University Transportation Center Research Project

Transportation System Security and State Transportation Agencies

Final Report

INCORPORATING SECURITY INTO THE TRANSPORTATION PLANNING PROCESS

By

Michael Meyer

Brandon Denny

Contract with

Research and Innovative Technology Administration (RITA)

In cooperation with

Georgia Transportation Institute / University Transportation Center

Disclaimer:

The contents of this report reflect the views of the author(s) who is (are) responsible for the facts and the accuracy of the data presented herein. This document is disseminated under the sponsorship of the Department of Transportation University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The contents do not necessarily reflect the official views or policies of the Research and Innovative Technology Administration, Georgia Institute of Technology, Georgia Tech Research Corporation or the Georgia Tech Applied Research Corporation. This report does not constitute a standard, specification, or regulation.

Incorporating Security into the Transportation Planning Process

Brandon Denny
Georgia Institute of Technology

Georgia Transportation Institute
University Transportation Center

Transportation research to benefit Georgia...and the world

Report 08-04
March 1, 2009

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
GTI-08-04		

4. Title and Subtitle	5. Report Date
Incorporating Security into the Transportation Planning Process	March 1, 2009
	6. Performing Organization Code: GTI/UTC

7. Author(s)	8. Performing Organization Report No.
Brandon Denny	08-04

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Georgia Transportation Institute/UTC Georgia Institute of Technology 790 Atlantic Drive Atlanta, GA 30332-0355	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Georgia Transportation Institute/UTC Georgia Institute of Technology 790 Atlantic Drive Atlanta, GA 30332-0355	Research Report, 2008-2009
	14. Sponsoring Agency Code

15. Supplementary Notes

This research is partly supported by the University of Tennessee's Southern Transportation Center.

16. Abstract

The transportation system is an important network established to ensure the mobility of people and goods between destinations. In addition, it also serves a vital role in responding to disasters, and therefore deserves special attention when those disasters threaten to decrease its support capability. The task of securing a transportation system consisting of multiple interconnected assets is a complex responsibility. As an owner and operator of major transportation infrastructure, state Departments of Transportation (DOTs) have a vested interest in ensuring this balance and represent an important mediator between federal and local interests, assuming nine key security planning roles in their traditional transportation planning duties: Coordinator, Analyzer/Planner, Financial Administrator, Infrastructure Owner, Infrastructure Operator, Implementer, Regulator, Information Provider, and Influencer.

Through their internal vulnerability assessments, the departments already perform a vital security planning function that can support their own planning efforts as well as others. Incorporating security into the transportation planning process requires modification as feedback of implementation methods is received. It does not mean transforming the DOT into a security agency, but rather incorporating a security perspective into the analysis of the system. This first involves establishing a more solid role as a coordinator in order to solidify vital linkages between agencies relevant to security planning. This interaction should reveal standardization issues the DOT can address in order to ensure effective collaboration, communication and coordination. Funding security measures may be difficult; but by incorporating security measures into initial analyzation and planning processes, they can be brought into the broader concept of the system rather than simply added as additional funding needs. The nine roles suggested earlier offer opportunities for state DOTs to overcome these and other challenges faced in the process of incorporating security into the transportation planning process. Through these roles, state DOTs can ensure that security efforts reach the parts of the system that require them and begin to build a more secure system.

17. Key Words	18. Distribution Statement
Transportation, Department of Transportation, Transportation Security, Vulnerability Assessment	No restrictions.

19. Security Classif (of this report)	20. Security Classif (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	55	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

TABLE OF CONTENTS

LIST OF TABLES iii

LIST OF FIGURES iv

LIST OF ABBREVIATIONS v

SUMMARY vi

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: CONCEPTUAL FRAMEWORK 3

CHAPTER 3: CHARACTERISTICS OF THE TRANSPORTATION SECURITY PLANNING ENVIRONMENT 6
- 3.1 National DOT Security Planning 7
- 3.2 State DOT Security Planning 9
  - 3.2.1 State Emergency Operations Plans 9
  - 3.2.2 Continuity of Operations Plans 12

CHAPTER 4: ASSESSING AND QUANTIFYING VULNERABILITY 15
- 4.1 Vulnerability Analysis 15
- 4.2 Critical Asset Identification 16
  - 4.2.1 Criticality assessment issues 19
- 4.3 Vulnerability Assessment 20
  - 4.3.1 Vulnerability Assessment Issues 22
- 4.4 Consequence Assessment 23
- 4.5 Countermeasures 25

CHAPTER 5: ISSUES IN TRANSPORTATION SECURITY PLANNING 26
- 5.1 Funding 26
- 5.2 Coordination 29
- 5.3 Standardization 31
- 5.4 Communications Equipment Compatibility 32
- 5.5 Role of Intelligent Transportation System 33

CHAPTER 6: CONCLUSIONS 35

CHAPTER 7: RECOMMENDATIONS 37

APPENDIX A: EMERGENCY SUPPORT FUNCTION #1 40

APPENDIX B: INTERVIEW QUESTIONNAIRE 50

APPENDIX C: CRITICAL ASSET FACTORS 51

APPENDIX D: VULNERABILITY FACTORS..... 52

REFERENCES 53

LIST OF TABLES

TABLE 1: EXAMPLE CRITICALITY SCORING TABLE 18

TABLE 2: EXAMPLE CRITICAL ASSET FACTOR SCALE 19

TABLE 3: EXAMPLE VULNERABILITY SCORING TABLE 22

TABLE 4: FACTOR VALUES FOR RECOGNITION AND ATTENDANCE 23

TABLE 5: A SUMMARY OF STATE DOT ROLES. 38

LIST OF FIGURES

FIGURE 1: THE POSITION AND ROLES OF THE STATE DOT 3

FIGURE 2: VULNERABILITY VERSUS CRITICALITY AND THE FOUR QUADRANTS OF CONSEQUENCE. 24

LIST OF ABBREVIATIONS

AASHTO	American Association of State Highway and Transportation Officials
COOP	Continuity of Operations Plan
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security
DOT	Department of Transportation
EMA	Emergency Management Agency
EOP	Emergency Operations Plan
FEMA	Federal Emergency Management Agency
GAO	General Accounting Office
HAR	Highway Advisory Radio
ICS	Incident Command System
ITS	Intelligent Transportation System
MPO	Metropolitan Planning Agency
MTI	Mineta Transportation Institute
NCHRP	National Cooperative Highway Research Program
NRP-CI	Catastrophic Incident National Response Plan
OEM	Office of Emergency Management
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users
TCRP	Transit Cooperative Research Program
TEA-21	Transportation Equity Act for the 21st Century

SUMMARY

The transportation system is an important network established to ensure the mobility of people and goods between destinations. In addition, it also serves a vital role in responding to disasters, and therefore deserves special attention when those disasters threaten to decrease its support capability. The importance of maintaining this capability is highlighted by the inclusion of transportation system security as a separate planning factor in the 2005 Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users legislation.

Yet the task of securing a transportation system consisting of multiple interconnecting assets is a difficult responsibility. It requires the ability to negotiate the balance between mobility and security in cooperation with multiple stakeholders and interests. It also faces important challenges such as coordinating the various interests and sources of information related to security planning, generating funding for security improvements or operations, and creating standards that ensure security plans exist on compatible platforms.

As an owner and operator of major transportation infrastructure, state Departments of Transportation (DOTs) have a vested interest in ensuring this balance and represent an important mediator between federal and local interests, assuming nine key security planning roles in their traditional transportation planning duties: Coordinator, Analyzer/Planner, Financial Administrator, Infrastructure Owner, Infrastructure Operator, Implementer, Regulator, Information Provider, and Influencer. Through their internal vulnerability assessments, the departments already perform a vital security planning function that can support their own planning efforts as well as others.

Incorporating security into the transportation planning process should be an ongoing effort of the state DOT, requiring modification as feedback of implementation methods is received. It does not mean transforming this transportation agency into a security agency, but rather incorporating a security perspective into the analysis of the system. This first involves establishing a more solid role as a coordinator in order to solidify vital linkages between agencies relevant to security planning. This interaction should reveal standardization issues the DOT can address in order to ensure effective collaboration, communication and coordination. Funding security measures may be difficult; but by incorporating security measures into initial analyzation and planning processes, they can be brought into the broader concept of the system rather than simply added as additional funding needs. The nine roles suggested earlier offer opportunities for state DOTs to overcome these and other challenges faced in the process of incorporating security into the transportation planning process. Through these roles, state DOTs can ensure that security efforts reach the parts of the system that require them and begin to build a more secure system.

Chapter 1:
Introduction

The U.S. transportation system consists of multiple interconnected assets including highways, transit systems, railroads, airports, waterways, pipelines and ports, as well as the vehicles, aircraft, and vessels that interact with these assets. Interdependencies exist between the transportation system and nearly every other sector of the economy, and it provides the backbone for maintaining important public works and government functions. Consequently, maintaining the security of the system is essential to America's continued economic prosperity because a threat to the transportation system can have a broad impact on everything it supports. Bridges alone currently account for a potential $10 billion impact from the loss of one of the 1000 bridges listed as critical to the U.S. (*1*). However, enhancing security can adversely affect mobility. The post-9/11 passenger aviation experience in the U.S. is one example of the delicate balance between security efforts and maintaining mobility, evidenced by the increase in total travel time associated with airport security checkpoints. Maintaining this balance is not an easy task as it involves multiple stakeholders that may complicate and inhibit the security planning process. For instance, despite the relatively quick post-9/11 legislative action supporting transportation security such as the USA Patriot Act and the Homeland Security Act, states are still facing funding issues for surface transportation security improvements several years later (*2*).

As an owner and operator of major transportation infrastructure, state Departments of Transportation (DOTs), have a vested interest in the continued operation of the transportation system as a whole (in contrast to a transit agency for example, whose primary focus is on the local transit system) and therefore are concerned with the system's resilience to multiple types of threats. As a planner and implementer of system components such as Intelligent Transportation System (ITS) technologies and evacuation route models, DOTs also possess the resources to evaluate and enhance the system. Although security planning cannot be left to a single agency due to its complexity, it seems that DOTs have the motivation and ability to unite the various security interests into a unified front; yet they currently do not.

The purpose of this report is to examine the environment in which transportation security planning currently exists at the level of the state DOT, as well as examine any issues or barriers related to the implementation of an effective security assessment and countermeasure program. This analysis involves determining the current as well as possible roles state DOTs assume in relation to other agencies in order to identify where they can be most effective in the security analysis process. Because there is very little existing literature specifically addressing the role of state DOTs in the security planning process, this analysis is based on multiple sources addressing particular issues in security planning as well as interviews with security planning officials at selected state DOTs. Four roles have already been suggested (Owner, Operator, Planner, Implementer), and an analysis of the issues will bring to light other possible roles, as well as allow for comparison of these roles against each other.

The following chapter introduces the conceptual framework that transportation security planning will be examined in, establishing the position of state DOTs in relation to other agencies involved in the same endeavor. Chapter 3 discusses the complications involved in planning for disasters within the transportation environment, specifically examining established emergency response practices among both the U.S. DOT and state DOTs, and their relationship with one another. Chapter 4 then moves to the pre-disaster phase, examining the process of assessing the vulnerability of critical transportation assets. Chapter 5 combines personal interviews of state DOT security planning personnel with recent literature examining unresolved issues in security planning, and uses this information to explore the opportunities for state DOTs to improve this planning through the roles presented in Chapter 2. Chapter 6 provides a summary analysis of these issues, with recommendations following in Chapter 7.

It is important to note that although the term "security" is used, this analysis is not specifically focused on activities developed in response to criminal or terrorist events. Instead, "security" is used here also in relation to the threat of environmental hazards and natural occurrences, representing the degree to which the transportation system and its operators can effectively anticipate and respond to various disasters.

Chapter 2:
Conceptual Framework

Figure 1 shows the relative position of state DOTs with respect to other agencies involved in transportation security planning and emergency management, and defines nine roles the DOT can assume through its authority or function. The National Response Framework, which outlines the principles that guide federal and local agencies in a unified response to emergencies, identifies 38 different agencies involved in disaster response (*3*). However, this discussion is limited to the transportation environment, and therefore is concerned specifically with state DOTs and the agencies it must coordinate with during its planning process.

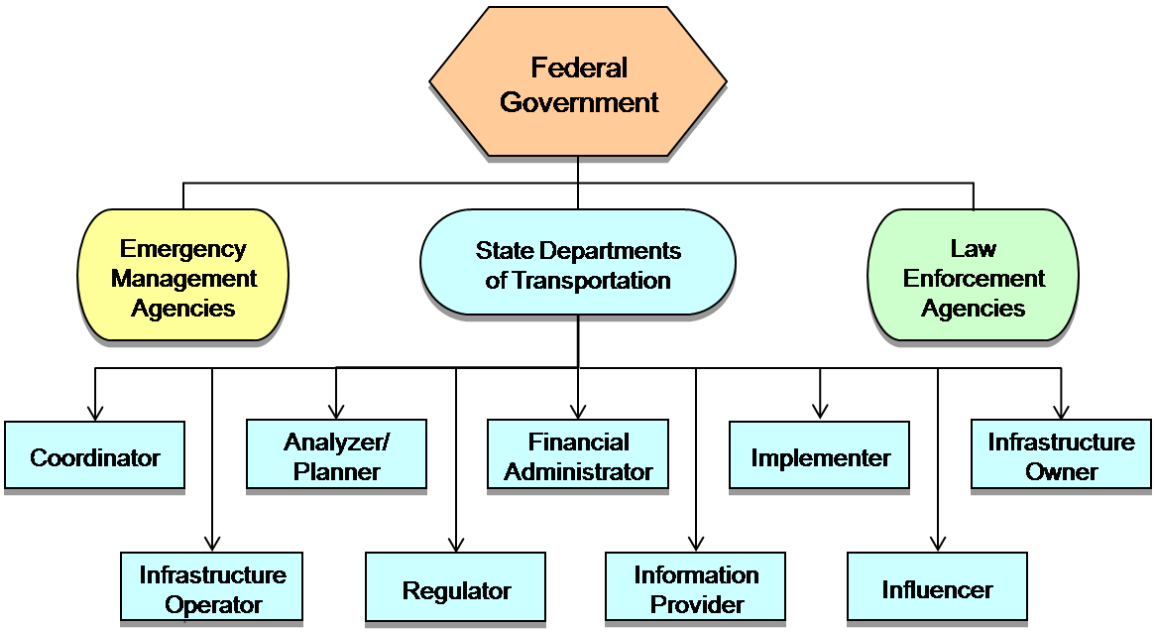


Figure 1: The position and roles of the state DOT Source: Author

The federal government—through agencies such as the U.S. DOT, the Federal Emergency Management Agency (FEMA), and Department of Homeland Security (DHS)—oversees the three agencies directly involved in emergency response planning within the transportation environment (Emergency Management Agencies (EMAs), state Departments of Transportation, and law enforcement agencies), providing general guidance through federal mandates in addition to serving as primary coordinators during national emergencies. In order to plan for their specific role in an emergency, the state DOT needs to coordinate with the state EMA, which establishes the general system for coordinating state response to disasters, and law enforcement agencies, whose security knowledge and expertise helps inform the security planning process. In return, the state DOT can provide critical information to these agencies, the federal government, and

other agencies as to the characteristics of the transportation system during an emergency. In this manner, the state DOT is both influenced by and influences coordinating agencies and federal agencies.

Figure 1 also highlights in blue the nine roles state DOTs assume in ensuring the effectiveness of the transportation system during a disaster. Through coordination with relevant agencies and targeted use of its budget, the state DOT is able to plan and implement strategies to protect its infrastructure and its users during and after a disaster. System analysis allows the DOT to obtain the information it needs to inform disaster response; and by regulating its infrastructure, the DOT is also able to influence the use of transportation infrastructure in accordance with disaster plans. Although these roles may appear hierarchical in the flow chart, in reality this is not the case. However, these roles can be broken up into two categories. Five of these roles (Coordinator, Analyzer/Planner, Financial Administrator, and Infrastructure Owner/Operator) represent opportunities for the DOT to change within its organization in order to more fluidly incorporate security into planning, while four of them (Implementer, Regulator, Information Provider, and Influencer) define how those internal changes will be reflected in a more secure transportation system. A brief description of each role is presented below. A more thorough discussion of these two categories is presented in the analysis and recommendations sections as they relate to the changing role of security in the transportation planning process.

- Coordinator – in the process of serving the public interest and implementing strategies to improve the state transportation system, the state DOT often must bring together multiple interested parties to develop a unified plan supported by multiple modes.
- Analyzer/Planner – in order to implement an effective statewide transportation plan, the state DOT must first obtain and evaluate transportation system information in order to ensure that future projects support a sustainable system.
- Financial Administrator – as the major distributor of transportation funds, the State DOT funnels money from the federal government to important projects.
- Implementer – the DOT not only determines the structure of the transportation system through its planning and analysis, it also influences the transportation environment (both its own and others) through the actual implementation of those plans.
- Infrastructure Owner – the state DOT is the major investor in transportation infrastructure (although other agencies also invest), providing the impetus to protect its investment.
- Infrastructure Operator – the state DOT not only owns transportation infrastructure but also operates it, providing the opportunity to implement operational strategies to security challenges.
- Regulator – by regulating the use of the transportation system that the state DOT owns and operates, it has the opportunity to influence that use as it relates to security issues.

- Information Provider – the state DOT collects and provides information on the transportation system for its own use in planning and operation, but also provides this information to system users and emergency responders in times of emergency to facilitate mobility and recovery.
- Influencer – through its actions in each of the aforementioned roles, the state DOT influences the transportation environment, shaping its ability to effectively respond to disasters.

Chapter 3:
Characteristics of the Transportation Security Planning Environment

Planning for disasters is a complicated and multi-faceted task. Transportation assets are vulnerable to both planned attacks, such as a terrorist or criminal acts, and natural disasters, such as being in the path of a hurricane. Terrorist acts alone represent a difficult planning situation considering the multiple possible objectives of such attacks (e.g. taking lives or destroying economic assets) in conjunction with numerous potential targets, from roadways to railways to airways, etc. Confounding this problem is the difficulty in obtaining information in relation to terrorist threats in comparison to natural disasters, since these actions rely on human decision making rather than a combination of natural occurrences. These kinds of events may even occur without reason, increasing the difficulty in predicting vulnerability.

Planning for a natural disaster is no less complicated. This is represented by the ongoing efforts to characterize and resolve the issues faced during and after Hurricane Katrina (*4*). Natural disasters such as hurricanes or tornadoes carry an additional complexity because their targets may not be as predictable as terrorist targets. In addition, although a natural disaster may not affect the most important parts of the transportation system, the importance of the system as a whole lies in the fact that it is an interconnected system; therefore emergency response may depend on the parts of the system that, though they are not nationally or even locally significant, will hinder the effectiveness of first responders if destroyed in a disaster.

Planning for disasters is further complicated by the characteristics of the system components. Fixed-guideway transit services such as commuter rail and subways offer higher passenger capacity over other methods, but are restricted to particular routes and have little flexibility to respond to an emergency situation on those routes. Highway and road systems offer the redundancy not found in rail systems, but the smaller capacity of individual vehicles coupled with a tendency to underutilize this capacity could also lead to problems during an emergency. The Houston evacuation prior to Hurricane Rita is one example where motorists were trapped on the highway because too many people tried to use it at the same time, clogging the road network and restricting movement for up to 48 hours (*5*). This is not to suggest that a rail system would have fared better, given that its evacuation capabilities are limited by the extent of the rail system.

The complicated nature of planning for a disaster, as well as the multitude of interests and stakeholders involved in responding to disasters, leads to the need to characterize the transportation system and its components in order to effectively plan for an emergency, as well as identify the organizational roles that are required in maintaining the essential functions of the transportation system during disruption. This complexity is reflected at the national level in the consolidation of dozens of emergency-management-related agencies into the Department of Homeland Security; whereas at the local level, "entities become even more numerous and the interactions more complex...typically, no single agency is responsible for transportation security" (*6*). State DOTs hold a crucial position as a mediator between local stakeholders, such as law enforcement, Metropolitan Planning Organizations (MPOs), and federal agencies. For instance, vulnerability

assessments of state transportation infrastructure performed by a DOT can be combined with information from local agencies in prevention and response strategies, as well as funneled to the federal government to prepare for or respond to national disasters.

Many of the elements of security planning, such as vulnerability assessment methods and DOT emergency operations plans, already exist. However, these elements are generally not combined in a concerted planning effort. The Transportation Equity Act for the 21st Century (TEA-21) introduced safety and security as one of seven federally mandated planning factors in 1998, but security was combined with another objective (safety) rather than receiving its own emphasis. Given the relatively small number of domestic terrorism incidents in the U.S. (regardless of their severity), it is not surprising that many DOTs and MPOs focused more heavily on safety than security. The amount of information related to safety incidents is much greater, and much less guarded, than that for security, and the intensity of its use has been a planning fundamental at least since the Highway Safety Act of 1966.

The events of September 11, 2001 elevated domestic security planning and prevention to a priority level, causing many transportation organizations such as the American Association of State Highway and Transportation Officials (AASHTO), the Transit Cooperative Research Program (TCRP) and the National Cooperative Highway Research Program (NCHRP) to review and press for updates to transportation security planning. However, a 2005 NCHRP report that evaluated the extent to which security was considered in the transportation planning process of DOTs and MPOs found "limited evidence that security has yet been given major priority in plans and programs of either the states or the metropolitan areas"(*6*). The 2005 Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) attempted to address this situation by separating safety and security as independent planning considerations in both metropolitan and statewide planning processes. Although security is separated from safety in SAFETEA-LU, it is listed as a secondary benefit of other concerns such as ITS research for information purposes or congestion mitigation, rather than a primary goal with supporting measures. This is not to say that this information gathering is unimportant, but it highlights the fact that little guidance is provided in terms of establishing security planning. Security was also highlighted as a needed component of federal research, but was not given dedicated funding.

3.1 National DOT Security Planning

At both the national and local levels, transportation agencies typically hold supporting roles in emergency response plans as the most knowledgeable source for the information necessary to move first responders into and out of an incident site, evacuate citizens, and generally maintain mobility. Under the Federal Catastrophic Incident National Response Plan (NRP-CI), the U.S. Department of Transportation—in conjunction with several other federal departments such as the Department of Agriculture or the Department of Defense, as well as civilian organizations such as the American Red Cross—is responsible for initiating actions to mobilize and deploy resources necessary to respond to a catastrophic incident such as medical equipment and search and rescue teams. The DOT specifically acts as the Department of Homeland Security's primary source of transportation-related information as DHS initiates the National Response

Framework. Designated as Emergency Support Function #1 (of 15 FEMA designated support functions), the fundamental responsibilities of the Department of Transportation during a catastrophic event include "managing transportation systems and infrastructure, including regulation of transportation, management of the Nation's airspace, and ensuring the safety and security of the national transportation system" (*7*). This annex is provided in Appendix A.

All of these responsibilities are performed under the direction of DHS, and are only begun once DHS has declared a particular incident as "catastrophic." The DOT essentially acts as a point of contact for transportation information, monitoring and absorbing information on the status of the transportation system (including infrastructure) and reporting it to the DHS. The DOT is also supposed to identify alternative transportation solutions in the event that some systems are incapacitated, as well as coordinate the recovery of those systems; however, the response plan specifically states that the DOT is "not responsible for the movement of goods, equipment, animals, or people," and that it is DHS that "is responsible for providing transportation assets and services (including contracts or other agreements for transportation assistance) for responders, equipment, and goods" (*7*). Although state DOTs are a significant source of local transportation-related information, no specific plan for linking the national and state DOT is outlined in this plan, other than the general designation of the U.S. DOT as a coordinating agency.

Under U.S. DOT Order 1900.9, enacted in 2000, the U.S. DOT outlined a somewhat more definitive position and set of priorities before, during and after an emergency. The U.S. DOT states that it will develop and maintain policies that ensure the continued operation of the transportation system, facilitate the repair of any part of the system that is damaged during a catastrophic incident, and provide or make available transportation resources in response to an emergency. The Order designates transportation system disruptions as a specific responsibility of each U.S. DOT employee, and also places responsibility for ensuring communications capabilities for emergency responders on the U.S. DOT. Significantly, this document defines a relationship between the national DOT and state DOTs in terms of both responding to and planning for an emergency. One of the U.S. DOT's priorities is to collaborate with appropriate organizations (such as state DOTs, law enforcement agencies, and other federal agencies) in ensuring that the national transportation system is prepared for emergencies. This document also states that the U.S. DOT will respond to emergency transportation requests in a manner consistent with priorities established by state as well as federal authorities. Federal intervention is still viewed as something to be reserved for significant incidents—just as in the NRP-CI—indicating that local DOTs are still the focal point for transportation-related emergency response until they are overwhelmed. However, unlike the NRP-CI, the U.S. DOT, in addition to outlining the specific roles within its agency, also considers how it will interact with state DOTs affected by the emergency, establishing an important link that will provide the federal agencies with necessary transportation information. Overall, the U.S. DOT retains the same oversight position as that outlined in the NRP-CI, but the position in relation to both local agencies beneath it and federal agencies above it is more clearly defined.

3.2 State DOT Security Planning

State DOTs serve a similar role with regard to State Emergency Response plans, with the exception that it is usually the State Office of Emergency Management (OEM) overseeing the governmental response. The OEM develops an all-hazards plan that provides the same fundamental approach to addressing various types of man-made or natural hazards, defining the roles and responsibilities of the various state agencies and authorities under the direction of the OEM. In addition, modified or more detailed plans are developed for threats that may be specific to certain regions or that require particular attention such as hurricanes or nuclear accidents. These additional plans are called annexes. After 9/11, AASHTO urged many DOTs to include terrorist incidents as an annex because they may require a different response or involve additional support agencies (such as law enforcement) than those already included in the general plan (*8*).

Typically, the OEM will use the Incident Command System (ICS) when responding to emergencies. The ICS provides a common set of objectives and strategies supported by a collective set of management principles, such as unity of command, which solidifies participants under a particular supervisor rather than multiple or changing supervisors, or common terminology, which clearly defines language and phrasing for communications among agencies that may not normally work together. Within this organizational structure, the DOT usually serves as the lead agency for transportation logistics. This means that the DOT should serve a vital role in almost any emergency response, given that most emergencies will require mobile responders, movement of goods and support vehicles, or the evacuation of those affected by the emergency. This effort may involve establishing the condition and potential for mobility along necessary routes, as well as designating the proper routes and restricting or issuing permits for these routes. Because the DOT should be able to characterize effectively the status of mobility along necessary routes, its primary responsibility within an OEM emergency plan is in support of many of the agencies involved in responding to an incident, especially law enforcement and emergency responders. The DOT also provides support in estimating the potential for reconstruction or rehabilitation of the affected transportation system after assessing any mobility restrictions.

3.2.1 State Emergency Operations Plans

Most state Emergency Response Plans list the DOT as one of the supporting agencies in the event of an incident. However, it is one among many agencies, and its specific responsibilities are not always clarified. In response, many state DOTs develop internal Emergency Operations Plans (EOP) that detail the responsibilities within the department as they relate to the transportation system. These plans include general procedures that mirror the state emergency management plan, but also address specific DOT responsibilities and activities in separate annexes. These annexes may include operations center plans detailing the procedure for assigning and notifying DOT personnel to emergency operations centers as well as activating the center, resource management plans providing details on emergency equipment and facilities and how resources can be transferred, traffic management plans detailing the procedures for using the roads and highways for evacuations, and hazard-specific plans that provide

procedures for hazards specific to the area and protocol for dealing with large gatherings of people pre- or post-catastrophe.

As part of the EOP, most DOTs specify the particular role they will assume among four different scenarios: as a first responder to an incident, within the broader context of the particular incident; as a surveyor and manager of the transportation system during and after an incident; and as a source of transportation system status information for the other agencies and the public. The EOP provides the DOT with guidelines to follow once an emergency has been declared, regardless of whether directives have been given and without having to wait for instructions. In a survey of state DOTs, AASHTO summarized the roles DOTs defined for themselves for the four different scenarios (*8*):

First Response

- Assist with evacuation of persons from immediate peril.
- Transport materials, personnel, and supplies in support of emergency activities. Assistance may include transporting resources from state agencies, from local governments from other parts of the state, or from private commercial companies.
- Assist in the design and implementation of alternate transportation services, such as mass transit systems, to temporarily replace transport capacity lost to disaster damage.
- Assess the condition of highways, bridges, tunnels and other components of the state's transportation infrastructure and:
  - Close those determined to be unsafe;
  - Post signing and barricades;
  - Notify law enforcement and emergency management personnel;
  - Protect, maintain and restore critical transportation routes and facilities; and
  - Develop detour routings as appropriate.
- Assess and report impacts to airports, ports, and marine facilities in the disaster area.
- Conduct aerial reconnaissance and photographic missions, provided resources are available.
- Provide hazardous materials containment response and damage assessment.
- Coordinate roadway clearance activities and prioritize and perform emergency repairs in the disaster area. Assist local governments in related repair activities.
- Remove and/or assist in debris removal and disposal, as appropriate, to provide emergency access to disaster areas or to assist in eliminating health and safety problems associated with debris.
- Coordinate state agency efforts in support of utility restoration.
- Issue permits required to repair/restore utility lines or pipes that are immediately adjacent to, or run over or under state highways.
- Provide needed equipment and/or technical assistance in support of the restoration of critical public works.

Concept of Operations

- Implement DOT emergency functions for the prioritization and/or allocation of state resources necessary to maintain and restore the state's transportation infrastructure.
- Provide all available and obtainable transportation resource support including:
  - Transportation equipment, e.g., passenger and utility vans, trucks and/or trailers; aircraft, aircrews, and ground and operations personnel and communications for transportation of emergency officials;
  - Transportation facilities, e.g., vehicle repair facilities, equipment, and personnel; fleet parking and storage areas to be used for staging, parking, and storage of emergency vehicles; motor pool and vehicle service facilities and personnel for refueling and servicing emergency vehicles;
  - Vehicular traffic management and control signs and devices e.g., barriers, cones, of various types;
  - Vehicular traffic flow data and information from permanent and temporary monitoring sites.
- Assign personnel to emergency operations center(s) to coordinate with and assist law enforcement agencies and other agencies involved in evacuation efforts.

System Surveillance and Management

- Monitor and control transportation systems and infrastructure, and coordinate transportation activities with other agencies (local, state, and Federal).
- Provide traffic control assistance.
- Assist state and local government entities in determining the most viable available transportation networks to, from, and within the disaster area and regulate the use of those networks for the movement of people, equipment, supplies, records, etc.
- Identify specific traffic management actions to maintain a smooth flow for evacuation routes and transport of emergency resources, including traffic control points, barricade plans, and potential one-way/reverse lane operations.
- Provide any highway clearances and waivers required to expedite the transportation of high-priority materials and the evacuation of personnel during periods of declared emergencies.
- Coordinate the closure of high-risk roadways such as bridges, tunnels, or flood prone sections of roadway.

Agency Communications

- Provide communications resources in support of statewide operations Public Information.
- Provide information on road closures, infrastructure damage, debris removal, and restoration activities related to highway systems and facilities.
- Provide real-time traffic counter data and traffic reports for roads within the affected area or on roads leading into the area.

- Assign appropriate personnel at key disaster sites to oversee operations and to provide consistent, verified public information to emergency management agencies, public information officers, and the media. When evacuation plans have been implemented, inform motorists which routes and intersections will lead to host shelters.

3.2.2 Continuity of Operations Plans

As the previous list indicates, state DOT Emergency Operations plans typically cover agency operations during and after a major incident, but they do not include plans for carrying out these responsibilities over periods of time longer than the occurrence of the incident or from locations or facilities other than those normally utilized by the DOT. If an incident also disrupts internal DOT operations such that essential functions must be reassigned to different personnel, relocated to an unfamiliar setting, or are rendered impossible, the DOT's Continuity of Operations (COOP) plan is the guideline for carrying out critical services under diminished operating capacity. Because not all incidents will severely incapacitate the internal functioning of a DOT, the COOP plan is enacted separately from the EOP in response to particular events. In the 2005 guide to establishing a COOP, TCRP and NCHRP defined five situations that trigger the use of the COOP, encompassing internal losses that would restrict the DOT's ability to respond to an emergency: "denial of use of facilities, loss of power, loss of telecommunications, suddenly unavailable personnel, or inaccessible information technology systems" (*9*).

Most DOT COOP plans are based on the post 9/11 FEMA circular *Continuity of Operations Federal Preparedness Circular 65*, which defines the COOP as an effort to ensure that agencies continue operating in support or lead capacity under a wide range of emergency situations (*9*). The typical DOT COOP plan outlines a strategy for performing essential functions in the event that facilities, vehicles, systems, or senior management or technical personnel are incapacitated or lost. These functions are vital to ensuring that emergency responders and management agencies are able to perform their duties during an emergency, as well as important in maintaining the safety of civilian system users, and typically encompass the "minimum legal, public safety, operational and maintenance, and public information requirements" (*9*). In order to maintain these functions, DOT COOP plans typically stipulate the formation of a replacement command unit immediately following an event that triggers the COOP plan. In the event that senior management personnel are unable to perform their duties, the unit will be comprised of previously determined personnel assigned to specific functions. This unit is expected to resume essential functions within 12 hours of an emergency, as well as execute additional functions as systems, facilities or personnel become available. The unit may continue its duties for up to 30 days or until normal operations resume, but the plan assumes that the organization will be restored or re-established by the 30-day mark, signifying the temporary nature of the unit.

To ensure the ability to carry out essential functions, COOP planning guides encourage the use and designation of alternative facilities, procedures and personnel. Alternative facilities can include secondary sites where monitoring and management can be performed, separate maintenance facilities that can accommodate vehicles whose garages are destroyed, and separate sites where operating records are stored in case originals are destroyed. COOP planning guides also encourage the creation of alternative

procedures that will be temporarily used to perform essential functions. Examples of these procedures include using transportation and law enforcement personnel to direct traffic if signals do not work, manually running automated train control systems, and giving bus operators pre-assigned routes in the event that communication is lost. The delegation of authority during an emergency is also critical in the development of a COOP guide, since time and communication can inhibit the establishment of a command structure post-disaster. COOP planning guides suggest the development of an order of succession that establishes authority in the event that certain DOT members are lost, ensuring that decisions continue to be made.

Upon establishing a COOP plan, a major factor in the successful implementation of the plan is training. Training DOT personnel in the procedures they will follow during an emergency ensures the quick application of the COOP guidelines, guaranteeing that essential functions will be performed. The lessons learned by various transportation agencies during the events of 9/11 provide examples of how proper training can ensure the execution of COOP objectives. Using alternative facilities to store vital documents in multiple places, as well as within secured online sites, became an unfortunate lesson when critical emergency response plans stored at the World Trade Center were lost. However, it also highlighted the importance of training; transportation and transit employees knew the proper procedures to maintain operations because they had recently completed an all-hazards training exercise that prepared them for the emergency. Training also proved important after multiple lines of communication, as well as the inherent chaotic nature of the terrorist attack, limited the exchange of system updates or directives among transportation personnel. Instead, many relied on the emergency procedures instilled during drills, which resulted in a faster response to the situation and less time wasted in deciding how to respond (*10*).

Once the COOP plan has been triggered, the plan follows three distinct phases: activation and relocation, alternate operating facility operations, and reconstitution. The establishment of the three phases within the plan is intended to focus and organize the attempt to restore the DOT once an emergency has happened. They represent the major objectives of the COOP plan, which is to maintain essential DOT functions while restoring the DOT to normal operating standards. The activation and relocation phase typically occurs within the first 12 hours after the COOP plan has been activated, and consists of notifying the necessary DOT personnel and specific local authorities of their respective responsibilities in maintaining essential DOT functions, as well as moving to the respective alternate locations and requesting any additional equipment or supplies that will be necessary. After this initial 12-hour phase, the alternate facility/work site operations phase can consume the next 30 days. After notifying the appropriate emergency management authorities of the DOT relocation due to the activation of the COOP plan, the majority of this phase consists of re-organizing DOT personnel. Employees not accounted for during the initial emergency are processed as they are received, and responsibilities are transferred to these employees according to the plan. Some employees' responsibilities may shift in accordance with the plan, and some employees may need to act as replacements for missing personnel, and these employees are guided through this process (although no information is given in the planning guidelines as to whose responsibility this is). As the situation becomes more stable, a redeployment plan is developed with the intention of phasing down the alternate facility,

leading to phase three. The reconstitution phase consists of informing all personnel of the termination of the COOP plan and the return to normal DOT operations. This phase may or may not consist of returning to the original facility, depending on damage, but is intended to involve the establishment of a permanent facility.

Chapter 4:
Assessing and Quantifying Vulnerability

The previous chapter focuses on the reaction of state and national transportation agencies to a disaster through emergency operations planning. This planning requires an understanding of the consequences of the loss of important sections of the transportation system on area recovery, which necessitates an examination of vulnerabilities. The possibility of losing a transportation system component is an important factor in the consideration of transportation alternatives for emergency response and aid personnel, and may be preventable through proper foresight. This chapter discusses one common method for determining the most vulnerable and critical assets within the transportation system as compiled by AASHTO.

4.1 Vulnerability Analysis

In response to the heightened state of awareness to transportation security following the terrorist attacks of September 11th, 2001, NCHRP funded the development of a resource for highway vulnerability assessment for use by state DOTs. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, produced in 2002, was intended to assist state DOTs in improving their security planning against terrorism by outlining a procedure for assessing the vulnerability of a wide range of physical assets to terrorist threats, developing countermeasures to those threats, and estimating the capital and operating costs of those countermeasures (*11*).

The guide was intended for use by any state DOT and applicable at all levels of DOT staff, from the executives initiating the assessment process to the employees conducting the assessment. The authors also intended for it to be useful to states already performing vulnerability assessments by offering the guide for comparison against current plans, allowing a state DOT to either validate an existing approach or bring it up to the standard proposed in the guide. For states in the early stages of developing an assessment process, the guide references other states' performances of the outlined procedures, providing descriptions of how other states apply these principles as well as issues and challenges newcomers should be prepared to face.

The guide assembles the vulnerability assessment process into three major phases:

I. **Pre-Assessment** - this phase involves planning and scheduling the vulnerability assessment process. An assessment team is assembled and led through training exercises to prepare for the assessment. Any resources necessary for the assessment are collected and external agencies with security or emergency response knowledge and capabilities, such as law enforcement or fire services, are contacted for support.

II. **Assessment** – in this phase, the vulnerability assessment of the system is performed. This process involves determining the criticality and vulnerability of particular components, leading to the identification of key components requiring further countermeasures to ensure their continued functioning during, or quick recovery from, a disaster.

III. **Post-Assessment** – once the assessment has been completed, cost-benefit analyses and trade-off studies can be used to determine a strategy for implementing the recommended countermeasures.

During the process of assembling a team for the vulnerability assessment, the guide suggests that members be recruited from different sections of the DOT. This will include departments with obvious assessment-related experience such as the construction division, design division, materials testing division, traffic operations division, and environmental management division, but should also include departments such as budget, purchasing, communications, and human resources among others. This provides a varied perspective on the criticality as well as the vulnerability of each section of infrastructure beyond physical measures. It also means early involvement of important personnel who may be critical to assessing the viability of countermeasures, which can increase the speed and efficiency of decision making.

The major portion of this guide is devoted to an explanation of the vulnerability assessment process. Although the guide was written specifically for terrorist incidents, the process can be broadened to include natural disaster preparedness, since the ultimate goal is to prepare for and respond to a disruption in the transportation system. Preparation for terrorist incidents is hampered by their inherent unpredictability in terms of when, where and how a terrorist will act. The intent of the vulnerability assessment process is to determine the where and how by identifying potential targets within the transportation system and determining what is required to disable those targets, leaving the "when" to law enforcement agencies or security authorities (*12*). Non-terrorist incidents may alleviate some of this uncertainty through a modicum of predictability (such as tracking hurricanes during hurricane season or monitoring nuclear reactors) and a level of understanding through methodical examination of previous incidents. However, all incidents have the potential to cause damage to the transportation system, regardless of the ways or extent to which the damage occurs. With this in mind, the vulnerability assessment process should account for both terrorist and non-terrorist threats in the process of evaluating the vulnerability factors.

The following six subsections follow the outline for phase II of a vulnerability assessment process as described in *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* (referred to as the guide), though each subsection may include a discussion of relevant issues or input for the process from other sources as noted. The process is guided by three basic goals: determining the likelihood that an incident will occur as well as the components likely to be affected, assessing the system and determining the amount of damage that may be caused, and then assessing the impacts of a component failure and the possible countermeasures to that failure. The process is intended to be iterative, acknowledging that assessment results—as well as new information—change risks, and therefore require periodic updating (*12*).

4.2 Critical Asset Identification

The assessment process begins with an identification of the assets that are critical to maintaining the essential functions of the DOT. The guide divides these assets into four categories: infrastructure, such as roads or bridges; physical facilities, such as headquarters buildings or traffic operations centers; equipment, such as variable

messaging systems or traffic signals; and employees, which includes non-government employees such as contractors and vendors. Criteria for establishing the criticality of the asset must be determined by the DOT, and each of these criteria must be given a weight to prioritize it among the other criteria. This does not mean that one criterion must outweigh another, which would indicate that the criteria are ranked; instead, the degree to which the criterion influences labeling an asset as critical determines the weight it is given, meaning that multiple criteria could have the same influence and therefore the same weight. For instance, the risk of casualties and importance to emergency response capabilities are two criteria that could be weighted the same as they are both severe consequences of an incident. The guide suggests assigning weights ranging from 5 (extremely important) to 1 (less important).

Asset redundancy is an example of one criterion that can be used to establish criticality because some components such as bridges and rail lines are usually one of only a few options for their purpose (*13*). Redundancy can also include personnel, which ensures that particular functions and responsibilities are carried out if particular personnel are lost or unable to carry out their duties, and the equipment needed to carry out the functions of the DOT during and after and emergency. Facility redundancy was a major issue during the 9/11 terrorist attacks because the Emergency Operations Center, with all of the emergency protocol documents, was located in the World Trade Center. After this building was destroyed, those involved in the response and recovery effort had to rely on training in order to carry out any plan because they did not have any guidelines (*10*).

Once the criteria have been weighted, every asset is assessed for every factor on a "yes" or "no" basis (either the asset does or does not meet the criteria). In this manner, each asset that meets the particular criterion is given the same weighted value for that criterion, regardless of the extent to which the criterion applies. For instance, if factor "A" weighted at a value of 4 applies to a particular asset, that asset receives a 4; if it does not, then that asset receives a 0. This is an attempt to mitigate subjectivity in the determination of asset criticality. The subjectivity lies in the designation of weight for the criterion, which should be agreed upon by knowledgeable professionals. Once the weight is established, it does not vary for each asset; either the criterion applies and it receives the corresponding weight, or it does not. For instance, the casualty risk is given a particular weight, and this weight applies whether one life may be lost or one thousand. The asset itself is not given a value based on the extent to which lives may be lost, which could be different than another asset, assuring consistency among assessments for all of the assets.

Certain factors may only apply to assets to a certain degree, and therefore the guide does suggest introducing a gradient for a particular criterion by splitting the criterion into moderate, major, etc. For instance, a state may decide that a moderate economic impact as a result of the loss of an asset may be easier to contain or rebound from than a major impact, which should be reflected in the prioritization of assets. The DOT needs to differentiate between a major economic consequence and a moderate economic consequence, and can do so by introducing both factors and weighing them according to the DOT's perception of severity. However, the guide warns that the introduction of gradients may complicate the process by increasing the number of judgments required during the assessment.

Once each asset has been assessed, the criticality weights are tallied for each asset, and, according to the guide, are divided by the total possible weight. The projects are then ranked by percentage. Some DOT's may define a particular cutoff point at which no further consideration will be given to the asset, in order to reduce the number of assets that will be considered over the entire process, which reduces time and cost. At the end of this process, the DOT may have a table similar to Table 1 below, which was taken from a hypothetical example in the guide.

Table 1: Example criticality scoring table

CRITICAL ASSET	CRITICAL ASSET FACTOR														TOTAL SCORE (x)
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	1	*2*	*5*	*1*	*3*	*3*	*5*	*5*	*5*	*4*	*1*	*5*	*2*	*1*	
Smith Bridge	1	2	5	1	3	3	5	5	5	4	1	5	2	1	43
Bayside Tunnel	1	2	5	1	3	3	5	5	5	4	1	5	2	1	43
Blue Bridge	1	0	5	0	3	3	5	5	5	4	0	5	2	0	38
Crystal Bridge	1	2	5	1	3	3	0	5	5	0	0	5	2	1	33
Interstate 1	1	2	5	1	3	3	5	0	0	4	1	5	2	1	33
Interstate 218	1	2	5	1	3	3	5	0	0	4	1	5	2	1	33
Interstate 88	1	2	5	1	3	3	5	0	0	4	1	5	2	1	33
Rt. 49	1	2	5	0	3	3	5	0	0	4	1	5	0	1	30
Rt. 6	1	2	5	0	3	3	5	0	0	4	1	5	0	1	30
Johnson Interchange	1	0	5	0	3	3	5	0	0	4	0	5	2	0	28
Headquarters Building	1	2	0	1	3	3	0	0	0	0	1	0	2	1	14

Source: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

In this table, the assets are listed on the left. The criteria developed by the assessment team are listed across the top according to their corresponding alphabetical designation. For instance, in this table "A" corresponds to "Ability to Provide Protection," "B" corresponds to "Relative Vulnerability to Attack," "C" corresponds to Casualty Risk," "D" corresponds to "Environmental Impact," "E" corresponds to "Replacement Cost," etc.. Although these factors are used here for example purposes only, the full list of factor values is given in Appendix C. Below the criteria are the corresponding weights determined by the assessment team. Note that within their respective row, each asset either receives the weighted score if they meet the criteria, or receives a "0" if they do not. These weights are then summed to a total score on the right and used to rank the projects. The more factors that are associated with a particular project, the higher the total score will be. At this point, the assessment team can decide to eliminate projects that do not meet a certain threshold based on their expertise with the assets and knowledge of DOT needs (*11*). The total score will be combined later with the vulnerability assessment to prioritize projects for countermeasure application.

4.2.1 Criticality assessment issues

Different assets represent varying levels of criticality, and the criticality assessment step is an attempt to quantify those differences. However, applying these weights in a binary fashion may not provide a complete picture of criticality issues. The guide does mention using a gradient when one factor does not fully represent the level of variation possible with the factor (such as varying levels of economic impact), but a different option (similar to the process of evaluating vulnerability, shown in the next section) involves establishing the likelihood that each criterion will happen for each asset. Criticality is instead represented as a scale, and the values of each factor can be evaluated on that scale. Using loss of human lives as an example factor, Table 2 represents possible scaled values, with 5 incurring the most loss and 0 representing no loss:

Table 2: Example critical asset factor scale

Critical Asset Factor	Values	Score
Human Loss		
High loss (50 or more deaths)	5	
Moderate-High loss (20 – 49 deaths)	4	4
Moderate loss (10 – 19 deaths)	3	
Low-Moderate loss (5 – 9 deaths)	2	
Low loss (1 – 4 deaths)	1	
Human loss unlikely (no deaths)	0	

Source: Author

Table 2 shows that this particular asset scored a value of 4 for the factor, which would then be combined with other factor values (evaluated the same way) for a total criticality score that more fully represents difference between critical transportation elements.

Another option would be to keep the weighted values for each factor, and in addition determine the probability of a particular transportation asset being affected by an event. The assigned weight for the respective criterion is then multiplied by the determined probability value, and the adjusted criterion values are totaled for the asset. The criticality factor retains the same weight determined at the beginning of the process, meaning the relative importance of that factor to the DOT is maintained throughout the process; but combining it with the probability of the factor occurring increases the accuracy of those weights in relation to other assets.

It is important that the process for determining a likelihood scale or probabilities is objective. England's Highways Agency uses a manual that provides probabilities associated with four factors involved in the calculation of risk of failure for highway structures: causes of failure, defects that may result in failure, degree of exposure to threats, and effect of these previous factors (*14*). The agency determines the probabilities for various conditions based on historical data before issuing look-up tables for reference when a particular asset is being evaluated. Multiple components within each factor are considered in the establishment of the factor's probability, which is then applied to the following equation:

L(Risk Event) = L(Cause) x L(Defect) x L(Exposure) x L(Effect)
Where L = Likelihood

Combining these four factors results in a value representing the likelihood of a risk event occurring based on pre-determined probabilities, which is then evaluated within a range of 0 (possible, but not likely) to 1 (certain).

If a manual is not available, another option is to use the Delphi method of consensus building. The Delphi method incorporates personnel with expertise related to the established criteria from the DOT as well as relevant agencies, including law enforcement and emergency response. The carefully selected panel is involved in an iterative group communication process, providing feedback through each individual's anonymous contribution to particular problems. During the process, each person is given a questionnaire, and the subsequent answers are displayed anonymously so that participants can either modify or retain their responses in light of the responses of the group. Each questionnaire and subsequent collation of answers represents a round, and the process can go through multiple rounds until reaching a pre-determined zenith, such as a particular number of rounds or a convergence of responses (*15*). However, the Delphi method does not guarantee a consensus for each subject because strong opinions may tend to polarize during the process, though this polarization does mean that points of contention can be highlighted and brought out into open discussion (*16*). The key benefits of this process include the removal of the negative effects of confrontation or group dynamics in decision making, the inclusion of constant feedback that contributes to the ability of a participant to reevaluate their opinion, and the degree of anonymity that allows participants to both freely critique other's judgments and openly admit to errors in their own judgment. This process is not without its "pitfalls," such as the possibility of using false feedback to manipulate participants, or inducing a false consensus by ignoring or downplaying disagreements (*17*).

4.3 Vulnerability Assessment

After identifying critical assets, a vulnerability assessment is performed on those assets in order to determine the possibility and extent to which each asset could be damaged during an incident. The assessment also considers the harm that may come to users of those assets—such as transit passengers, drivers or employees—as well as damage to any element involved in monitoring and managing the operation of the system.

The process begins with a determination of the threats to the asset. These threats may be natural, such as tornadoes, earthquakes, or floods. Generally, these conditions are known to the region and the asset's designers, and the assets are built to resist these natural occurrences. Acts of terrorism are more unpredictable than natural incidents in terms of determining when they will happen (a lack of previous threats or actions does not guarantee safety for the future), though the specific targets may be easier to predict given that terrorists generally have reasons for choosing those targets. Because terrorist incidents generally require additional considerations and are usually accounted for in a separate annex to security plans, they are discussed later in this section.

Vulnerability can be linked to several factors. One factor is the structural stability of the physical components of the system, including roads, railways, bridges and buildings. Structural stability is a straightforward factor to assess because the DOT

should already possess knowledge of the materials and structural elements used in the design of the particular asset. Structural information is also static information, meaning that the elements of the structure usually do not change. Although materials do deteriorate and structures can deform over time, these characteristics can be accounted for and factored into the vulnerability assessment. However, it is important to note that data may be collected from multiple sources, depending on the asset. This can lead to compatibility issues between data sets, resulting in extra time needed to link the data together in order to provide useful results. This provides an opportunity for state DOTs to intervene as system regulators and process implementers by organizing and ensuring the consistent use of an effective data format that can be easily transferred among agencies, reducing time and confusion (*12, 18*).

The availability of response resources is highly important in the consideration of the vulnerability of an asset, in terms of both the initial response to the incident and the subsequent recovery. The fast and efficient response to a disaster by emergency personnel can determine the number of lives saved or lost, which, as discussed earlier, can affect the number of personnel available for a recovery effort if a significant DOT facility is attacked or destroyed. This response effort is influenced by the number of resources available, as well as the quality and type of resources, which is true of both the emergency responders and the DOT personnel. This relates to the concept of redundancy in that the more personnel available, the less likely that all of them will be lost in a major catastrophe. Also, more highly trained personnel will be able to more quickly react to an incident, increasing the probability of a successful recovery from an incident. The relative location of critical assets to emergency responders, as well as the distance from facilities (both DOT and private) that are influential to recovery efforts is another important consideration. No matter how many or how effective emergency response personnel are, if they are a great distance from an important asset it will be more difficult for them to respond quickly to the incident. Likewise, the time required to replace or restore an asset is influenced by the time it takes to get the necessary equipment and materials to the site.

Terrorist activities involve additional vulnerability considerations that are exemplified by the separate terrorist annexes typically found in emergency response plans. The annexes are also characterized by the addition of particular law enforcement agents among the list of cooperating agencies, as well as the need for additional countermeasure techniques for preventing attacks, such as biometrics or crime prevention through environmental design (CPTED) (*7*). Planning for terrorist incidents generally involves a consideration of the amount of effort required to disable or destroy a target. One factor in this is the accessibility of the asset, which is a major consideration for transit systems due to their inherent openness. Another is the aforementioned structural stability, because knowledge of the materials and design of the structure influences the understanding of the ways and means to destroy it. The amount of security, surveillance, or other attack deterrents at the asset also influences the requirements for a successful attack. Other factors that influence terrorist incident planning include the symbolic importance of the asset, of which the 9/11 attacks on the World Trade Center and Pentagon are examples; and the frequency and volume of users, of which the 1995 Sarin gas attack on the Tokyo subway and the 2004 Madrid train bombings are examples.

Once the factors associated with vulnerability have been established, values for those factors must be determined in order to compare them with the criticality factors; however, this process does not involve the same weighting process performed in the criticality assessment. The AASHTO guide (which only considers terrorist incidents in its account of the vulnerability assessment process) proposes assigning values ranging from "extremely important" (5) to "less important" (1) for paired subsets of vulnerability factors. For instance, the proximity of vehicle access points is paired with the level of security at the asset because both characteristics are part of the overall accessibility of the asset. Values ranging from 1 to 5 are assigned by the assessment team for each of the two sub-factors of accessibility (proximity and security level), and then multiplied together to get the respective factor value. The overall vulnerability value is then determined as the sum of each of the vulnerability factor values, which can be seen below in Table 3, taken from a hypothetical example in the guide. Table 3 shows how factors such as access proximity (labeled as "C") and level of security (labeled as "D") are combined, then added to other paired factors for each asset. A full list of these example factors is given in Appendix D. The sum of these combinations gives the total vulnerability score on the right.

Table 3: Example vulnerability scoring table

CRITICAL ASSET	VULNERABILITY FACTOR											TOTAL SCORE (y)
	(A	*	B)	+	(C	*	D)	+	(E	*	F)	
	1-5	*	1-5	+	1-5	*	1-5	+	1-5	*	1-5	
Smith Bridge	5		2		5		5		4		2	43
Bayside Tunnel	4		5		4		3		3		2	38
Blue Bridge	3		4		3		5		5		3	42
Crystal Bridge	2		3		4		3		2		4	26
Interstate 1	4		2		3		4		4		5	40
Interstate 218	3		3		4		4		2		4	33
Interstate 88	4		4		3		3		4		5	45
Rt. 49	5		5		1		3		5		2	38
Rt. 6	3		3		3		4		5		3	36
Johnson Interchange	2		4		2		4		1		4	20
Headquarters Building	5		5		1		5		3		2	36

Source: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

4.3.1 Vulnerability Assessment Issues

One issue in this step of the process is that sub-factors that should be considered individually are combined with other related, but possibly distinct factors, overemphasizing their interdependence as well as equalizing their severity. For instance, in determining the vulnerability of an asset to a terrorist attack, the number of users for an asset is combined with the level of visibility. Assets with high visibility and a large number of users are considered more vulnerable than less visible assets with few users, a plausible perspective with respect to terrorism. However, either factor could

independently be a strong reason for a terrorist attack, given that terrorists have different agendas. The terrorist attack may utilize a recognized target or a large number of casualties to incite terror, and combining these two factors may reduce their significance. As an example, assume we are evaluating two sites (A and B) based on the AASHTO guide, one with a high level of recognition/low attendance and one with medium recognition/medium attendance. Using Table 4 below, site A would receive two separate values, a 5 and a 1, and site B would receive a 3 and a 3. Table 4 is taken from a hypothetical example in the guide.

Table 4: Factor values for Recognition and Attendance

Visibility and Attendance	LEVEL OF RECOGNITION (A)	1	Largely invisible in the community
		2	Visible by the community
		3	Visible Statewide
		4	Visible Nationwide
		5	Visible Worldwide
	ATTENDANCE/ USERS (B)	1	Less than 10
		2	10 to 100 (Major Incident per FEMA)
		3	100 to 1000
		4	1000 to 3000
		5	Greater than 3000 (Catastrophic Incident per FEMA)

Source: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

In this example, because combined values are multiplied together, site A receives a factor value of 5 (5 x 1) while site B receives the higher value of 9 (3 x 3). Although site A may be a more desirable target due to its high visibility (similar to the Eiffel tower or Washington monument), Site B, with lower visibility and a moderate possibility of casualties, receives a value almost double that of site A. Now consider using these same default values, but adding them rather than multiplying them, and the two sites would be equal (5+1 and 3+3). This seems a more appropriate comparison of the desirability of these two targets. In essence, combining factor values can either add unnecessary emphasis on or reduce the appropriate valuation of a particular factor.

4.4 Consequence Assessment

At this point in the assessment, the critical assets have been identified and their respective level of vulnerability has been determined. However, not every critical asset will have the same level of vulnerability, and those that are more vulnerable will require more consideration. The purpose of the consequence assessment is to determine the most vulnerable assets reaching a predetermined threshold. This is accomplished by plotting the criticality of the asset against its vulnerability.

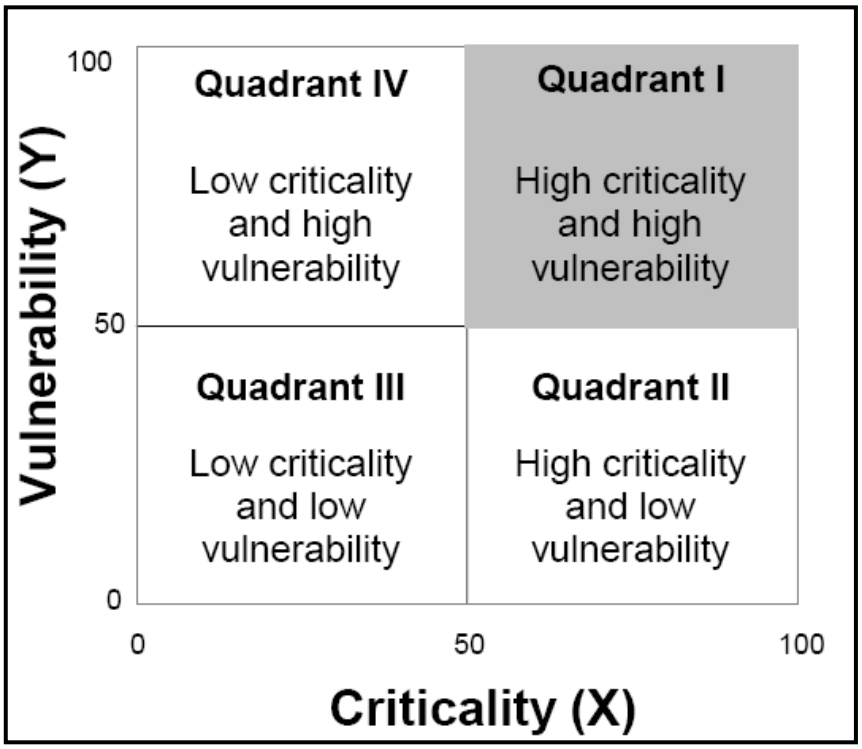
Using the method prescribed in the guide, the criticality and vulnerability values determined earlier in the assessment process are normalized by their respective maximum values:

$$\text{Normalized criticality of asset n} = X_n = (C_n / C_{max})*100$$

$$\text{Normalized vulnerability of asset n} = Y_n = (V_n / V_{max})*100$$

The base values now represent percentages of the maximum possible criticality or vulnerability. Representing these values as percentages reflects the effort in determining the factors for criticality and vulnerability; because the individual factors have already been imbued with a level of severity or influence during their formulation, X_n and Y_n represent the extent to which each asset is critical or vulnerable respectively. Also, by normalizing vulnerability and criticality they are placed on a scale of 0 to 100 by which they can be compared.

The comparison of the two values is usually represented in a plot of the X and Y values for each asset, which is shown on the next page in a plot taken from the guide (Figure 2).



Source: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

Figure 2: Vulnerability versus criticality and the four quadrants of consequence.

Plotting the value provides a visual representation of the ranking of one project against another. According to this figure, any asset with X and Y values of 50 or higher is of greater consequence to the DOT than projects falling into any of the other quadrants, and therefore requires countermeasures to mitigate the impacts of an incident. The level at which these quadrants are set can be determined by the DOT prior to the assessment in order to meet with DOT goals in terms of fortifying critical assets or reducing vulnerability. This does not mean that assets falling into other quadrants do not require

attention; the process is simply meant to provide a means by which different assets can be compared.

4.5 Countermeasures

Once priority assets have been determined in the consequence assessment, countermeasures to the possible incidents need to be proposed and evaluated. This is a crucial step in the assessment process because all prior efforts to determine the vulnerability of critical parts of the transportation system are wasted if an attempt to improve the system is not made. However, this may also prove to be the most difficult step in the process. The difficulty at this juncture is a result of the fact that developing countermeasures can be an involved and complex process, considering that most approaches involve a layered system of detection, defense and response. Applying a layered response means that each component is dependent on the other two, so success depends on the proper development and application of all three. These three components are often performed in cooperation with external agencies, which adds to the complexity by requiring the coordination of joint efforts. Further aggravating the issue is the fact that countermeasures require funding, and the choice to pursue a particular countermeasure will most likely mean sacrifices in other transportation projects.

DOT involvement in the security planning process does not end at the beginning of countermeasure selection; yet for external agencies involved in security countermeasures such as anti-terrorism task forces or earth-quake monitoring stations, the transportation system may not be its primary security concern as it would be for a state DOT. Their focus may involve only one of the three components, detecting, defending, or responding to the event. Local transportation agencies' focus may only be concerned with threats in particular areas or on particular modes. To ensure the security of the transportation system, the coordination of relevant parties will most likely fall to the state DOT. This is an important role because the different responsibilities will require outside input for success. For instance, emergency responders need route information to determine the best possible choice—as well as the best alternative in the event the route is lost—for getting to the scene of a disaster quickly. Likewise, terrorist information from law enforcement agencies or weather information from reporting agencies is crucial to determine those assets that are more likely to be damaged.

Funding is another crucial issue that will require a champion. Security-related personnel or technologies will not be provided out of good will, and local agencies such as MPOs or transit agencies generally look to state DOTs for funding. State DOTs possess more resources for acquiring funds than local agencies (though it is not an easy task), and have an established relationship with the federal government that provides a platform to lobby for increased security funding. However, obtaining this funding is not a simple or reliable process. The issues associated with gaining the necessary funds, as well as other issues involved in security planning, are discussed in the following chapter.

Chapter 5:
Issues in Transportation Security Planning

The vulnerability assessment process is crucial to enhancing the security of the transportation system, and it is a large but necessary responsibility of the state DOT. But the process has several problems, including data compatibility issues, problems associated with the prescribed methods of weighting factors, and issues with subjectivity influencing the process. The final countermeasure selection step is the most significant part of the vulnerability assessment process because it is the application of the knowledge acquired from assessing the infrastructure. This step also raises issues, and the problems associated with it hinder the effectiveness of other parts of the process. Highlighting these issues sheds light on areas where state DOTs can assume stronger roles in ensuring the security of the transportation system.

Using published reports on security planning issues as well as interviews with DOT personnel, this chapter reviews some common issues with the vulnerability assessment process. California, New York, Virginia, Maryland, North Dakota, Florida and Ohio were selected for use in this analysis based on factors such as relative exposure to natural or man-made threats, availability of planning information and complexity of the planning environment. For example, California presents a complex planning environment due to characteristics the multiple types of hazards that can occur across the expanse of the state; whereas Maryland presents a contrasting planning environment that focuses on fewer issues. The interview questionnaire can be found in Appendix B. Although multiple personnel were interviewed for this report, interviews are not specifically referenced in this section for two reasons: first, some information provided was used for analysis purposes in this report, but was not intended for public dissemination; and second, most respondents reiterated issues found in literature used in this report, so the literature is primary used as the source and cited here.

5.1 Funding

Implementing countermeasures to natural and man-made disasters is one of the most important steps in the vulnerability assessment process. Gathering important information on structural vulnerability or possible terrorist threats to particular transit systems means very little if that information is not used to protect transportation assets and their users. As Chapter 4 showed, there are various types of countermeasures, from infrastructure development, to technological enhancements, to increases in personnel; however, one common thread among these measures is that none of them are free. State DOTs play a large and important role in assessing and planning for the vulnerabilities of their transportation systems, but they can do very little about those vulnerabilities without sufficient funds. One of the most important roles state DOTs can assume in the overall security planning process is as a financier. This role may mean securing and providing funds dedicated to security measures through in-state legislative measures or new funding mechanisms, just as many states have become more creative in securing funds for their general projects when faced with a budget crisis due to factors such as the decrease in

gasoline tax revenue. This role may also involve serving as the spokesperson to the federal government in attempting to secure more dedicated funding for transportation security projects, considering that local funding may not be sufficient.

The events of 9/11 brought transportation security into the forefront of national policy and local concern, and the subsequent attempts to increase the amount of security planning and practice to prevent terrorism provide multiple examples of the funding issues DOTs face in trying to implement security strategies. In a 2003 report on the post-9/11 efforts to enhance the security of highways and transit systems, Howitt and Makler found that although the aviation sector had greatly improved its security measures as a result of the Aviation and Transportation Security Act, "surface transportation has been effectively placed in a secondary tier of public services in terms of protective actions" (*2*). Although most would agree that highways and transit systems are vulnerable to attack, even the heightened state of security awareness following 9/11 could not guarantee dedicated security funding to support terrorist countermeasures for surface transportation. Instead, funding was focused on four aspects of security planning and emergency response: airline security, intelligence/law enforcement, emergency medical and public health infrastructure, and emergency response personnel training.

Each of these factors is an important consideration in security planning and recovery, and it is expected that they would be the focus after an event such as 9/11. Health infrastructure and response personnel training both represent a focus on the aftermath portion of security planning. These factors come into play once a disaster has happened and the focus is shifted to recovering from the disaster and mitigating the loss of human lives. It is a very important consideration in the planning process because no plan is guaranteed to work completely. Intelligence gathering and law enforcement services are an integral part of the initial planning spectrum because they provide the information concerning an impending disaster (in this case a terrorist attack) as well as serving the important role of deterring or capturing those responsible. Any authority would likely enhance the focus on intelligence and law enforcement given this event to both prevent another attack and catch the terrorists.

The focus on airline security is also a likely response to terrorism because it is now necessary to both ensure that the event does not happen again and assure passengers that it is safe to fly to keep the system functional. This initial attention is a natural reaction, yet it essentially places the entire burden of transportation security on one component of the system. Providing money for intelligence gathering or emergency response personnel supports all aspects of disaster planning and response. Yet the post-9/11 funding initiatives focused only on one possible way terrorists could use the system to their advantage. If a terrorist intends to do harm in an open or broad manner, the multiple reasons the transportation system is a good target have already been discussed; and as a system, there are multiple components that can be exploited. Although initially focusing on airlines is an appropriate response given the environment, successive funding opportunities should enhance the ability to secure the whole system rather than a single part.

Initial efforts to increase the amount of funding available for transportation security have fallen short (*2*). Several post-9/11 bills passed by Congress, such as the USA Patriot Act and Homeland Security Act, provide general-purpose grants to states for security functions, but do not provide dedicated funding, forcing security needs to

compete for the same funding as traditional projects. Because many states initially perceived that the federal government would or should provide dedicated homeland security funds for transportation security, they were often reluctant to tap into general purpose transportation funds for something that may be perceived as a security enhancement, despite the heightened emphasis on security after 9/11. However, providing federal general purpose homeland security funds further complicated the issue when other agencies such as intelligence agencies, first responders or public health agencies, who were seen as traditional users of these types of funds, established competitive claims for the same funds transportation agencies were seeking (*2*). The early stages of funding for security planning can therefore be characterized as a catch-22, with transportation agencies reluctant to dip into transportation funds, which inhibits the ability to complete other traditional projects, but unable to compete for dedicated security funds.

Although the Transportation Security Administration is responsible for the security of U.S. highways, railroads, buses, mass transit systems, pipelines, ports, and 450 U.S. airports, only 1% of the $6.8 billion budget proposed under the Department of Homeland Security Appropriations Bill (S. 3181) was devoted to surface transportation security. This equates to $47 million, while aviation security received $4.8 billion, or 71% of the budget. Of this $47 million, only a portion goes to implementing specific countermeasures as a part of the overall security environment, including vulnerability assessments, information sharing resources, and security exercises. This asymmetry is not specific to the TSA, but is instead a broader symptom of the funding problem. In a 2002 General Accounting Office (GAO) survey of 155 transit systems concerning federal involvement in transit security planning, increased funding was cited as the most important role the federal government could play in assisting transit systems with security planning (*19*). But simply providing dedicated security funding is not a clear-cut solution. Among the principle findings of a 2005 Mineta Transportation Institute (MTI) report on transit security in the U.S., the MTI found that although the threat to transit systems is usually aimed at systems in the largest and most politically and economically influential cities, this is at odds with "a political system of public finance that favors distributing funding somewhat equally across jurisdictions" (*20*). The authors conclude that rather than focusing on the most critical (and therefore most likely to be targeted) systems, Congress will continue to distribute funds "equally" in a manner representative of the ethos of public finance and jurisdictional accountability. Although this system may simply seem unfair when per-rider transit subsidies are much higher in smaller cities than transit-heavy cities like New York or San Francisco, it becomes a travesty when it undermines the effective implementation of security plans in vulnerable systems.

It seems apparent that state DOTs cannot currently rely specifically on federal funding to support their security plans; and although events such as the world trade center terrorist attacks and Hurricane Katrina bring national attention to problem areas in security planning, it does not necessarily bring immediate solutions. Instead, DOTs must assume a more proactive role in terms of both procuring the federal funds that are available—just as they do with federal sources for traditional transportation projects—and developing new sources of revenue. The introduction of security as a separate planning factor through SAFETEA-LU guidelines may mean that countermeasures will be incorporated as integral parts of transportation improvement programs, so that security

features are integrated into new construction. Countermeasures could also be funded through user fees similar to congestion or distance-based pricing, given that users may be more inclined to pay for their safety and security over the ability to save time during their commute (a charge many have become used to from airline travel). Regardless of the means, it is clear that state DOTs must lead the effort to procure financing for security countermeasures, or else mandated security planning efforts could be fruitless without money to implement them.

5.2 Coordination

Security planning is an extensive process involving the coordination of multiple departments within a DOT as well as external agencies. As the owner and operator of the largest portions of state transportation systems, state DOTs have a vested interest in ensuring the safety and security of transportation infrastructure that extends beyond simple responsibility. To do this, DOTs cannot act alone; they need transportation data from local agencies in conjunction with their own, and they need information specific to law enforcement agencies to better understand threats against their systems. In collaboration with these various interests, the DOT needs to maintain a balance between security and mobility. Law enforcement agencies may tend to stress the importance of deterring threats and keeping the system safe, and no DOT would want to see the destruction of a subway, highway, or airport; but too many restrictions can affect the ability to keep the system moving and effectively transporting people and goods. This is the inherent problem in transportation security planning, and it represents the fact that different agencies represent different perspectives on appropriate strategies. State DOTs have the greatest interest in keeping the system as a whole securely running, and subsequently must play the largest role in coordinating the various interests while maintaining efficient and effective collaboration.

In a 2006 UCLA study on security planning in U.S. transit agencies, Taylor et al reviewed 113 providers and found that 46% of transit agencies with rail have conducted vulnerability assessments, as opposed to 13% of those without rail (*21*). This difference is attributed by the authors to the perception by transit agency managers that rail is highly vulnerable to terrorist attack, though it is important to note that agencies with rail systems tend to be larger agencies with more resources to conduct an assessment. However, the authors point out that some facilities without rail do have large, enclosed bus facilities that may be no less tempting a target from a terrorist's perspective, but are not gaining the vulnerability assessment attention simply because they are not part of a rail system. Rail systems are not attacked because they are rail systems; they are attacked because of qualities such as their openness, large population of riders and high visibility that meet the goals of a terrorist action. This misperception may arise from a misunderstanding of how terrorists operate, which is influenced by intelligence and law enforcement agencies. Better communication between the agencies that evaluate terrorist characteristics and transportation agencies could solve an issue such as this by clarifying the intentions and targets of terrorist groups, allowing the agency to better perform its vulnerability assessment with an advanced knowledge of credible threats.

Coordination between transit agencies and agencies that can provide the necessary terrorist information seems to be a persistent issue, according to two post-9/11 GAO

reports (*19*, *22*). State DOTs may have more opportunities to come into contact with these agencies than smaller, regionally or modally focused agencies, and therefore can assume a larger role in coordinating information sharing. The multiple interests involved in terrorism preparedness for the system as a whole—including federal sources such as Anti-Terrorism Task Forces (ATTF) and Joint Terrorism Task Forces (JTTF) that may be supported by state resources—could be overwhelming for smaller agencies within the state to attempt to maintain cooperative relationships with. The complexity of coordinating transportation agencies with these groups—which can include simply determining who the representative should be or when a meeting is taking place—coupled with the fact that appropriate information may come from multiple sources indicates that coordination would be better handled by an umbrella agency like the state DOT, which can devote attention to maintaining connections that might extend across state boundaries and up to the federal government. Placing coordination efforts in the hands of the state DOT also maintains a system-wide focus on security issues; regional or local agencies may only be concerned with their particular asset, and therefore may not locate information outside of their area.

Three specific coordination issues were highlighted in a 2007 FHWA report on common issues in emergency preparedness and response: lack of understanding and experience with the Incident Command System (ICS), interagency difficulties with agency specific terms or acronyms, and the incompatibility of communication equipment (*23*). Although ICS is incorporated into many DOT Emergency Response Plans (as previously discussed), this does not mean that every person on the DOT staff has had ICS training. Whereas law enforcement and first responders will most likely have more experience with this system as it is integral to their work, and not every incident will require the involvement of the DOT. The responsibility falls on the DOT to ensure that essential personnel are properly trained to follow the ICS system in the event of a disaster because a lack of understanding could slow response efforts and lead to a loss of life.

This training may also include an introduction to terms specific to either agency. Agencies may have particular language or terms natural to that specific agency but uncommon for other agencies, and in order to work together there should be some assurance that agencies speak the same language. Because DOT involvement may not always be as extensive as emergency response or law enforcement agencies, the DOT should be more proactive in merging the language of its various subsidiaries and gaining and disseminating the knowledge of other agencies it will need to communicate with. Emergency responders and law enforcement agencies generally communicate on a common platform (although federal agencies such as the Federal Bureau of Investigation can be independent), but transit agencies are not always part of this network. This is another area where the DOT needs to be proactive in assuring coordination for the sake of efficient communication. As the owner and operator of its internal communication system, it is up to the DOT to ensure that this system can be used in the event of an emergency to communicate with other agencies that may need their support. Emergency operations plans and training are not effective if directions and information cannot be communicated between the parties involved in the response effort.

Another coordination issue raised by this report concerns emergency evacuation routes and the lack of coordinated planning. Evacuations may require movement across local, regional and state boundaries, and proper planning helps to ensure efficiency.

According to this report, many routes are planned at the local level but are not placed into a regional context, while some regions have not formulated plans (*23*). Mismatched or missing plans could lead to coordination issues between areas and their respective routes, and these issues will be easier to solve before rather than during an incident. The federal government provides evacuation assistance to state and local governments for them to establish and maintain evacuation plans; but as a 2007 GAO report found, gaps in requirements to "plan, train and conduct exercises" for evacuation routes can leave the financial assistance ineffective *(4)*. This problem highlights the issue of coordination for state DOTs, offering an opportunity to play a large role in assuring regional coordination where local interests may cause division, as well as maintaining accountability where the federal government cannot.

Vulnerability assessments are the core of security planning, yet this same report shows that, although many transportation agencies have performed "at least a cursory assessment," the lack of coordination is devaluing those assessments (*23*). A lack of coordination with other local agencies or jurisdictions resulted in multiple lists of critical and vulnerable infrastructure being developed for the same community, wasting time and money. Many agencies are not identifying methods for monitoring or securing critical infrastructure once they are identified. Some assessments were not performed in conjunction with a law enforcement agency or not shared with those agencies, although the report shows that few coordinated efforts exist to communicate the results among relevant agencies. This report highlights a serious deficiency among transportation agencies, and an opportunity to resolve an issue that the aforementioned evidence suggests will not resolve itself.

5.3 Standardization

Increasing the coordination among transportation agencies and external agencies will also highlight disparities in methods and standards in security planning procedures. An increase in the interaction between agencies could also provide the opportunity to evaluate the benefits and costs of these variations in order to determine the best approach to emergency preparedness. It may also serve to inform various agencies of these standards so that each agency is aware of this standardization, leading to an understanding of the differences or similarities in each agency's practices prior to the event of an emergency.

The TSA has placed a large amount of effort into standardizing aviation security practices, though other modes have not received the same amount of attention (*20*, *22*). A lack of resources inhibits smaller transportation agencies from independently developing security standards, although independent developments could increase the confusion by increasing the variety of standards. State DOTs however have the resources and the broad perspective to coordinate the standardization of security guidelines. Although the role of the TSA in security regulations is increasing, there are multiple opportunities for state DOTs to take action. These efforts could range from a focus on system users, such as standards for transit system exit signs or the content and structure of hazard warning systems, to a focus on the system personnel through training standards. The infrastructure and vehicles that make up the system would also benefit through such efforts as design standards or operational regulations, such as minimum parking distances

to important buildings or restricted parking near bridges. The planning process itself could also benefit through vulnerability assessment standards such as mandating the particular types of data sets to be used, which reduces the possibility of incompatible data sets.

State DOTs already serve as a standard making organization with respect to the normal operations of the transportation system, so security regulations would not be a new direction or stretch of resources for them. They already have an interest in maintaining the system through vulnerability analysis and planning, so this seems a natural extension of those responsibilities. It is also in their best interest to ensure that smaller agencies under their guidance are following the same procedures so that there will be no confusion surrounding the security guidelines, which could cause serious problems if they are not uncovered until the event of an emergency. The current relaxed state of federal regulations with regard to security planning— represented by the fact that the SAFETEA-LU mandate goes no further than saying that security must be independent of safety in the transportation plan—is not so much a void as it is an opportunity to establish the best practices for an individual state, which may not be the same across different regions of the country. Establishing security guidelines based on an evaluation of known procedures give the state DOT the opportunity to both define their role in security planning and define their position of what is appropriate for their state.

5.4 Communications Equipment Compatibility

Coordination and standardization issues culminate in problems associated with the incompatibility of communications equipment among agencies involved in disaster response. The ability to communicate is vital to the functioning of any disaster response effort, especially for transportation officials who need to relay the conditions of the transportation network in order to ensure that response plans can be carried out effectively. As mentioned in the previous discussion of COOP plans, the lack of redundancy in communications systems restricted communication between some of the people and agencies involved in the response to the 9/11 attacks. It would seem that a nationally recognized disaster such as this would provide the impetus for reform, yet a 2007 FHWA report on transportation emergency response showed that redundancy remained an issue six years later (*23*).

Another issue is that many transportation agencies are not able to communicate on the same platform as first-responder agencies, leaving a gap in communications abilities. This is essentially a technology issue in which different agencies have communications devices of various caliber or age, which will ultimately require additional funding and investment to resolve. Some smaller states are resolving the issue by updating their technology and placing everyone on the same platform, while some larger states are not (possibly due to the cost). Putting every agency on the same platform does not necessarily resolve communications issues, but may rather increase the need to coordinate, plan and train personnel on the proper guidelines for usage (i.e. assigning radio frequencies for particular purposes). Ensuring the ability to communicate does not necessarily mean that information will be conveyed effectively either. Some larger states that experience more varied types of emergencies more frequently have opted to maintain their current communications systems and instead focus on ICS training, which gives

personnel a better understanding of the leadership system and who they are reporting to during an emergency.

It seems that a balanced approach of communication ability and command structure is necessary for effective coordination during an emergency, which is a regulatory standpoint that the DOT will have to evaluate and enforce. The technological deficiencies that hinder communication are generally on the side of the transportation agencies, since communication technology is more integral to law enforcement and first responder agencies. Command system strategies are also generally more developed within these agencies, meaning that transportation agencies need to position themselves within these structures. These tasks may require more resources than smaller agencies can spare, and may require not only interstate coordination and cooperation but intrastate as well. The DOT seems to be in the prime position for overcoming these impediments and establishing an effective communications strategy.

5.5 Role of Intelligent Transportation System

ITS functions highlight the capabilities of state DOTS as transportation security information providers. In addition to non-emergency uses, ITS applications such as variable message signs, highway advisory radio (HAR), surveillance cameras, and transportation management centers play an important role in the collection and dissemination of transportation system information, both for use in vulnerability analysis and in providing critical information to emergency agencies and system users (*24*). Its importance is exemplified in SAFETEA-LU, Title V, Subtitle C—Intelligent Transportation System Research, Section 5303 (a)(5), which mandates ITS research to "[improve] the Nation's ability to respond to security—related or other manmade emergencies and natural disasters," although it only provides funding for "outreach, public relations, displays, tours, and brochures." The information provided by ITS technologies can be invaluable to system planners and other agencies that need this information to correctly assess the characteristics of the network. Even more important is the ability of ITS technologies to assist in the evaluation of the post-disaster system and inform users of critical issues or available routes.

A 2007 FHWA report on common issues in emergency preparedness and response showed that some locales are not incorporating ITS capabilities into security planning, and some first-responder agencies are not aware of the capabilities of the system to aid in disaster response (*23*). For instance, some locations utilize real-time video surveillance, and therefore are not able to record the system for law enforcement use; in other instances, legislation prevents the use of this information by law enforcement agencies. Although the variation in legal practices between states makes recommendations difficult, the situation still needs to be addressed (*23*). Other issues are more technical in nature, such as terrain obstructions restricting HAR or cell phone updates.

Resolving issues such as these is a critical step for the DOT because transportation system information is its essential role in an emergency. Outside of an emergency, this information is the key to establishing coordination among the different relevant agencies. Emergency management agencies and law enforcement agencies may need this information to properly carry out their duties, and providing this information

can establish important relationships that lead to effective communication between agency personnel. Although other agencies such as EMAs or MPOs may have an interest in securing this information or ensuring its proper use, it is typically the DOT that owns and operates ITS equipment. In contrast to the issues discussed previously, ITS issues represent a particular instance in which the DOT is the focal point for correcting the issue. Although other agencies may have greater involvement in overall emergency planning or direct emergency response, ITS issues present a direct opportunity for DOTs to influence security planning issues.

Chapter 6:
Conclusions

In his 2007 testimony before the U.S. House of Representatives' Subcommittee on Homeland Security, the Director of Homeland Security and Justice Issues, William O. Jenkins Jr., clearly conveyed the need for coordination among those involved in emergency planning and response: "In preparing for, responding to, and recovering from any catastrophic disaster, the legal authorities, roles and responsibilities, and lines of authority at all levels of government must be clearly defined, effectively communicated, and well understood to facilitate rapid and effective decision making" (*4*). One respondent to an MTI security practice study conveyed this idea in a slightly more succinct manner: "...emergencies are not the time to meet your counterpart in different agencies" (*20*). The role of coordinator is both an important and a difficult one. Chapter 3 discussed the complexity of the security planning environment, which involves many stakeholders that smaller agencies may not have the resources to maintain contact with. The U.S. DOT, a larger entity with more varied resources, maintains a plan for coordinating state DOTs once a national emergency has been declared, but coordinating multiple local authorities could also over-extend the resources of federal agencies (not to mention encountering resistance). For example, DHS grants to state and local governments for security efforts were not sufficiently kept track of, showing that decisions could be made but oversight could not be maintained (*4*).

The significant position state DOTs hold between federal agencies and local authorities is one that should not be squandered. State DOTs have the resources and motivation to improve the collaboration and communication that establishes relationships integral security planning. Yet it is important that DOTs navigate the balance between being an authority and a resource. The DOTs role as a coordinator is to ensure that various agencies communicate so that each agency has the proper frame of reference and different efforts do not overlap or mismatch; their role is not to fill in any perceived gaps on the part of other agencies. There is an important distinction between transportation personnel and emergency responders that should be maintained; otherwise the situation becomes what may be colloquially described as "the tail wagging the dog." The DOT ultimately serves a supporting role, even in their efforts to secure the transportation system. Cross-communication informs a DOT's vulnerability assessment process and emergency response procedures, allowing them to better protect their infrastructure. But this effort then becomes feedback for emergency responders to ensure they can properly do their job, as well as ensuring that critical assets important in response efforts are maintained. The coordination effort should not be an attempt to assume the responsibilities of law enforcement and other response agencies. Instead some agencies are supplying the skills of DOT personnel to emergency responders to support disaster relief. The New York DOT is one example of an agency that has held training classes during which first responders are taught to use DOT snow clearing equipment in the event that DOT operators are not available (C. Thomas, personal communication, Oct. 17, 2008).

State DOTs can serve an important position in improving the issues mentioned in Chapter 5 and solidifying the role of security in the transportation planning process. Standardizing transportation security practices can improve familiarity and reduce errors before, during and after an emergency, and coordinating agencies and improving communication can help streamline efforts at all stages. Yet, as mentioned before, funding initiatives in surface transportation security may be an obstacle. Although they may be able to channel some funding for particular strategies, state DOTs will never be able to cover all proposals, whether operational or capital investments. But what agency can? Funding is and will always be an issue for any agency. Although the efforts of congress to assuage this issue may have fallen short, this does not mean that security planning has been crippled. Lack of funds affects other aspects of the planning process in the same way. Incorporating security into the planning process may require difficult decisions when it comes to capital infrastructure investment, but this incorporation is not reliant on money alone. Incorporating security into the planning process requires a paradigm shift because it means considering more than just the mobility requirements of today. Attention must be shifted to the potential breakdown of the transportation system from external threats and a consideration of how the transportation system will be able to react to those threats to either maintain efficiency or ensure recovery. Updating the transportation system to reflect this perspective will require financial investment, but the need to first adopt this perspective cannot be ignored.

Chapter 7:
Recommendations

The incorporation of security into the transportation planning process has not been accomplished through mandate alone because it cannot be considered simply as Step X in the process. It is also not a singular goal to strive for, and then rest once it is accomplished. As with most of the transportation planning process, security planning requires frequent modification as feedback is analyzed. However, it is a principle that can reach into every aspect of the transportation system.

Chapter 2 mentioned five roles through which security concerns can be incorporated into the normal cycle of decision-making and implementation: Coordinator, Analyzer/Planner, Financial Administrator, Infrastructure Owner and Infrastructure Operator. The DOT already performs each of these roles, and each role represents a method by which security can become ingrained in the transportation system. This is not to say that a DOT should become a security agency; instead, it is a conceptual restructuring that includes security planning in increments, amounting to a more secure system as a whole. A summary of the possible actions and intended goals of these nine roles discussed throughout this report is presented in Table 5 at the end of this section.

Establishing a more solid role as a coordinator appears to be the first step in this process. By solidifying its role as a vital link between relevant agencies, DOTs not only guarantee their interests but ensure that the job itself is done. All of the DOTs interviewed for this report had established contacts within these relevant agencies, and most maintained updated lists of personnel to ensure the persistence of these connections and awareness of counterparts within those agencies. Bringing this to the next level of meaningful interaction may require effort on the part of the DOT, such as calling to attention the reasons why other agencies may need DOT security information. This does not mean micro-managing local transportation agencies, but instead could involve updates at particular intervals or ensuring that stakeholders are made aware of the planning process.

This interaction may bring to light relevant standardization issues as methods are compared and information is received, and the DOT can resolve these issues both by mandating standards and through the process of analyzing and planning the system. Through their authority, state DOTs can set standards necessary for proper security planning, such as specifying appropriate data formats for vulnerability assessments. Through the consideration of security factors in the course of analyzing and planning the system, the DOT also sets standards. These considerations may change the perception of how the system should be composed, which in turn affects the infrastructure owned and operated by the DOT. This gradual implementation of standards will then begin to be reflected in coordination efforts as personnel are able to communicate more fluidly with one another based on a common understanding and perspective.

The role of financial administrator is an important one in the process of analyzing and planning for the refurbishment or new construction of facilities, as well as the training of personnel. Whereas the vulnerability assessment process may tend to stress the immediacy of particular security concerns, this restricts the focus to particular

projects rather than ensuring the security of the system. While the need for retroactive enhancements cannot be ignored, funding projects on a case-by-case basis may lock the security planning process within the concept of only applying it when it is needed. The funding process must be intertwined with the analyzation and planning process in order to ensure that funding choices fit within the broader context of security planning. This means that rather than choosing to fund particular security projects, security needs should by highlighted during the planning of the system and considered a part of the project. Just as the paving of a new road requires the painting of lines, the introduction of a new turnstile in a subway station can include relevant security measures.

Incorporating security through these five roles can then be reflected in four different DOT roles: Implementer, Regulator, Information Provider, and Influencer. By implementing its own security considerations and regulating the use the system, the DOT naturally influences the security of the system. Its role as an information provider to the public through ITS was discussed in Chapter 6, but no less important is its role as an information provider to other supporting agencies. By obtaining and providing information necessary for first responders to respond to disasters and for federal agencies to evaluate their security policies, the DOT provides valuable information used to maintain the security of the transportation system. And by simply exercising these aforementioned abilities, the DOT influences the role of security in any system user.

Table 5: A summary of state DOT roles.

Role	Action	Goal
Coordinator	• Establish and maintain a list of counterparts among relevant agencies • Initiate regular meetings for updates and stakeholder input • Instruct relevant personnel in the use of vital transportation equipment	• Establish effective communication • Solidify a role as a vital link between security-related agencies • Clarify roles of supporting agencies
Analyzer/Planner	• Incorporate security evaluations and concerns into the initial analysis phase of each new project • Perform vulnerability assessments on existing infrastructure	• Establish transportation system security concerns • Incorporate security concerns into the early stages of the planning process

Financial Administrator	• Incorporate security needs into system funding plans instead of focusing on funding particular security measures • Evaluate the effect of funding choices on security factors	• Establish funding for security efforts
Implementer	• Implement security policies	• Ensure planning efforts affect transportation system
Infrastructure Owner	• Initiate analyzation and planning activities to ensure the security of the state transportation system • Identify critical transportation infrastructure • Ensure the capability to maintain as well as initiate security measures	• Ensure the security of transportation infrastructure
Infrastructure Operator	• Incorporate security plans into operational procedures • Update and maintain COOP plans • Gather information necessary to effective security planning	• Ensure the implementation of security measures
Regulator	• Ensure standardization of communications abilities with law enforcement	• Ensure standards • Enforce requirements
Information Provider	• Increase awareness of ITS capabilities among relevant coordinating agencies, especially emergency responders	• Effectively communicate necessary transportation system information to support disaster response
Influencer	• Incorporate security into the transportation planning process	• Influence the security of the transportation environment and related infrastructure

Source: Author

Appendix A:

Emergency Support Function #1

Emergency Support Function #1 – Transportation Annex

ESF Coordinator:

Department of Transportation

Primary Agency:

Department of Transportation

Support Agencies:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of the Interior
Department of Justice
Department of State
General Services Administration
U.S. Postal Service

INTRODUCTION

Purpose

Emergency Support Function (ESF) #1 – Transportation provides support to the Department of Homeland Security (DHS) by assisting Federal, State, tribal, and local governmental entities, voluntary organizations, nongovernmental organizations, and the private sector in the management of transportation systems and infrastructure during domestic threats or in response to incidents. ESF #1 also participates in prevention, preparedness, response, recovery, and mitigation activities. ESF #1 carries out the Department of Transportation (DOT)'s statutory responsibilities, including regulation of transportation, management of the Nation's airspace, and ensuring the safety and security of the national transportation system.

Scope

ESF #1 embodies considerable intermodal expertise and public and private sector transportation stakeholder relationships. DOT, with the assistance of the ESF #1 support agencies, provides transportation assistance in domestic incident management, including the following activities:

- Monitor and report status of and damage to the transportation system and infrastructure as a result of the incident.
- Identify temporary alternative transportation solutions that can be implemented by others when systems or infrastructure are damaged, unavailable, or overwhelmed.
- Perform activities conducted under the direct authority of DOT elements as these relate to aviation, maritime, surface, railroad, and pipeline transportation.
- Coordinate the restoration and recovery of the transportation systems and infrastructure.
- Coordinate and support prevention, preparedness, response, recovery, and mitigation activities among transportation stakeholders within the authorities and resource limitations of ESF #1 agencies.

ESF #1 is not responsible for movement of goods, equipment, animals, or people.

Policies

Primary responsibility for management of incidents involving transportation normally rests with State and local authorities and the private sector, which own and operate the majority of the Nation's transportation resources. As such, a Federal response must acknowledge State and local transportation policies, authorities, and plans that manage transportation systems and prioritize the movement of relief personnel and supplies during emergencies.

The Secretary of Transportation coordinates ESF #1, consistent with DOT's statutory mission, to promote fast, safe, efficient, and convenient transportation in support of the national objectives of general welfare, economic growth and stability, and the security of the United States.

DHS/Federal Emergency Management Agency (FEMA) is responsible for the provision of transportation assets and services (including contracts or other agreements for transportation assistance) for responders, equipment, and goods, consistent with the ESF #7 – Logistics Management and Resource Support Annex.

The ability to sustain transportation services, mitigate adverse economic impacts, meet societal needs, and move emergency relief personnel and commodities will hinge on effective transportation decisions at all levels. Unnecessary reductions or restrictions to transportation will directly impact the effectiveness of all prevention, preparedness, response, recovery, and mitigation efforts.

Department of Defense (DOD) transportation support will be provided in accordance with Defense Support of Civil Authorities, the memorandum of understanding between DOD and DOT concerning commercial aviation programs, and the memorandum of agreement between DOD and DOT concerning the National Defense Reserve Fleet and the Ready Reserve Force.

DOT/Federal Aviation Administration (FAA) is responsible for the operation and regulation of the U.S. National Airspace System, including during emergencies.

In cases where State, tribal, and local authorities are overwhelmed, Federal support for mass evacuations is addressed in the Mass Evacuation Incident Annex to the *National Response Framework (NRF)*. ESF #1 can provide any or all of the activities within the scope of this annex to support the Mass Evacuation Incident Annex.

During mass evacuations, consistent with the Mass Evacuation Incident Annex, DHS/FEMA provides transport for persons, including individuals with special needs, provided they meet the following criteria:

- Evacuees can be accommodated at both embarkation points and at destination general population shelters.
- Evacuees can travel on commercial long-haul buses, aircraft or passenger trains, or lift-equipped buses.
- Evacuees do not have medical needs indicating that they should be transported by ESF #8 – Public Health and Medical Services.

Consistent with the Mass Evacuation Incident Annex and the Post-Katrina Emergency Management Reform Act, DHS/FEMA is responsible for evacuation of service and companion animals.

Evacuation of medical patients is the responsibility of ESF #8. DHS/FEMA can support ESF #8 by providing limited bus evacuations between medical facilities within the limitations and capabilities of the assets and drivers.

CONCEPT OF OPERATIONS

General

ESF #1 provides DHS with a single point to obtain key transportation-related information, planning, and emergency management, including prevention, preparedness, response, recovery, and mitigation capabilities at the Headquarters, regional, State, and local levels. The ESF #1 structure integrates DOT and support agency capabilities and resources into the *NRF* and the *National Incident Management System (NIMS)*.

Initial response activities that ESF #1 conducts during emergencies include the following:

- Monitoring and reporting the status of and damage to the transportation system and infrastructure.
- Identifying temporary alternative transportation solutions to be implemented by others when primary systems or routes are unavailable or overwhelmed.
- Implementing appropriate air traffic and airspace management measures.
- Coordinating the issuance of regulatory waivers and exemptions.

In addition to the above initial activities, ESF #1 provides longer-term coordination of the restoration and recovery of the affected transportation systems and infrastructure if required.

Activation

The National Response Coordination Center (NRCC) issues operation orders and mission assignments to activate ESF #1 based on the scope and magnitude of the threat or incident.

The NRCC notifies the DOT Crisis Management Center (CMC), which serves as the focal point for the Department's emergency response and the formal point of contact for ESF #1 activation within DOT.

DOT, in turn, activates Headquarters and regional ESF #1 staff and primary and support agencies as required, including support to specialized teams such as modal transportation experts acting under the *NRF*. In cases where Regional Response Coordination Centers (RRCCs) activate ESF #1 in individual regions, the Regional Emergency Transportation Coordinator (RETCO) notifies the CMC and coordinates activation and activities with ESF #1 in the NRCC.

ORGANIZATION

Headquarters Response Organization

NRCC: When activated, ESF #1 provides staff to the NRCC. Staffing levels and composition will be determined by the scope, scale, and nature of the threat or incident. Additional technical expertise, planning, and operational support are provided by DOT Headquarters and field offices.

DOT Emergency Response Team: DOT activates the Department's Emergency Response Team. The team works closely with other departments and agencies and DOT's extensive stakeholder network to assess the affected transportation systems, identify alternatives to damaged or overwhelmed modes to be implemented by others, and identify the sector's needs.

DOT/FAA Response Cells: FAA activates specialized response cells to manage and coordinate air navigation services and other aviation-related efforts.

Regional Response Organization

DOT's Regional Emergency Transportation Program: The Regional Emergency Transportation Program provides the staff and expertise required to support ESF #1 in the field. The program consists of a Headquarters element and 10 regions, which are based on the standard Federal regions. The Regional Emergency Transportation Coordinators and Representatives (RETCO/RETREP) provide full-time, collateral duty and volunteer DOT and contractor staff to augment regional and State incident command structures. This includes RRCCs, Joint Field Offices (JFOs), and State emergency operations centers, as needed. This cadre also provides regional DOT transportation support during nonemergency periods in contingency planning efforts within the limits of available resources and/or as funded by FEMA.

The DOT RETCO provides direction for the regional ESF #1 mission. The RETCO is the Secretary of Transportation's representative for emergency preparedness and response matters within the region and receives policy guidance and operational direction from the Office of the Secretary.

The RETCO is responsible for the administrative support of DOT individuals involved in regional emergency transportation operations and coordination with DOT Headquarters in the management of all financial transactions undertaken through mission assignments and interagency agreements issued to ESF #1.

ACTIONS: INITIAL ACTIONS

National Activation

DOT: Immediately upon notification of a threat or an imminent or actual incident, the following actions will be taken, as required:

- Initiate reporting to the Office of the Secretary of Transportation, the National Operations Center (NOC) elements (NOC watch, National Infrastructure Coordinating Center (NICC), NRCC, and TSOC), Domestic Readiness Group (DRG), Counterterrorism Security Group (CSG), DOT operating administrations and regional offices, and the RETCO.
- Activate the DOT Emergency Response Team.
- Staff ESF #1 at the NRCC.
- Dispatch staff to the Incident Management Planning Team (IMPT), DRG, CSG, NRCC, RRCC(s), JFO(s), and Evacuation Liaison Team.
- Activate the RETCOs and RETREPs.
- Inform and invite participation by ESF #1 support agencies.

Support Agencies: Provide staff and support to ESF #1.

Regional Activation

At the regional level (RRCC and/or JFO), the RETCO or a designated representative establishes communications with the NRCC, the FCO/FRC, the CMC, and the Principal Federal Official (if designated).

Initial Emergency Support Activities

- **Monitor and report status of and damage to transportation systems and infrastructure as a result of the incident.** DOT provides this information (via the CMC) to the NOC, NRCC, and NICC, as well as the affected RRCCs and JFOs. Information is compiled from a variety of sources, including ESF #1 support agencies, ESF #1 cadre at various locations, each of DOT's Operating Administrations (through more than 300 field offices nationwide), and key transportation associations and transportation providers. Reports include specific damages sustained, ongoing recovery efforts, alternatives planned or implemented by others, and assessments of the impact.

  The NOC, NICC, and Transportation Security Operations Center (TSOC) provide relevant situational awareness and threat information reports input to ESF #1 in its lead role in reporting the status of transportation infrastructure.

- **Identify temporary alternative transportation solutions implemented by others when systems or infrastructure are damaged, unavailable, or overwhelmed.** Primary responsibility for arranging for alternate transportation services lies at the State and local levels, with the system owner or operator and/or State and local government. However, during major incidents, or when Federal coordination or funding support is required, ESF #1 identifies alternate transportation services implemented by others.

  The Transportation Security Administration, as Sector-Specific Agency for transportation, supports ESF #1 in the identification and prioritization of critical transportation infrastructure and key resources (CIKR) and, in cases of terrorist threats or attacks, will recommend actions to protect these resources.

  The DHS Office of Infrastructure Protection supports ESF #1 in the identification and prioritization of nontransportation CIKR that may be impacted by transportation.

  Within the limits of the scope of this annex, the RETCO or designated alternate coordinates with appropriate State, tribal, and local entities, DOT Headquarters, and the NRCC in decisions regarding issues such as movement restrictions, critical facilities closures, and evacuations.

  On a case-by-case basis, and within the limits of the scope of this annex, DOT will assist DHS/FEMA in coordinating passenger rail support to mass evacuations under the Mass Evacuation Incident Annex, when activated.

  In addition to the above activities, during major evacuations, ESF #1 provides support to the DHS/FEMA-led Evacuation Liaison Team to assist in coordination of large-scale highway evacuations, especially when involving more than one State.

- **Perform activities conducted under the direct authority of DOT elements.** This includes a variety of statutory activities, including management of the National Airspace System; maritime, surface transportation, railroad, and pipeline regulatory activities; funding; issuing transportation regulatory waivers and exemptions (e.g., hours of service, hazardous materials regulations, etc.); and other emergency support.

The RETCO or designated alternate coordinates with appropriate DOT regional operating administrations on the implementation of specific DOT statutory authorities providing immediate assistance. Examples include airspace management, long-term recovery of the transportation infrastructure, and any authorized mitigation efforts.

ACTIONS: CONTINUING AND ONGOING ACTIONS

In addition to sustaining the initial actions, ESF #1 provides long-term coordination of the restoration and recovery of the affected transportation systems and infrastructure.

- **Coordinate the restoration and recovery of the transportation infrastructure.** Primary responsibility for coordinating the restoration and recovery of the transportation infrastructure beyond the State and local level rests with DOT through the unique resources and expertise of each Operating Administration and the ESF #1 support agencies to facilitate recovery.

  Prioritization of restoration efforts is based on response needs as identified within the JFO, RRCC, and NRCC, as well as the State, regional, or national interdependencies that may have far-reaching impacts.

  Several DOT Operating Administrations have individual programs, funding sources, and technical experts (e.g., inspectors, engineers, etc.) that can be utilized to support restoration and recovery efforts. These include the FAA, the Federal Highway Administration, the Federal Transit Administration, the Federal Railroad Administration, the Pipeline and Hazardous Materials Safety Administration, the Maritime Administration, and the Research and Innovative Technologies Administration (including the Volpe Transportation Center).

- **Coordinate and support prevention, preparedness, and mitigation activities among transportation stakeholders.** This is a continuous activity that is conducted within the authorities and resource limitations of ESF #1 agencies. Activities include supporting Federal, State, and local planning efforts as they relate to transportation, including evacuation planning, contingency plans, etc. as well as working with the designated Special Needs Advisor, as described in the *NIMS*, to address persons with special needs in the planning process.

RESPONSIBILITIES

ESF Coordinator: DOT

DOT is responsible for planning and coordination of activities affecting transportation throughout prevention, preparedness, response, recovery, and mitigation. These activities include planning and coordination, maintaining ongoing contact with ESF primary and support agencies, conducting periodic ESF meetings and conference calls, coordinating efforts with State/local/tribal and private-sector organizations, and coordinating ESF activities relating to catastrophic incident and mass evacuation planning and critical infrastructure preparedness as appropriate.

DOT:

- Provides support to DHS in prevention, preparedness, response, recovery, and mitigation activities among transportation infrastructure stakeholders at the regional, State, and local levels within the authorities and resource limitations of ESF #1 agencies. (Preparedness for mass evacuations is addressed in the Mass Evacuation Incident Annex.)

- Supports planning and coordination elements of preparedness as requested and funded on a reimbursable basis by DHS.

- Manages the financial aspects of the Federal ESF #1 response, including management of Stafford Act mission assignments or reimbursable agreements for non-Stafford Act Federal-to-Federal support.

Primary Agency: DOT

- Manages the headquarters and the regional ESF #1 activities.

- Provides trained personnel to staff ESF #1 positions at the NRCC, the RRCC, the JFO, or any other temporary facility in the impacted region appropriate to the ESF #1 mission.

- Deploys members to fill positions on emergency response teams, the IMPT, and other entities as necessary.

- Through DOT/FAA, oversees the operation and regulation of the U.S. National Airspace System, including during emergencies. Under certain conditions, DOT/FAA may delegate use of specified airspace for national defense, homeland security, law enforcement, and response (e.g., search and rescue) missions, but retains control of the airspace at all times. DOT/FAA may also implement air traffic and airspace management measures such as temporary flight restrictions in conjunction with these missions. Coordination of these activities can be initiated through ESF #1 or directly with DOT/FAA, as appropriate.

- Works with primary and support agencies, State and local transportation departments, and industry partners, and with input from the NICC and TSOC, to assess and report the damage to the transportation infrastructure and analyze the impact of the incident on transportation operations, nationally and regionally.

- Coordinates and implements, as required, emergency-related response and recovery functions performed under DOT statutory authorities. This includes management of the airspace within and surrounding the disaster-impacted area, emergency highway funding for federally owned highways and highways on the Federal Aid System, hazardous material movement, and damage assessment, including safety- and security-related actions.

- Provides technical assistance to Federal, State, tribal, and local governmental entities in determining the most viable transportation networks to, from, and within the incident area and on availability of accessible transportation.

- Assists in restoring the transportation infrastructure through ESF #3 – Public Works and Engineering and the Stafford Act program.

SUPPORT AGENCIES

Agency	Functions
Department of Agriculture (USDA)	**Forest Service** • If available, provides transportation assets to ESF #1 when Forest Service resources are the most effective to support the ESF #1 mission. • If available, provides appropriate engineering and contracting/procurement personnel and equipment to assist in emergency removal of debris, demolition, repair of roads and bridges, and temporary repair of essential public facilities. Resources will be assigned commensurate with each unit's level of training and the adequacy and availability of equipment. ESF #4 – Firefighting or the USDA/Forest Service Disaster and Emergency Operations Branch is the contact for this support.
Department of Commerce (DOC)	**National Oceanic and Atmospheric Administration (NOAA)** Provides the following products and information to support ESF #1 activities, including mass evacuations: • Forecasts, watches, and warnings including weather, storm surge, and dispersion forecasts. • Surface and marine forecasts and nowcasts including ice and debris tracking. • Emergency hydrographic surveys, search and recovery, obstruction location, and vessel traffic rerouting in ports and waterways. • Remote aerial and orbital imagery through the DOC/NOAA desk at the NOC.
Department of Defense	• Provides military transportation capacity from the U.S. Transportation Command (USTRANSCOM) or other organizations to move essential resources, including DOT response personnel and associated equipment and supplies, when requested and upon approval by the Secretary of Defense. USTRANSCOM also provides staff to the headquarters ESF #1 function and the regional ESF #1 when requested and upon approval by the Secretary of Defense. • Provides assets to complement temporarily degraded or disrupted DOT/FAA air navigation services capabilities as requested by DOT/FAA and ESF #1.
	U.S. Army Corps of Engineers (USACE) • Provides support in the emergency operation and restoration of inland waterways, ports, and harbors under the supervision of DOD/USACE, including dredging operations. • Assists in restoring the transportation infrastructure.
Department of Energy (DOE)	• When requested, DOE/National Nuclear Security Administration provides fixed-wing and rotary aircraft to support radiological environment surveys and/or search capabilities during a radiological or nuclear incident. • Provides information on status of, needs for, and plans for restoration of interdependent infrastructure.

Agency	Functions
Department of Homeland Security	**Customs and Border Protection (CBP)** • Identifies and provides transportation-related DHS/CBP assets and resources. • Provides assets to complement temporarily degraded or disrupted DOT/FAA air navigation services capabilities as requested by DOT/FAA and ESF #1.
	Federal Emergency Management Agency • Provides timely funding for activation and Stafford Act-eligible ESF #1 activities. • Provides necessary funding for ESF #1 participation in DHS- and FEMA-sponsored planning, training, exercises, and other preparedness activities.
	Transportation Security Administration • Through the TSOC, provides relevant transportation and threat information reports, including Information Sharing and Analysis Centers reports, to ESF #1 in its lead role in reporting the status of transportation infrastructure. • Serves as ESF #1 liaison to ESF #13 – Public Safety and Security, as appropriate. • Leads efforts to protect transportation infrastructure from the effects of acts of terrorism, and supports efforts to protect transportation infrastructure from the effects of manmade and natural disasters. • Provides assets to address security and on-site coordination requirements for the ground operations and in-flight segments of mass air evacuation operations as requested by ESF #1. • Provides assistance in the allocation and prioritization of resources through the Infrastructure Liaison and the NICC.
	U.S. Coast Guard • Identifies and provides assets and resources in support of the ESF #1 mission. • Coordinates with support agencies and other maritime stakeholders through ESF #1 to prioritize, evaluate, and support restoration of domestic ports, shipping, waterways, and related systems and infrastructure. • Provides staff to the DOT CMC during emergencies to provide status of maritime domain, including ports, waterways and operations, in ESF #1 for integration in overall transportation sector status reporting.
	Office of Infrastructure Protection: Provides information and assistance concerning the recovery and restoration of transportation critical infrastructure, as well as all other CIKR impacted by transportation.
Department of the Interior (DOI)	• Identifies, and if available, provides departmental transportation assets (e.g., fixed-wing aircraft and all-terrain vehicles) and support resources (e.g., mechanics, pilots) if these are the most effective to support the ESF #1 mission. Resources will be assigned commensurate with each unit's level of training and the adequacy and availability of equipment. ESF #4 or the DOI Operations Center is the contact for this support. • Provides information on status of, needs for, and plans for restoration of infrastructure.
Department of Justice	Identifies and provides departmental transportation support assets in support of the ESF #1 mission when not committed for internal operations.

Agency	Functions
Department of State (DOS)	• When requested, provides liaison to the DOT CMC in the event of incidents having potential international implications. • In accordance with the International Coordination Support Annex, coordinates international offers of transportation-related assistance and support. • In coordination with DOT/FAA, modify or revoke previously approved foreign diplomatic aircraft clearances. This DOS action does not obviate the continuing need for flight crews to check the pertinent Notices to Airmen released by DOT/FAA. DOS will reference DOT/FAA airspace restrictions, including Temporary Flight Restrictions, as part of its processing of requests from foreign embassies/missions for diplomatic aircraft clearance.
General Services Administration	Assists in identifying sources for and contracting transportation services needed for execution of the ESF #1 mission.
U.S. Postal Service	Collects and reports on transportation infrastructure disruption and damages as information becomes available.

Appendix B:

Interview Questionnaire

Security Planning Questionnaire – State Departments of Transportation

1. How does security planning fit into your current transportation planning process?
   a. Is this a direct response to SAFETEA-LU provisions?
   b. What components, such as vulnerability assessments or evacuation modeling, are you specifically involved in?
2. What funding strategies have you used (or plan to use) to support pre-disaster security measures that are proposed as a result of the planning and assessment process?
3. What coordination issues have you experienced with external agencies such as EMAs, federal agencies or law enforcement agencies?
   a. What non-transportation agencies do you coordinate with?
   b. What transportation agencies do you coordinate with?
4. What activities does your DOT pursue to promote connection between internal personnel and external agencies in regards to security planning?
5. Has your DOT experienced any implementation issues in regards to security plans or policy?
6. What other issues has your DOT experienced in the security planning process?

Appendix C:

Critical Asset Factors

CRITICAL ASSET FACTOR	VALUE	DESCRIPTION
Deter/Defend Factors		
A) Ability to Provide Protection	1	Does the asset lack a system of measures for protection? (i.e., Physical or response force)
B) Relative Vulnerability to Attack	2	Is the asset relatively vulnerable to an attack? (i.e., Due to location, prominence, or other factors)
Loss and Damage Consequences		
C) Casualty Risk	5	Is there a possibility of serious injury or loss of life resulting from an attack on the asset?
D) Environmental Impact	1	Will an attack on the asset have an ecological impact of altering the environment?
E) Replacement Cost	3	Will significant replacement cost (the current cost of replacing the asset with a new one of equal effectiveness) be incurred if the asset is attacked?
F) Replacement/Down Time	3	Will an attack on the asset cause significant replacement/down time?
Consequences to Public Services		
G) Emergency Response Function	5	Does the asset serve an emergency response function and will the action or activity of emergency response be affected?
H) Government Continuity	5	Is the asset necessary to maintain government continuity?
I) Military Importance	5	Is the asset important to military functions?
Consequences to the General Public		
J) Available Alternate	4	Is this the only asset that can perform its primary function? (i.e., There are no alternate facilities that will substitute adequately if this asset is damaged or destroyed)
K) Communication Dependency	1	Is communication dependent upon the asset?
L) Economic Impact	5	Will damage to the asset have an effect on the means of living, or the resources and wealth of a region or state?
M) Functional Importance	2	Is there an overall value of the asset performing or staying operational?
N) Symbolic Importance	1	Does the asset have symbolic importance?

Source: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

Appendix D:

Vulnerability Factors

VULNERABILITY FACTOR and DEFAULT VALUE			*DEFINITION*
Visibility and Attendance	**LEVEL OF RECOGNITION (A)**	1	Largely invisible in the community
		2	Visible by the community
		3	Visible Statewide
		4	Visible Nationwide
		5	Visible Worldwide
	ATTENDANCE/ USERS (B)	1	Less than 10
		2	10 to 100 (Major Incident per FEMA)
		3	100 to 1000
		4	1000 to 3000
		5	Greater than 3000 (Catastrophic Incident per FEMA)
Access to the Asset	**ACCESS PROXIMITY (C)**	1	Asset with no vehicle traffic and no parking within 50 feet
		2	Asset with no unauthorized vehicle traffic and no parking within 50 feet
		3	Asset with vehicle traffic but no vehicle parking within 50 feet
		4	Asset with vehicle traffic but no unauthorized vehicle parking within 50 feet
		5	Asset with open access for vehicle traffic and parking within 50 feet
	SECURITY LEVEL (D)	1	Controlled and protected security access with a response force available
		2	Controlled and protected security access without a response force
		3	Controlled security access but not protected
		4	Protected but not controlled security access
		5	Unprotected and uncontrolled security access

VULNERABILITY FACTOR and DEFAULT VALUE			*DEFINITION*
Site Specific Hazards	**RECEPTOR IMPACTS (E)**	1	No environmental or human receptor effects
		2	Acute or chronic toxic effects to environmental receptor(s)
		3	Acute and chronic effects to environmental receptor(s)
		4	Acute or chronic effects to human receptor(s)
		5	Acute and chronic effects to environmental and human receptor(s)
	VOLUME (F)	1	No materials present
		2	Small quantities of a single material present
		3	Small quantities of multiple materials present
		4	Large quantities of a single material present
		5	Large quantities of multiple materials present

Source: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

REFERENCES

(1) AASHTO. *Protecting America's Roads, Bridges, & Tunnels: The Role of State DOTs in Homeland Security*. http://www.transportation.org/sites/security/docs/Final%20-%20Protecting%20America%27s%20Roads%20Bridges%20%20Tunnels.pdf. Accessed 07/13/2008.

(2) A.M. Howitt, and J. Makler. *Protecting America's Highways and Transit Systems Against Terrorism.* Presented at 82nd Annual Meeting of the Transportation Research Board, Washington, D.C., 2003.

(3) Federal Emergency Management Agency. *Emergency Support Function Annexes: Introduction.* http://www.fema.gov/pdf/emergency/nrf/nrf-esf-intro.pdf. Accessed 04/25/2008.

(4) W. O. Jenkins, Jr. *Preparing for and Responding to Disasters* (GAO-07-395T). Testimony before the U.S. House, Committee on Appropriations, Subcommittee on Homeland Security. Washington, DC: General Accounting Office. March 7, 2007

(5) T. Litman. *Lessons from Katrina and Rita: What Major Disasters can Teach Transportation Planners.* Journal of Transportation Engineering, Vol. 132, Jan. 2006, pp. 11-18.

(6) D. L. Dornan, and M.P. Maier. *NCHRP Report 525, Vol. 3: Incorporating Security into the Transportation Planning Process.* Transportation Research Board of the National Academies, Washington, D.C., 2005.

(7) Federal Emergency Management Agency. *Emergency Support Function #1 – Transportation Annex.* http://www.fema.gov/pdf/emergency/nrf/nrf-esf-01.pdf. Accessed 04/25/2008.

(8) Parsons Brinckerhoff, PB Farradyne Incorporated. *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents.* AASHTO, Washington, D.C., 2002.

(9) A. Boyd, J. Caton, A. Singleton, P. Bromley, and C. Yorks. *TCRP Report 86, Vol. 8/NCHRP Report 525, Vol. 8: Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies.* Transportation Research Board of the National Academies, Washington, D.C., 2005.

(10) B.M. Jenkins, and F. Edwards-Winslow. *Saving City Lifelines: Lessons Learned in the 9-11 Terrorist Attacks.* Mineta Transportation Institute Report 02-06. Mineta Transportation Institute, San Jose, CA, Sept. 2003.

(11) M.C. Smith, S. Rowshan, S.J. Krill, J.E. Seplow, and W.C. Sauntry. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* AASHTO, Washington, D.C., 2002.

(12) L. C. Murray (ed.). *Risk Assessment and Prioritization*. Volpe National Transportation Systems Center, Cambridge, MA, 2003. URL. Accessed 04/26/2008.

(13) M. Meyer. The Nation's Transportation System as a Security Challenge. In *Wiley Handbook of Science and Technology for Homeland Security* (J. G. Voeller, ed.), John Wiley and Sons, Inc., 2008.

(14) D. Geiger, et al. *Transportation Asset Management in Australia, Canada, England, and New Zealand.* Report FHWA-PL-05-019. FHWA, U.S. Department of Transportation, 2005.

(15) G. Rowe, and G. Wright. *The Delphi Technique as a Forecasting Tool: Issues and Analysis*. International Journal of Forecasting, Volume 15, Issue 4, pp. 353-374.

(16) M. Meyer, and E. Miller. *Urban Transportation Planning: A Decision-Oriented Approach.* McGraw-Hill, Inc., New York, 1984.

(17) H. A. Linstone, and M. Turoff. *The Delphi Method: Techniques and Applications.* Addison-Wesley Publishing Co., Reading, Mass., 1975.

(18) J. Xia, M. Chen, and R. Liu. *A Framework for Risk Assessment of Highway Network*. Presented at 84th Annual Meeting of the Transportation Research Board, Washington, D.C., 2005.

(19) General Accounting Office. *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*. Report GAO-03-263. Washington, D.C., Dec., 2002.

(20) B. Taylor, R. Liggett, and E. Cavanagh. *Designing and Operating Safe and Secure Transit Systems: Assessing Current Practices in the United States and Abroad.* MTI Report 04-05. Mineta Transportation Institute, San Jose, CA, Nov., 2005.

(21) B. D. Taylor, C. N.Y. Fink, and R. Liggett. *Responding to Security Threats in the Post-9/11 Era: A Portrait of U.S. Urban Public Transit*. Public Works Management & Policy, Vol. 11, No. 1, 2006, pp. 1-15.

(22) C. A. Berrick. *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts* (GAO-07-459T). Testimony, Feb. 13, 2007, before the U.S. House, Committee on Appropriations, Subcommittee on Homeland Security. Washington, DC: General Accounting Office.

(23) N. Houston. *Common Issues in Emergency Transportation Operations Preparedness and Response: Results of the FHWA Workshop Series.* Report FHWA-HOP-07-090. FHWA, U.S. Department of Transportation, 2007.

(24) C. Zimmerman, P. Bolton, M. Raman, T. Kell, S. Unholz, and C. Bausher. *Communicating With the Public Using ATIS During Disasters: A Guide for Practitioners.* Report FHWA-HOP-07-068. FHWA, U.S. Department of Transportation, Apr., 2007.