations, and for mutual aid partners and contractors.

- Available classroom and simulation training and techniques for effectively conveying scene check-in, management, staging logistics, and incident documentation requirements to transportation employees.

⇒ Recovery can be complicated by the presence of persistent agents, additional threats, extensive physical damages, and mass casualties. The community and the transportation system should consider their approaches to staffing and managing the operational periods required to stabilize the event and support long term recovery.

Figure 22 (on the last page of this section) shows sample operational shifts of ongoing management modes in comparison to emergency response modes immediately following a security-related incident. The transportation system should expect that response to a major incident will result in multiple operational periods, comprised initially of 12 hour shifts, then giving way to longer planning phases as the incident is brought under control.

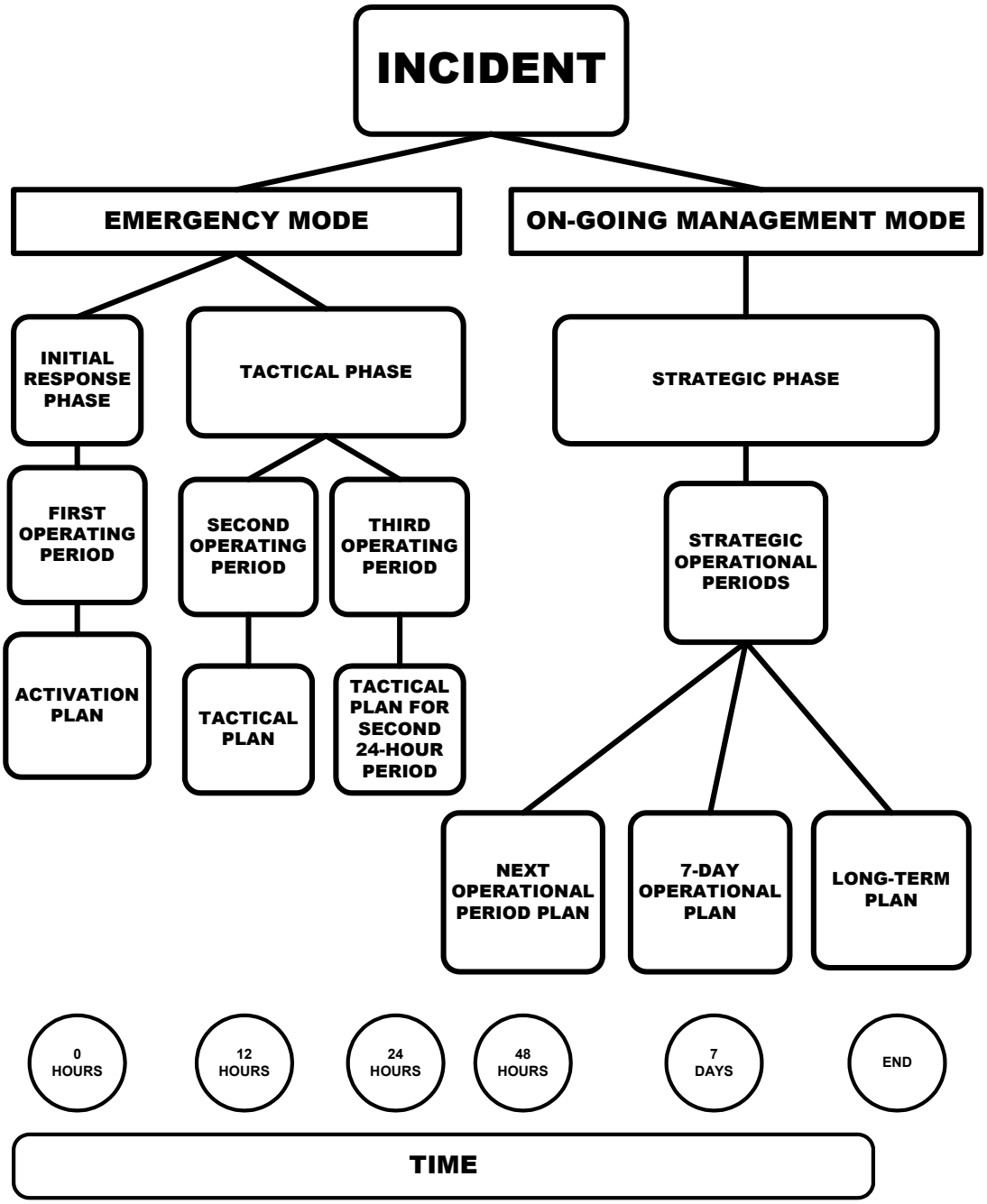


Figure 22: Sample Operational Shifts

Appendix E: Sample Grant Processing Guidelines

WHAT: Security/Emergency Management Grants for Emergency Preparedness Drills

PURPOSE: To conduct emergency response drill(s) and exercise(s) designed to test and evaluate the transportation agency's internal and external notification and response procedures and interagency communication and operations at the command post and incident scene. For transportation agencies conducting multiple exercises, at least one exercise should address a terrorist incident.

GOALS AND OBJECTIVES:

Testing effectiveness and ability of Emergency Management Plans at a minimum, this must include the items listed above in 'Purpose.' Examples of additional elements typically contained in an exercise include:

1. Ability to work with regional and local emergency response personnel
2. Communications link with passengers
3. Identification of ICS components you are using
4. Assignment of personnel to critical functions
5. Protection of emergency scene e.g. power off, protection of personnel in right-of-way, etc.
6. Initiation of evacuation procedures
7. Coordination with other emergency responders
8. Identification of staging area for equipment and personnel
9. Notification to other supporting agencies
10. Mitigation and recovery

REQUIREMENTS:

Pre-Grant: Identify pre-grant requirements, i.e., description of the exercise scenario, goals and objectives and budget for each drill.

Progress Reporting: Identify progress reporting requirements, i.e., the dates each drill was completed and the date the After-Action Plan was completed.

After-Action Report: This Report should be required as a condition of the grant award.

PERIOD OF AVAILABILITY: Define a period of availability for receipt of funds

SAMPLE ELIGIBLE EXPENSES:

- Materials, supplies, rental equipment to conduct each drill
- Consultant fees for technical assistance in the developing and evaluating the drills
- Additional operating expenses that may be incurred, for example: alternative service provided due to service disruption
- Emergency services agency expenses such as overtime wages and use of agency equipment and supplies
- Wages related to the direct delivery of services in support of the drill

INELIGIBLE EXPENSES:

- Any capital expenses

REVIEW CRITERIA:

- Transportation agency should complete one full-scale drill at a minimum
- Multiple drills including a tabletop exercise are encouraged
- Interagency coordination with other first responders is critical
- For metropolitan areas with more than one transit operator, transportation agencies are encouraged to submit one unified application
- Cost should be proportionate to complexity of drills

Appendix F: A Memorandum of Understanding between [Local Public Safety Agency] and the [Local Transit Agency]

Purpose

This Memorandum of Understanding (MOU) is intended to document the intention of the [local transit agency] and [local public safety agency] to work together, on a continuing and lasting basis, toward maximum cooperation and mutual assistance in the areas of disaster response and emergency preparedness. To the maximum extent possible, the parties will develop joint programs for planning, training, conducting exercises, and responding to disasters impacting the [local transit agency] and/or [local public safety agency] or the community served by both agencies. Specifically, this MOU will address:

The development of a mutual aid agreement between the [local transit agency] and the [local public safety agency] in the event of disasters, natural or manmade, that overwhelm the capabilities of either;

The development of a joint exercise that requires the response of both entities in responding to disasters such as, but not limited to, an oil spill to the environment;

The development of a coordinated response in event of terrorist use of weapons of mass destruction within the [local transit agency] or community served by the [local public safety agency] and in accordance with the *Homeland Security Domestic Preparedness Program*.

Mutual Aid Agreement

The State of [name of state] authorizes the state and its political subdivisions to develop and enter into mutual aid agreements for reciprocal emergency aid in case of emergencies too extensive to be dealt with effectively unassisted.

It is in the best interest of the citizens of [name of community] for the [local public transit agency to enter into such a mutual aid agreement with [local public safety agency] to provide for expeditious emergency assistance, resources permitting, in the event of a catastrophic event or natural disaster in the city and/or surrounding county.

The [local transit agency] desires to provide reciprocal assistance to [local public safety agency], resources permitting, in the event of a natural or man-made disaster.

Mutual Aid Agreements provide the mechanism that enhances and leverages existing capabilities.

The process for creating a Mutual Aid Agreement between the [local transit agency] and the [local public safety agency] begins with:

- ⇒ a working group will be established. This group will review current local, state, and federal laws to clearly identify any limitations to how each party will provide assistance during emergencies;

- ⇒ a draft agreement will be written (unless the law says otherwise) including the terms of the agreement, the participating parties, period of assistance, definitions of disasters or emergencies, and designating an authorized representative who can execute the agreement;

- ⇒ the agreement will identify available services and resources, with some specific reference to the type of resources that can and cannot be used. Limitations will be spelled out also, to ensure the resources are not exhausted;

- ⇒ the Agreement will identify exactly how to request assistance, for instance, the "trigger" for a request - a local emergency or disaster declaration;

- ⇒ the Agreement will explain how the agency will request and what the expected committed response would be;

- ⇒ the Agreement will identify who can make the request, and whether it should be written or oral. If possible a form will be developed clearly explaining what is needed and for what length of time;

- ⇒ the Agreement will define operational procedures and explain who will maintain control of the resources provided and who will provide required maintenance for any equipment made available;

- ⇒ the Agreement will make provisions for any food, housing, or communications support required for personnel who respond to an emergency or disaster; and

- ⇒ the Agreement will define reimbursable expenses, including personnel, material, and equipment costs and for replacing damaged or destroyed equipment.

Joint Oil Spill Exercise

The [local transit agency] and [local public safety agency] intend to test capabilities and limitations of both entities in responding to an oil spill into the environment during a joint exercise in FY 2003. An Exercise Planning Team comprising of representatives from [local public safety agency]; [local transit agency]; and the [city/county] Emergency Operations Center will:

- ⇒ define the type of exercise, develop an exercise scenario, and ensure active participation by [local transit agency] and [local public safety agency] response organizations;

- ⇒ identify a list of key entities who will have responsibility for developing, controlling, and participating in the exercise;

- ⇒ identify resources for developing and conducting the exercise;

- ⇒ establish a timeline for keeping such an approach on track;
- ⇒ conduct the exercise; and
- ⇒ review the lessons learned from the exercise and incorporate them into future response and exercise plans.

Domestic Preparedness

The [local transit agency] serves one of the 120 cities selected by the U.S. Department of Defense to receive extensive training to prepare the community for the potential of a terrorist attack using weapons of mass destruction. The U.S. Army Chemical and Biological Command [conducted/will conduct] this training during the period [identify date]. [Local public safety agency] participated in this training with the [local transit agency].

The [local transit agency] will continue to coordinate development of its Domestic Preparedness Program with [local public safety agency]. Specifically, the [local public safety agency] will:

- ⇒ coordinate with the [local transit agency] on its plans for responding to terrorist use of weapons of mass destruction planning and operations;
- ⇒ encourage transit first responders to participate in training offered by the [local public safety agency];
- ⇒ invite [local transit agency] to participate in the development and conduct of the Biological Attack Tabletop Exercise and other follow-up exercises;
- ⇒ collaborate with [local transit agency] in the purchase of response, detection, and decontamination equipment for incidents involving terrorist use of nuclear, biological or chemical agents to ensure the right mix of equipment is available for responding to such incidents; and
- ⇒ provide reciprocal support, resources permitting, to the [local transit agency] in the event of an incident on an agency vehicle or in an agency facility.

Agreement Modification Process

Modifications to this agreement may be presented at anytime and shall be mutually agreed upon in writing after joint discussions involving both parties.

This Agreement shall become effective when executed by both parties and shall remain in effect for a period of five (5) years, and shall automatically be renewed for successive five (5) year periods unless terminated by either party upon sixty (60) days prior written notice.

IN WITNESS WHEREOF, the parties' authorized officers have executed this Agreement on the date first above written.