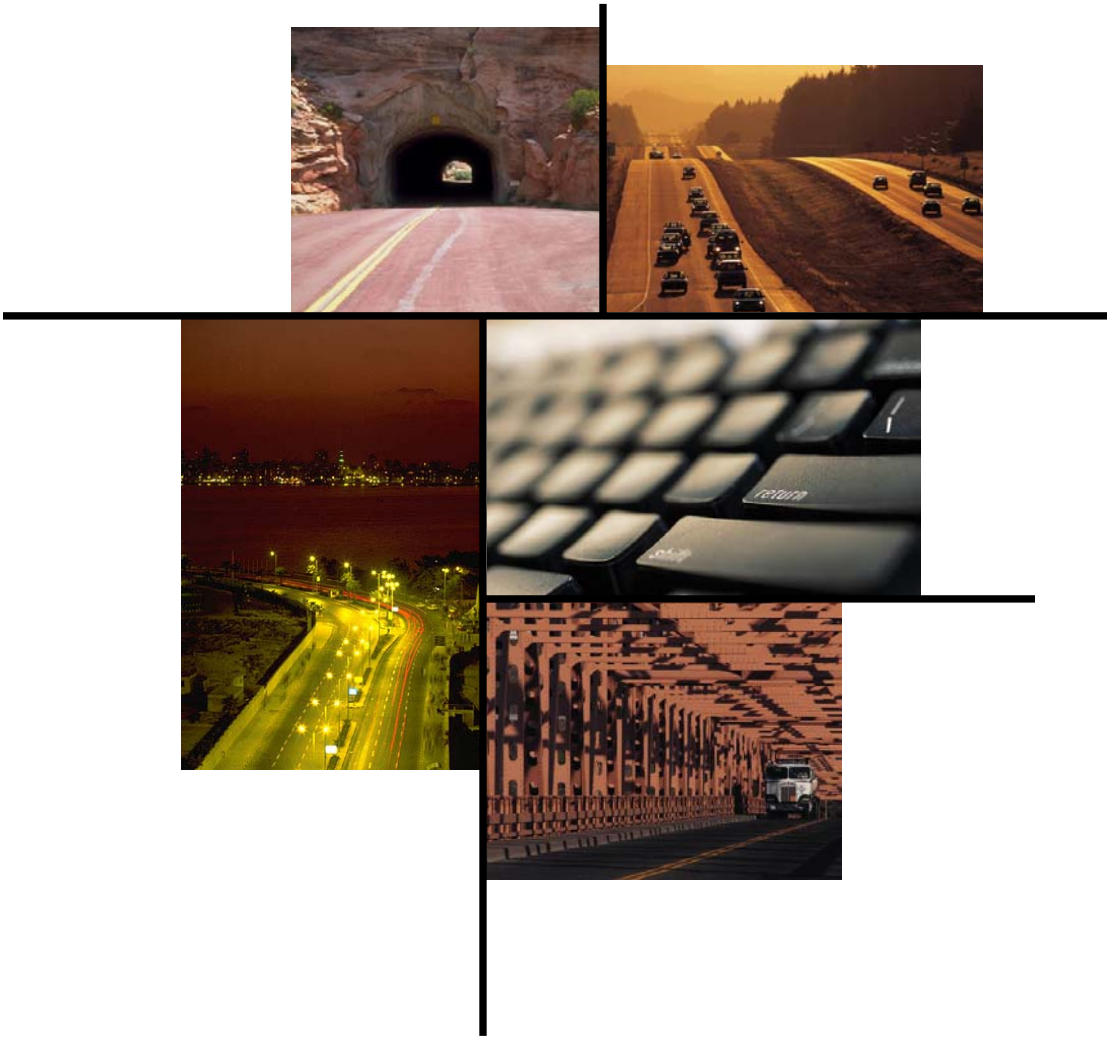
VOLUME II:

EFFECTIVE PRACTICES IN STATE DEPARTMENT OF TRANSPORTATION SECURITY PLANNING



Prepared by:
Volpe National Transportation Systems Center
Research and Special Programs Administration
U.S. Department of Transportation

August 2004

[This page left intentionally blank.]

ACKNOWLEDGEMENTS

This report was prepared by the US Department of Transportation/Research and Special Programs Administration/Volpe National Transportation Systems Center (Volpe Center). This work was funded under Project Plan Agreement HW2Q with the Federal Highway Administration (FHWA). Funding for this report was provided from the FHWA Transportation Pooled Fund Program. The sponsoring state departments of transportation (DOTs) were the Pennsylvania Department of Transportation (PennDOT) as the lead DOT, the Arizona Department of Transportation and the Indiana Department of Transportation.

Rachel Winkeller, Acting Division Chief, Planning and Policy Analysis Division led the project team. Matthew Rabkin, Planning and Policy Analysis Division, provided technical expertise. Key contributors were Jordan Karp and Benjamin Rasmussen of Chenega Advanced Solutions and Engineering, LLC. Robert Brodesky of EG&G Technical Services, Inc. provided contributions to Volume II and III of the report. Hannah Rakoff of Chenega Advanced Solutions and Engineering, LLC provided contributions to Volume III.

For additional information about this report contact:

Rachel Winkeller
Acting Division Chief
Planning and Policy Analysis Division
US Department of Transportation/Volpe Center
55 Broadway, DTS-46
Cambridge, MA 02142
Phone: 617-494-2764
Email: winkeller@volpe.dot.gov

Or

Matthew Rabkin
Planning and Policy Analysis Division
US Department of Transportation/Volpe Center
55 Broadway, DTS-46
Cambridge, MA 02142
Phone: 617-494-2151
Email: rabkin@volpe.dot.gov

[This page left intentionally blank.]

TABLE OF CONTENTS

I. Introduction 1

II. Effective Practices 3

Findings 4

A. Overall Strategic Direction 4

B. Organizational Structure 6

C. Roles and Responsibilities 8

D. Relationships with External Agencies and Transportation Providers 11

E. Plans and Procedures 13

F. Communications 16

G. Intelligent Transportation Systems (ITS) 17

H. Infrastructure Protection 18

I. Training 21

Endnotes 25

Appendix A: Interviewees 28

Bibliography 29

[This page left intentionally blank.]

I. INTRODUCTION

Since September 11, 2001, state departments of transportation (DOTs) have been assuming a more proactive role in security and emergency management. The purpose of this Effective Practices Report is to document key lessons learned by state DOTs as they have expanded their security responsibilities.

This report is part of a Federal Highway Administration (FHWA) transportation pooled fund research project to develop a transportation security plan for the Pennsylvania Department of Transportation (PennDOT). FHWA asked the U.S. Department of Transportation's Volpe Center to assist PennDOT in developing a strategic approach to improving its existing security efforts. This project – funded by Pennsylvania, Indiana, and Arizona – produced three separate volumes:

- Volume I: A review of the current state of PennDOT's security planning. This includes the findings from extensive interviews with staff from PennDOT and other relevant agencies, as well as a review of PennDOT's existing security documents.
- Volume II: This Effective Practices Report.
- Volume III: A list of specific recommendations for PennDOT. This was developed from the findings of the first two phases of work.

This report, Volume II, documents key lessons learned by state DOTs as they have expanded their security responsibilities. Volpe Center staff interviewed security officials from seven state DOTs, chosen because of their agencies' reputations for being advanced in the field of security planning, as well as selected federal transportation and security officials involved in security planning. Volpe Center staff also conducted a review of reports concerning state transportation security planning efforts.

The research process generated approximately 30 key findings, detailed in this report. For clarity, they have been organized into nine broad themes relating to state transportation security planning:

1. Overall strategic direction
2. Organizational structure
3. Roles and responsibilities
4. Relationships with external agencies and transportation providers
5. Plans and procedures
6. Communications
7. Intelligent Transportation Systems
8. Infrastructure protection
9. Training

The findings of this report are summarized in the table below (Table 1).

Table 1: Findings Organized by Theme

A. Overall Strategic Direction
A.1 Build a business case to explain the importance of transportation.
A.2 Make sure the DOT plays an integral role in state security planning efforts.
A.3 Recognize that security is an important ongoing priority.
A.4 Integrate security into an "All Hazards" emergency management approach.
A.5 Actively seek out resources to support the security effort.
B. Organizational Structure
B.1 Establish a formal security and emergency management program with a core group of dedicated staff.
B.2 Provide the security function with substantial organizational authority.
B.3 Tailor the security organization to the department's internal organizational structure and the state's security and emergency response needs.
B.4 Develop a multidisciplinary staff with the appropriate range of skills.
C. Roles and Responsibilities
C.1 Ensure DOT staff people understand their roles and are prepared to fulfill their responsibilities regarding security and emergency management.
C.2 Make sure to understand the needs and expectations of other agencies.
C.3 Play an active role in evacuation planning, including cross-jurisdictional evacuations.
D. Relationships with External Agencies and Transportation Providers
D.1 Establish good institutional and personal relationships at federal, state, regional, and local levels.
D.2 Pay particular attention to fostering relationships at the regional/local level.
D.3 Do not limit relationships to those within the public sector.
E. Plans and Procedures
E.1 Develop plans and procedures for security and emergency management.
E.2 Undertake periodic evaluations and updates of security and emergency management plans.
E.3 Include the protection of key information as an essential component of a security plan.
E.4 Develop plans to ensure continuity of operations during emergencies and/or adverse conditions.
E.5 Have a plan for communicating with the public.
F. Communications
F.1 Establish interoperable and redundant communication systems.
G. Intelligent Transportation Systems (ITS)
G.1 Use ITS as a key resource for security planning and incident response.
G.2 Expand the role of TMCs/TCCs to include 24/7 operations and/or serve as an EOC.
H. Infrastructure Protection
H.1 Use the AASHTO methodology to prioritize assets, assess vulnerabilities and risks, and develop potential countermeasures.
H.2 Include staff from other agencies on Threat and Vulnerability Assessment (TVA) teams.
H.3 Be cautious about large capital investments in security.
H.4 Devote additional effort to highest priority critical assets.
I. Training
I.1 Provide all DOT staff with, at minimum, basic terrorism awareness training.
I.2 Provide supplemental security training, based on job responsibilities.
I.3 Perform exercises to test response.

II. EFFECTIVE PRACTICES

In response to the increased threat of terrorism, state departments of transportation (DOTs) have been focusing on security as a critical component of their planning and operations. This includes:

- Incorporating engineering-oriented security considerations into system-wide planning as well as the design, construction and maintenance of transportation facilities;
- Identifying and implementing policies, procedures and technologies that will assist with the detection, mitigation and response to acts of terrorism; and
- Preparing responses for a broader range of emergency situations.

The purpose of this Effective Practices Report is to identify steps as well as options a DOT can employ to develop and sustain a security program. The report contains a variety of approaches and techniques that have worked for different states. Each DOT, however, faces a particular set of circumstances and challenges. What works well in one state may not work well in another; each DOT must determine which strategies will most effectively address its particular needs.

This report is the result of interviews with state DOT and federal transportation and security officials involved in security planning, conducted in January and February 2004, and of a review of reports on state transportation security planning efforts.[1] The following state DOTs were contacted for this research, chosen based on the recommendations of staff from the American Association of State Highway and Transportation Officials (AASHTO) as state DOTs who are advanced in the field of security:

- Illinois
- Maryland
- Missouri
- New Jersey
- Texas
- Virginia
- Washington

Additional interviews were also held with officials from AASHTO, the Federal Highway Administration (FHWA), the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA). The reviewed reports are from a variety of sources, including AASHTO, the Transportation Research Board (TRB), TRB's National Cooperative Highway Research Program (NHRCP), the Institute for Transportation Engineers (ITE), and the federal government.

The research process generated approximately 30 key findings, detailed in this report. For clarity, they have been organized into nine broad themes relating to state transportation security planning:

1. Overall strategic direction

2. Organizational structure
3. Roles and responsibilities
4. Relationships with external agencies and transportation providers
5. Plans and procedures
6. Communications
7. Intelligent Transportation Systems
8. Infrastructure protection
9. Training

Findings

A. Overall Strategic Direction

A.1 Build a business case to explain the importance of transportation.

Almost every DOT interviewed stated the importance of emphasizing the critical nature of transportation's role in state security. As one DOT official reported, "Transportation is very robust, and people take us for granted, particularly with respect to the highways. They need to understand how important transportation is and that transportation needs to be at the table [for security planning]." The senior staff of state DOTs need to demonstrate to state officials the importance of transportation as part of an effective homeland security strategy. State officials will then be more willing to channel resources to bolster DOT-sponsored transportation security efforts.

When building a business case for the importance of transportation, interviewees cautioned DOTs to look at transportation as a comprehensive system beyond just the DOT's assets. "Don't have blinders on that say 'we only deal with state DOT bridges and highways,'" said one; instead, look at all transportation assets and impacts at local, regional, statewide, super-regional, and national levels. Understand the commercial relationships within the state and the economic impact of the transportation infrastructure. As the executive director of FHWA, Bud Wright, points out, "The surface transportation system is vital to our economy, defense, and quality of life, and it is extremely vulnerable to attack due to its enormity and accessibility."[2] AASHTO's Blue Ribbon Panel on Bridge and Tunnel Security estimates that the "loss of a critical bridge or tunnel at one of the numerous 'choke points' in the highway system could result in hundreds or thousands of casualties, billions of dollars worth of direct reconstruction costs, and even greater socioeconomic costs."[3]

DOTs have used documentation of the importance of transportation in homeland security and economic stability to benefit their security planning. In one state, transportation assets were previously ranked near the bottom of all the state's security-related assets; the DOT has since successfully lobbied to have them moved significantly higher on the list and has secured additional funding, based on convincing arguments about transportation's importance. Another DOT acquired more resources for its security efforts by performing numerous analyses of the security needs of the state and demonstrating transportation's role; state officials recognized transportation's importance and directed resources accordingly.

A.2 Make sure the DOT plays an integral role in state security planning efforts.

Interviewees stressed that it is critical not only to build a business case for the importance of transportation, but also to actively market this business case and to become a full player within the state's security and emergency management community. As one interviewee stated, "You need to be proactive and always be an advocate for the transportation world." Another added, "Once a DOT has made its role understood and has earned the respect of the community, it can impress upon people the importance of preparedness."

To keep transportation in the forefront of security planning efforts, it is particularly important to establish strong relationships with the state's homeland security apparatus. Multiple interviewees mentioned how helpful it has been to have the support of the governor when trying to expand the transportation security effort. Several DOTs pointed out how their relationships with other officials and agencies have helped them increase the resources directed to transportation security. As one interviewee reported, "Transportation is at the table, and we fight for every dime we get."

A.3 Recognize that security is an important ongoing priority.

DOTs have realized that security is a full-time responsibility if it is to be done well. An interviewee summed up the situation as, "You need to do security consistently, forever." For many DOTs, this involves a major commitment of staff and funding, and may require a significant cultural change on the part of the agency.

Traditionally, security has been a secondary consideration at most DOTs. Incident and emergency management have rarely received top management priority and are typically conducted as fragmented, part-time reactive activities. In order to deal with security effectively, interviewees stressed the importance of establishing a formal, structured program with a dedicated budget, clear performance goals, accountabilities, and lines of authority.

In states such as Virginia, transportation agencies have even worked to embed security mandates in state policies and legislation, to ensure resources do not vary with changes in political administrations or during times of perceived diminished threat.

A.4 Integrate security into an "All Hazards" emergency management approach.

Instead of having separate plans for each threat, all the DOTs interviewed recommend building off existing emergency planning efforts and incorporating security into an "All-Hazards" approach. This involves preparing an agency to respond to an event, whether natural or man-made, based on the consequences of the event rather than the cause. The same fundamental approach is taken to address any type of emergency. In those instances where a particular emergency may require a modified or expanded approach, additional sections can be added to the basic emergency management plan. Some DOTs, for example, have added plans specific to terrorism.

Using an "all hazards" approach can be more efficient since, as one official pointed out, "Two-thirds to three-fourths of security is good incident management." Another stressed, "Do not reinvent the wheel. There is no benefit, and potentially much harm, in adopting new programs if existing ones will do."

While the basic structure of "All-Hazards" plans offers a foundation for developing a coordinated response to a terrorist incident, DOTs should be aware that this approach can be more complex to implement. Different response requirements, cooperation with additional agencies, and additional internal coordination significantly increase the workload for agency staff.

A.5 Actively seek out resources to support the security effort.

Securing adequate and sustainable resources to support the security effort is a key element of state DOT security programs. Roughly half of the DOTs interviewed have staff people specifically tasked to identify and pursue research-oriented and other grants, Department of Homeland Security initiatives, and other funding opportunities to bolster DOT security efforts. DOTs also recommended working with Metropolitan Planning Organizations (MPOs) to secure Federal Highway Administration (FHWA) funds. Participation in FHWA workshops is another option that has helped some DOT security programs gain access to new resources, simply through networking with other participating agencies and learning about additional funding opportunities.

Focusing on expenditures that can have multiple benefits is particularly effective in advocating for security funding. DOTs have concentrated on targeting projects, such as Intelligent Transportation System (ITS) networks, that serve an everyday operational purpose as well as supporting security goals for communicating with and directing the traveling public. Similarly, scheduled bridge upgrades or a seismic improvement program can be adapted to add security-oriented design features. These are investments that can both provide everyday benefits and improve security.

B. Organizational Structure

B.1 Establish a formal security and emergency management program with a core group of dedicated staff.

Interviewees emphasized the criticality of having a group of staff people whose sole responsibility is security and emergency management. Both the literature and interviewees argued that a formal program structure with dedicated staff is essential to carry out the type and levels of improvement necessary for an effective security and emergency management program. A separate program also makes it easier to measure performance and costs.

Several DOTs have used this approach with great success. Their security and emergency management staff members are dedicated to security and emergency management full-time, and have no adjunct set of responsibilities. This empowers them to spend more time on activities such as planning, coordinating with other agencies, and training.

The size of the dedicated security and emergency management staff varies among DOTs, depending on the circumstances in each state and perceived needs: Among the DOTs interviewed, the smallest security and emergency management staff consists only of people working on security and emergency management part-time; the largest security and emergency management staff has approximately 30 full-time people; and the majority have 1-2 full-time security and emergency management staff, with some additional part-time help.

B.2 Provide the security function with substantial organizational authority.

Interviewees stressed that the staff responsible for security needs to be relatively high in the organizational hierarchy of the DOT. This is particularly important in developing relationships with key external players in security and emergency management. The staff needs to be high enough in the organization to be empowered to commit agency resources to incident management. In addition, security officials need to be positioned high enough to be invited to state and interstate security exercises and functions, including governor-appointed state security task forces. Having someone from the DOT on these task forces is key, interviewees said, not only to coordinate activities and build relationships across departments, but also to be aware of where and how resources are being allocated to the state's security efforts. Interviewees also recommended that staff person(s) have official security clearance, so they have access to confidential information that affects their jurisdiction.

Being positioned high in the DOT organizational hierarchy is also critical for garnering support and mobilizing resources internally. Implementation of security policies, procedures and programs requires extensive coordination and cooperation across a DOT. As one interviewee noted, the size of the staff does not always matter, as long as the people responsible for security have sufficient authority within the agency.

B.3 Tailor the security organization to the department's internal organizational structure and the state's security needs.

Interviewees did not feel there is a single "best practice" organizational model for addressing security. Each state's efforts will vary, depending on how the DOT is organized and what the state's security needs are. Even among the DOTs interviewed, there were significant variations in organization and staffing:

- The staff in charge of security is positioned within three levels below the Secretary of Transportation.
- The security of roads, bridges, and tunnels ("horizontal" infrastructure) and the security of DOT buildings, voice and data communications systems, and work vehicles ("vertical" infrastructure) may be addressed together, or separately with responsibility divided among multiple divisions within the agency.
- Responsibility for security may be strongly centralized within the DOT, or may be district-oriented with the central office providing assistance and support to the regional offices.
- Staff may be dedicated full-time to security, they may split their time with other DOT responsibilities, or there may be a mix of both.

One DOT, for example, has three branches within its security effort: transportation protection and security, critical infrastructure information, and its emergency operations center. Additionally, each of the DOT's district offices has one person with part-time overlay security duties who serves as the security liaison between the central office and district office. A different DOT has Emergency Response Managers (ERMs): two to three people from each DOT district office who have ancillary security duties. The ERMs cover all of the state's geography and are convened for meetings as needed. In a third DOT, groups of people

with particular capabilities, such as bridge inspection, have been designated as special teams that can be deployed anywhere in the state on very short notice to respond to emergency situations.[4]

B.4 Develop a multidisciplinary staff with the appropriate range of skills.

It takes a broad set of staff skills to implement and manage an effective security program; program managers should work to establish a strong multidisciplinary staff over time. The following are those knowledge, skills and abilities specified by interviewees as being helpful for security programs:

- Law enforcement and/or military experience;
- Technology/information systems knowledge;
- Knowledge of the state transportation system;
- Management and operations knowledge;
- Knowledge of the procurement system;
- Experience identifying funding and writing grants;
- Emergency response knowledge;
- Knowledge of multiple transportation modes;
- Facilities protection knowledge;
- Cyber security knowledge;
- Engineering training and experience in dealing with security issues; and
- Experience with threat and vulnerability assessments.

C. Roles and Responsibilities

C.1 Ensure DOT staff people understand their roles and are prepared to fulfill their responsibilities regarding security and emergency management.

Interviewees stressed the importance of clearly communicating the roles and responsibilities of staff with regards to security and emergency management. For instance, while DOT employees may not be formally designated as "first responders", they are often the first to reach an incident scene, and therefore need to know what they should and should not do in different types of situations. One DOT surveyed its staff members to get a realistic assessment of their understanding of their security and emergency response roles and responsibilities. The two key questions asked were: (1) if staff members were aware of what would be asked of them in security and emergency management situations, and (2) if staff members would show up to perform their jobs during an emergency. A high proportion of employees responded positively to both questions.

Interviewees recommended that DOTs identify those personnel that need to be available during an emergency ("essential" personnel) and clearly define their roles and responsibilities. It was also recommended that DOTs prepare, distribute and regularly update

lists of after hours contact numbers to ensure that those DOT personnel who may be required to work during emergency situations can be reached.

When designating emergency personnel, DOTs should plan for redundancy. For example, one state DOT interviewee found that one of its district's response plans failed to account for the possibility that an emergency could directly affect staff people or their families, in which case they would not be expected, or might not be able, to work. In this instance, the DOT's central office helped the district develop a protocol for obtaining additional personnel from other districts. Other sources also recommended that DOTs in adjoining states develop policies and procedures for sharing personnel and resources during emergency situations.

A method which many DOTs have found helpful in clarifying roles and responsibilities, particularly with regard to inter-agency coordination, is training in Incident/Unified Command Systems (ICS or UCS). Incident and unified command systems outline chain of command and help overcome coordination problems among multiple agencies responding to an emergency.

In addition to clarifying roles and responsibilities, DOTs should define decision-making power in emergency situations: who is authorized to make what kinds of decisions in what circumstances, and how decisions should be communicated. In the Volpe Center's case study of the effects of catastrophic events on the transportation system, many transportation officials stressed the need to empower field staff to make decisions during an emergency, particularly when there is a loss of communications between managers and field staff. Interviewees from New York City, for instance, reported that it was helpful on September 11, 2001 for field staff to be able to make operating decisions on their own in the absence of communications from headquarters.[5]

C.2 Make sure to understand the needs and expectations of other agencies.

Some of the confusion about DOT roles and responsibilities is due to a lack of planning and/or communication among agencies involved in security and incident response. Interviewees stressed the importance of both understanding other agencies' expectations and clearly communicating to other agencies what the DOT can and will do. "Don't assume anything," said one official; contact other agencies and ask them what they are expecting from the DOT in the event of an emergency.

In some cases, external agencies may have unrealistic expectations regarding a DOT's authority, which can cause problems during a response. If expectations are unreasonable, it is much better to address them ahead of time rather than when an emergency actually occurs. One DOT, for example, found that some external agencies had developed their own security plans involving DOT assistance, in this case relating to the Homeland Security Advisory System, without consulting the DOT: Airport officials informed the DOT that the airport emergency plan relied on the DOT to close the off-ramp to the airport in certain situations, something the DOT was unwilling to do.

Interviewees cited expectations about what equipment and materiel their agencies are able to provide as another issue needing clarification. Making a list of DOT resources may help other agencies see what resources are available to them through the DOT and where in the state they are located. Many sources recommend that a DOT develop a specific list of equipment, including information on where the equipment is located, and how many of each

item is available. Such a list can also be the basis for establishing a protocol among agencies for obtaining additional resources in emergency situations.

By talking with other agencies, DOTs can not only uncover mismatches in expectations, but can also identify gaps in communications and/or planning. The following are examples of gaps identified by participants in FHWA regional workshops of transportation and emergency management personnel:[6]

- Quarantine situations: "In almost all regions, the enforcement of a quarantine situation was identified as an issue. Most regions indicated there was clear authority by someone in government to enact a quarantine but there was almost universal agreement that there were no plans in place as to how to enforce a quarantine."[7]
- Surveillance of critical infrastructure: "While many agencies have identified certain infrastructure as vulnerable, they have not established a method by which they or their law enforcement agency will routinely monitor that infrastructure nor how they will check it for safety if a terrorist threat is received or the threat level elevated. Further, there does not appear to be a coordinated effort among agencies to communicate their findings once those checks have been completed."[8]
- Closing of highways: It is not always clear who has authority to close the interstate system in an emergency. While many DOTs know who has the authority in their own state, they do not know who has the authority in adjoining states.[9]

By becoming aware of these issues, DOTs can work with other agencies to resolve them before an incident occurs.

C.3 Play an active role in evacuation planning, including cross-jurisdictional evacuations.

One aspect of security in which DOTs can play a key role is evacuation planning, particularly at the regional scale. Interviewees were quick to point out that DOTs are one of the few types of agencies with control over statewide infrastructure that is essential for evacuations.

In the FHWA regional workshops, evacuation planning emerged as an issue needing improvement: "Many regions have not designated emergency or evacuation routes to be used in the event of an emergency, particularly a terrorist incident. While some regions have identified routes to be used to re-route traffic in the event of an incident such as a vehicle crash that involves a road closure, these route plans are often very localized and do not address the need for a regional evacuation. Many evacuation plans are prepared at a county level and are not coordinated across county lines or state boundaries, creating an incomplete and/or inconsistent evacuation route system."[10]

A number of DOTs interviewed said that they collaborate with neighboring states and regions on such activities as evacuation planning. This can be particularly important where large cities or critical infrastructure, such as bridges, are located on state boundaries. A side benefit of the coordination around evacuation planning, according to one interviewee, is that it has encouraged more overall collaboration and sharing of information about security issues.

A successful example of a regional evacuation planning initiative is the I-95 Corridor Coalition (http://www.i95coalition.org), which includes transportation authorities and

organizations from 14 states and the District of Columbia, and allows for the rapid exchange of traffic information in the Northeast and mid-Atlantic United States. The ability to quickly disseminate regional information in an emergency has proven valuable, as this resource was used extensively during and after the September 11th terrorist attacks.[11]

Efforts have even expanded to a nationwide scale. The Evacuation Traffic Information System (ETIS) is a new system in which some states are participating. Its goal is to provide an evacuation database with information available for all states. This allows states to be notified of events in other states that may affect their own traffic.[12]

D. Relationships with External Agencies and Transportation Providers

D.1 Establish good institutional and personal relationships at federal, state, regional, and local levels.

Almost every interviewee focused on good working relationships with other agencies at all levels of government as a fundamental aspect of successful security planning. By having prior relationships and knowing your partners when an emergency occurs, response activities will be better coordinated and the overall impact of the emergency will be mitigated. As one interviewee stated, "Five minutes before the music starts is not the time to learn how to dance."

In addition to working closely with emergency management and law enforcement agencies, sources recommended that DOTs establish relationships with other, less obvious agencies. Likely candidates include state health departments, who look to DOTs for help in moving medical supplies and managing quarantine situations, and regional and local planning agencies who can channel funding to certain emergency response functions such as ITS systems and evacuation planning. Transit agencies also tend to be overlooked in emergency transportation plans, even though they are critical to response and recovery.[13] On the federal level, interviewees recommended that DOTs establish relationships with the FBI's local or regional Joint Terrorism Task Forces, FHWA headquarters and field offices, and Department of Homeland Security (DHS), in particular the Office of Domestic Preparedness and Border and Transportation Security.

Relationships can be formal or informal, depending on the DOT's circumstances. Many transportation officials encourage the establishment of formal interagency Memoranda of Understanding (MOUs) or Memoranda of Agreement (MOAs), particularly to document the resources that each local, state, region, and federal agency may provide during emergency response and recovery efforts. MOUs and MOAs can take many different forms and may include the following elements:[14]

- A list of participating agencies, including contact information of approving officials;
- Definition of jurisdictional boundaries for primary responding organizations;
- Detailed definition of the chain of command and control, communication, and evacuation procedures to be followed at the scene of the incident;
- A statement to address potential changes in protocols;

- Identification and description of equipment resources to be made available for incident response;
- Description of personnel and their duties;
- Training and exercise responsibilities;
- Provisions for revision(s) to the MOU; and
- Provision for the identification and documentation of costs to be tracked for potential reimbursement.

D.2 Pay particular attention to fostering relationships at the regional/local level.

Interviewees repeatedly pointed out that all incidents start locally, and therefore an effective DOT should cultivate good relationships with agencies at the local level in order to coordinate their emergency planning and response efforts. A key finding of case studies done by the Volpe Center for FHWA on the effects of catastrophic events on the transportation system is that relationships established during normal times are critical to emergency management success.[15]

DOTs have fostered institutional relationships in many ways. A common suggestion is to hold interagency and cross-jurisdictional meetings to develop joint plans or conduct joint training exercises. These meetings not only help refine emergency planning strategies, but they are also invaluable in helping DOT staff get to know their counterparts in other agencies.

Another method of collaboration is to co-locate staff or facilities. One DOT reported that they invited the state Highway Patrol to share facilities in a number of their county DOT offices. They even have a staff person from a neighboring state's Highway Patrol in their office where a large city is located on the shared border between the states. Some DOTs are doing this with their operations control centers; the Virginia DOT (VDOT) is jointly planning a Public Safety and Transportation Operations Center that will house facilities for VDOT, the Virginia State Police, and Fairfax County 911 and Emergency Management services.

D.3 Do not limit relationships to those within the public sector.

While relationships with public agencies are vital, it is important to foster communications with private sector entities as well. Interviewees cited the expertise and experience of all transportation providers, both public and private, as useful for developing security practices. The private sector can also provide equipment needed in an emergency. During the blackout of August 2003, private fleets were available to assist in the movement of stranded commuters, as a result of a memorandum of understanding between New Jersey Transit and private carriers.[16]

By determining which private sector companies can provide support in emergency response and setting up agreements and contracting procedures in advance, DOTs can save time and money during crises. In one region participating in FHWA emergency operations preparedness and response workshops, the local Committee of Heavy Contractors assembled and published a brochure that lists all the contractors in the region, their contact information

and the types of resources they have available, such as trucks, barrier walls, cranes, etc. Participants reported "the brochure enables the DOT and other agencies to have resource information at their fingertips that is invaluable in responding to an emergency quickly."[17]

Another potential area of cooperation with the private sector is around evacuation planning. DOTs have found it helpful to coordinate evacuation plans with large employers in local areas, to enable an evacuation of the local workforce to occur smoothly.

E. Plans and Procedures

E.1 Develop plans and procedures for security and emergency management.

The importance of advance planning and preparation cannot be emphasized enough. As one DOT official stated, "Planning minimizes the range of confusion by establishing what's going to happen and who's going to do what. In an emergency situation, this can save critical time."

As mentioned earlier in this report, interviewees recommended that security be incorporated into existing emergency planning efforts (an "All Hazards" approach). Plans specific to terrorism's unique threats should be added to basic emergency management plans. Another theme from the research is that plans should be supplemented with formalized standard operating procedures (SOPs), so response to security and emergency situations will be consistent, predictable, and understood by all DOT personnel and other collaborating agencies.

For example, a number of DOTs have developed a checklist of actions, similar to an SOP, to be taken by their personnel for each Threat Condition of the Homeland Security Advisory System (HSAS). Several interviewees identified the checklist developed by the State of Washington's DOT as a benchmark among these types of documents.

Interviewees suggested that, since local conditions can vary across a state, DOT districts should be encouraged to modify security plans and HSAS checklists to target their particular security issues. One DOT's central office addressed this by establishing minimum requirements for district security efforts, and then having each district supplement the requirements as needed; other states have each district develop its own security plan, based on a framework provided by the central office for guidance. Interviewees also recommended that DOTs coordinate their SOPs/HSAS checklists with other state and local agencies and, if possible, neighboring states.

E.2 Undertake periodic evaluations and updates of security and emergency management plans.

Interviewees warned that having security and emergency response plans is not enough; these plans must evolve to address changes in threats and a DOT's response capabilities and to incorporate lessons learned from exercises and actual events. One official described his agency's policy: "Plan, drill, exercise, then rework the plan and do it again."

Several reports similarly advise DOTs to undertake regular audits, to assess security policies and to ensure that actual procedures are in compliance with the DOT's plans. A report from Harvard University cautions that new plans of action "must include mechanisms for

systematic evaluation of their effectiveness over time. Unless some means of determining what is working and what is not are in place, states and localities run the risk of confusing action with success."[18]

As the Volpe Center points out in its case studies, after any emergency it is key that agencies that worked together meet to evaluate their performance. The Volpe Center points to two reviews conducted after the blackout of August 2003 as examples. First, staff members from the Ambassador Bridge, the Detroit-Canada Tunnel Corporation, U.S. and Canadian customers, local law enforcement agencies and other entities held a transportation debriefing to discuss issues such as backup power generation, coordinated radio communications, Emergency Operations Centers (EOCs), and communications with the public. Second, transportation and emergency response agencies formed the Trans-Hudson Emergency Transportation Task force to deal with issues of moving people from New York City to New Jersey.[19]

E.3 Include the protection of key information as an essential component of a security plan.

Interviewees identified the protection of critical information regarding state transportation assets and procedures as an important issue for transportation security. A terrorist could use sensitive information to identify effective targets or determine how to circumvent security and response measures in use by the DOT and other agencies. For these reasons, certain documents should not be available to the general public.

Shielding information is not always a straightforward process. It can be difficult for public agencies to avoid public disclosure, since the open records laws in many states require that many types of documents be made public. Several sources stressed that a DOT should be aware of document control regulations, know how to protect key information within the context of its state's Freedom of Information (FOI) laws ("sunshine laws"), and develop policies for releasing information to other agencies and private contractors.

One DOT, for example, has an entire division of its security effort dedicated to the handling of secure documents. Another DOT successfully lobbied its state legislature to amend the FOI law so certain plans do not have to be shared with the public. Other states have laws that establish a "need-to-know" clearance that covers most confidential information. The Virginia Freedom of Information Act contains a number of exclusions for information related to transportation infrastructure and business reports.[20] Additionally, TSA has the ability to classify documents as SSI under USC § 49 CFR Part 1520, and has expressed a willingness to help state agencies shield their documents.

E.4 Develop plans to ensure continuity of operations during emergencies and/or adverse conditions.

Continuity of Operations (COO) or Continuity of Government (COG) plans are an important part of security planning. Continuity of Operations plans should address not only operational concerns, such as identifying alternate sites where staff can convene, but also backup options for the technology within facilities. The Volpe Center case study of catastrophic events emphasizes the need to build redundancy into institutions and physical systems. The report recommends that, "At a minimum, emergency response planners should consider designing redundancy into the system in several areas: the regional transportation network, agency

personnel, communications and utilities, control centers, and equipment and supplies."[21] They point out that New York City's Office of Emergency Management had been located in the World Trade Center; a temporary office had to be relocated three times on September 11, 2001.

Similarly, ITE emphasizes the importance of redundancy in the recovery phase. They recommend that DOTs focus on redundancy for transportation facilities, communication equipment, transit facilities, and ITS systems;[22] this includes DOT state-, district- and county-level facilities.

A lesson learned during the blackouts in 2003 is that while planning is good, there is no substitute for actual practice and testing. DOTs should regularly test their critical support systems, such as backup power supplies, to ensure their reliability in emergencies. Some agencies had backup equipment failure due to lack of proper maintenance (e.g, regular checks of backup battery charge status).

E.5 Have a plan for communicating with the public.

Interviewees pointed out that the traveling public and commercial carriers are a DOT's customers; the DOT therefore needs the ability to communicate with the groups it serves. This is particularly true during emergencies when road closings and transit service changes can occur frequently and significantly impact normal travel routes. Information must be given to the public and the media as quickly as possible to avoid rumors and address concerns. On September 11, 2001, for example, inaccurate information was disseminated that the Washington, D.C. Metrorail was closed. As a result, more people walked instead of taking the subway, which added to the congestion.[23]

A DOT needs to anticipate what the transportation consequences of an event will be, and disseminate information to reduce the impacts of the incident. Some recommendations on how to deal with the media and public include the following:

- Work with the state EOC to define the specific role of DOT in providing information to the public during an emergency.
- Develop a strategy for dealing with the media, elected officials and the public during emergencies.
- Include a section in emergency response plans and procedures on how to communicate with the public about transportation service changes during and after an incident.[24]
- Develop relationships with the media prior to emergencies.

A report from FHWA regional workshops of transportation and emergency management personnel cites examples of how different agencies have approached public communications.[25] In one region the Metropolitan Planning Organization (MPO) has led an effort to identify and test a single location from which information can be disseminated in emergencies. In another region, a Joint Information Center (JIC) is being established to ensure all agencies release consistent information to the public and the media; a different region is doing the same, but with the Department of Emergency Management as the agency responsible for operating the JIC. Another region has established the local Fire Department as the responsible agency for emergency public information and two Fire Chiefs have been

assigned as Public Information Officers for all events. One DOT has a process for activating an Emergency Information Center to provide media briefings.

Other effective practices reported by workshop participants included the following:[26] a DOT can maintain a toll free telephone number as a way to provide information to the public; these can be very helpful in emergency response. Many toll free numbers use recorded messages, but some can be converted to be staffed by a live person, as needed. Agencies need to be prepared for a large volume of calls during emergencies, and should be able to staff their phone lines 24 hours a day when necessary. Most DOTs maintain a website to provide routine public information; these can be used to provide emergency information as well.

F. Communications

F.1 Establish interoperable and redundant communication systems.

A concern voiced by many interviewees and reports is that interagency communications are one of the weakest links in emergency management. As the Volpe Center case studies point out, the demand for communications is highest during an emergency - precisely the time that communications may be most vulnerable to technological failures.[27]

The importance of interoperable and reliable data and voice communications among agencies cannot be overestimated: integrated emergency response communications systems enable responders from different agencies and jurisdictions to talk to each other easily in real-time.

An FHWA document, "Lessons Learned in Emergency Transportation Operations Preparedness and Response," highlights some of the communications problems facing DOTs. It reports that while some first responder agencies can communicate on a common platform, transportation agencies are often not part of the shared network. DOTs typically have their own internal communications networks, but communications equipment may not be available in all vehicles that are used in emergency response. In addition, some forms of communication have limited application outside of normal business hours. Finally, DOTs may rely on communications systems for which there is little redundancy, so that if cell phone service, electricity or land phone lines are not functional in an emergency, they have limited alternatives.[28]

In the absence of an interoperable communications device, the security coordinators of several DOTs interviewed said they rely on redundant combinations of communication devices to communicate with law enforcement: cell phones, satellite phones, pages, and radios in their cars. The hope is that they will always be able to contact the necessary person via at least one of these options. The Volpe Center case studies found that the more communications options available to an agency, the more likely the agency would be able to operate during an emergency. In each of the catastrophic events the Volpe Center studied, at least some technologies failed and the technologies that worked continually varied from event to event.[29]

Transportation managers are adopting a variety of new technologies for emergency situations. These include: mobile communications and command centers with satellite and computer technology; global satellite phones; secure websites for security-related information; instant messaging programs; and walkie-talkies incorporated into cellular phones.[30, 31] Interviewees in the Volpe Center study also stressed the importance of older

technologies, such as facsimile machines, pagers, 800 numbers and conference call lines, older radio systems and dedicated landlines to communicate within and among agencies.[32]

Another option is to use government sponsored priority communications systems, such as Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS). These two services provide pre-approved users with priority routing of landline (GETS) and wireless (WPS) calls during emergencies.[33]

Finally, another effective practice is to provide training or drills on communications protocols for emergencies. Some agencies have developed specific procedures and conducted training for employees on what to do in an emergency when non-standard communications equipment fails.[34]

G. Intelligent Transportation Systems (ITS)

G.1 Use ITS as a key resource for security planning and incident response.

Advanced traffic management technologies are not only useful for everyday operations; they can also provide aid in emergency response and incident monitoring. Intelligent Transportation System (ITS) devices, including signals, cameras, radios, web sites, message signs, and highway advisory radio, can play a significant role in security planning and emergency response.

Once a catastrophic event has occurred, ITS technologies can aid in providing information about existing conditions to decision makers internally, as well as to external agencies and the public. Consideration, however, must be given to how ITS information can be collected and shared effectively. ITE states that the most important step is to enable ITS traffic management centers to share data and video with state or local EOCs.[35] This can be accomplished through shared feeds from traffic cameras and other devices. One interviewee said that his state's EOC even has a dedicated computer terminal linked to the DOT's ITS system. On September 11, 2001, TRANSCOM's multi-agency communications capability proved its value in keeping multiple New York City agencies up to date regarding post-incident travel conditions. ITS traffic management features were also used to enable reverse traffic flows and special emergency access in some areas.[36]

Unfortunately, situations such as those described above are not the norm. The FHWA found that, in general, ITS capabilities have not been incorporated into emergency planning; some emergency response agencies are not even aware of the ITS capabilities within their region or how they can be employed in emergency situations.[37] As DOTs invest in ITS technologies, they need to think about how to take advantage of the technologies for security-related surveillance and incident response as well as everyday traffic control and communications.

As DOTs increase their use of ITS equipment, they should also consider how to protect these systems to ensure their continued operation during catastrophic events. The 2003 blackout demonstrated the vulnerability of advanced technology to the loss of power both in the field and at the control centers. As one official pointed out, without power ITS data "go right in the wastebasket, during a time when you could ultimately use it the most."[38]

G.2 Expand the role of TMCs/TCCs to include 24/7 operations and/or serve as an EOC.

Interviewees pointed to traffic management centers (TMCs/TCCs) as a resource that is often not leveraged for security and emergency response. They recommended that TMCs/TCCs have the functional flexibility to be converted to EOCs during incidents. The FHWA report on its regional workshops on emergency transportation operations preparedness and response cites some of the benefits of such an arrangement:

In some regions, the TMC serves as an EOC or is co-located with the statewide EOC. These arrangements allow for close coordination between the DOT and their counterparts in emergency response and allow the ITS resources operated from the TMC to be quickly employed for emergency response. In addition, the TMC resources such as surveillance (CCTV) cameras can be used to monitor critical infrastructure, especially in the case of heightened threat level conditions. In at least one state, the DOT maintains an Incident Management Manual that identifies specific personnel to staff the EOC.[39]

Enabling a TMC to function as an effective EOC requires forethought in its design and operation. One of the primary issues is operating hours: some DOTs already have their TMCs/TCCs operate on a 24-hour schedule, while many do not. The facility should have the ability to receive and process information (along with real-time visual images) on an ongoing basis and may need access to special agency information systems, such as purchasing, design, and personnel, during emergency situations. Some interviewees' TMCs have workspaces to accommodate staff people from other agencies, both during standard peak hours and during emergency situations. The FHWA references one state TMC that even has a fully licensed radio station to provide traffic information.[40]

As with ITS equipment, a DOT should take reasonable steps to ensure the TMC/TCC is protected, since it could be considered a target by terrorists. Measures could include perimeter security, hardening, and data security.

H. Infrastructure Protection

H.1 Use the AASHTO methodology to prioritize assets, assess vulnerabilities and risks, and develop potential countermeasures.

Formal threat and vulnerability assessments are becoming a standard component of DOT security programs; according to the FHWA, most transportation agencies have done at least a preliminary assessment to determine what infrastructure is vulnerable.[41] A number of interviewees who have performed these assessments for their states recommend using AASHTO's vulnerability assessment document, *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection,*[42] as a framework. One DOT official advised agencies who use AASHTO's Guide to "stay the course of the tool; carry through the entire process."

AASHTO/NCHRP is currently in the process of revising and enhancing the Guide to make it applicable to a broader range of assets than transportation. The current version of the Guide outlines six major steps for conducting a vulnerability assessment (Figure 1[43]). The first step is to identify the transportation assets that are critical to the DOT's mission. AASHTO recommends looking at four categories of assets: 1) infrastructure, such as highways, bridges, tunnels and overpasses; 2) facilities, such as buildings, maintenance yards, rest areas, and weigh stations; 3) equipment, which includes vehicles, signal and control systems, variable message systems, and communications systems; and 4) personnel, which includes DOT employees, contractors, and vendors. The Guide provides sample factors for ranking these assets (e.g., consequences to the economy, the military, the public, emergency response if the asset is damaged or lost; replacement cost and downtime) and developing a prioritized list. AASHTO cautions states to limit the list of critical assets--the more assets deemed critical, the more time and resources needed to complete the assessment. Interviewees noted that the process of determining the cut-off point for the assets to be assessed is somewhat subjective, depending on factors such as state size, total number and type of assets, and agency budget.

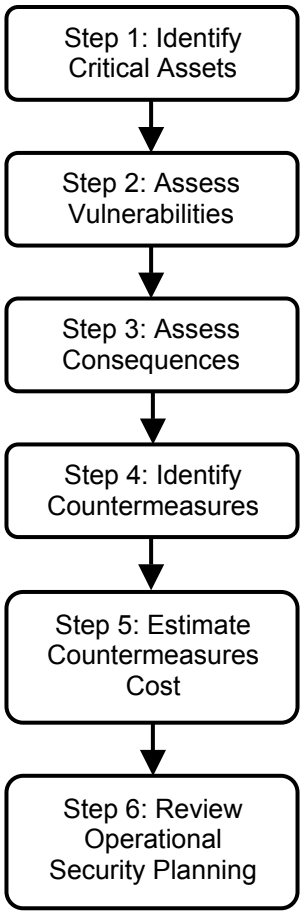


Figure 1: Six steps for conducting a vulnerability assessment[44]

The second step of the process is to systematically identify and evaluate the critical assets in terms of their susceptibility to attack. Vulnerability factors include the visibility of the asset, including the level of recognition and the number of people typically present; the ability to gain access to the asset; and the presence of site-specific hazards, such as chemicals or explosives.

Step three integrates steps one and two by plotting the criticality and vulnerability scores on a matrix. As Figure 2 shows, the objective is to identify those assets that are high in both criticality and vulnerability.[44]

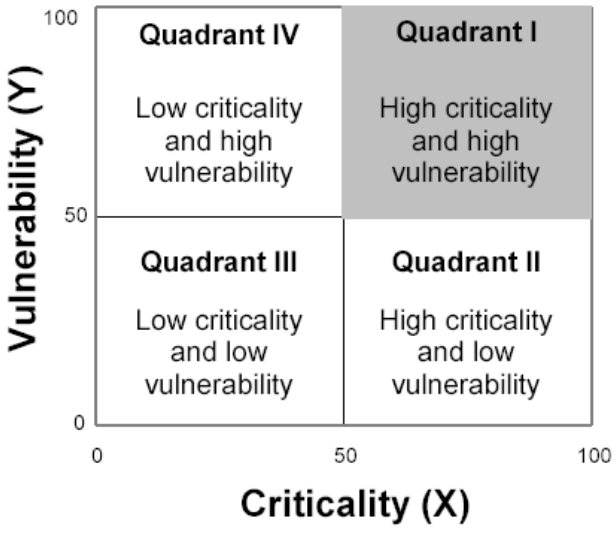


Figure 2: Criticality and Vulnerability Matrix[45]

Step four entails the identification of potential countermeasures for deterrence, detection and defense. AASHTO recommends mapping countermeasures to high-priority critical assets and assessing whether proposed countermeasures will reduce threats and vulnerabilities to these assets.

Step five is the development of cost estimates for implementing the selected countermeasures. AASHTO recommends combining countermeasures into

"packages." In some cases, a single measure – like video surveillance in an urban area – will apply to multiple assets. In other cases, multiple countermeasures may be needed to protect a single asset. For example, the vulnerability of a bridge may be diminished by increasing inspection efforts, installing barriers to make access more difficult, and improving lighting.

Step six of the AASHTO methodology is to develop security operational plans. Plans can include such elements as access restrictions, procedures for implementing countermeasures, and plans and procedures for responding to security and emergency management situations.

H.2 Include staff from other agencies on Threat and Vulnerability Assessment (TVA) teams.

Interviewees stressed the importance of creating diverse and multidisciplinary threat and vulnerability assessment teams, including a cross-section of expertise and interests not only from within the state DOT but also from external agencies. Multidisciplinary teams serve three purposes: they bring perspectives from their fields of expertise; they promote consistent methodologies and understanding; and they help build interagency relationships.

In its regional workshops on security and emergency management, the FHWA found that in many cases, the "[threat and vulnerability] assessment was not done in conjunction with a law enforcement agency nor has it been shared with law enforcement agencies…In addition, the assessments were often not done in coordination with local agencies so the methods for determining vulnerabilities and how to rank the criticality of the infrastructure is not coordinated, resulting in different criteria used in the same community."[45]

DOT interviewees who had included other agencies on their TVA teams were quick to point out the benefits. One DOT official reported that they had involved an explosives expert in their team and "It was amazing to find out how vulnerable some of our assets were." Another DOT stated that intelligence personnel had helped them consider their structures from a different point of view.

AASHTO notes in its Guide that different skills, knowledge and experience are required for different steps in the vulnerability assessment process. Transportation professional in State DOTs and local Departments of Public Works (DPWs) understand mobility, transportation operations, and structural design issues. Threat experts typically reside in federal, state, and local law enforcement agencies; vulnerability experts may be design engineers, security specialists, or operating personnel familiar with control procedures and operating parameters. Personnel involved in developing mitigation strategies may be law enforcement personnel, technology vendors, engineers, security specialists, site managers, resource specialists and others who might suggest options for reducing the likelihood of attack or the impact if an attack should occur.[46]

H.3 Be cautious about large capital investments in security.

Interviewees felt strongly that DOTs should be cautious about big investments in countermeasures. One DOT official warned, "My agency could go overboard on spending and be no better off. We need to take reasonable steps to provide a reasonable level of security." Another official added that it is often more cost effective to focus on response capabilities.

All sources agree that, for new structures, it is more cost effective to incorporate security measures at the time of construction; DOTs should therefore ensure that consideration is given to security during the design phase of planned facilities. For existing structures, however, deterrence and detection measures may be more appropriate and more cost effective than structural hardening.

Examples of potential low-cost countermeasures that may generate effective improvements in security include the following:[47, 48]

- Eliminate parking under or near critical infrastructure (or limit parking to authorized vehicles).
- Improve lighting and clear overgrown vegetation, to improve lines of sight to critical areas.
- Install physical barriers to make access to critical infrastructure more difficult.
- Conduct commercial motor vehicle (CMV) inspections near critical assets to increase staff presence.
- Promote employee and public involvement in informal surveillance for bridges and other critical assets.
- Establish systems for recording who enters and exits critical facilities.

H.4 Devote additional effort to highest priority critical assets.

Interviewees from multiple DOTs agree that specific effort should be devoted to top-ranked critical assets; they feel that critical links in the transportation network deserve extra attention and effort to ensure their protection.

For instance, site-specific plans can be developed for the top assets. One DOT has these plans in place for each of their top 20 critical bridges in case they are ever damaged or destroyed. These plans can include specific details about alternative traffic or commerce routes, repair and replacement alternatives, and specific staff people who will be tasked to recovery work. This agency also recommends an on-site walk-through with law enforcement agencies and operations staff, with these plans in hand, to ensure all agencies are on the same page.

Texas DOT has developed a number of documents to assist in the protection of its critical assets. These documents include a transportation infrastructure security plan (draft), a vulnerability/countermeasures report for district staff to fill out on each of their critical assets, and emergency response procedures for district staff to develop coordinated emergency response plans for each identified critical structure within their district.

I. Training

I.1 Provide all DOT staff with, at minimum, basic terrorism awareness training.

Interviewees repeatedly stressed the importance of staff preparedness for effective security and emergency response. They believe fundamental security training needs to occur at all levels and locations of the DOT; many DOTs described staff training programs that are both

ongoing and continuous, and security education and training that is integrated into standard operating procedures.

While some types of training are for specialized groups, such as first responders or field personnel, interviewees stressed that terrorism awareness training is important for the entire staff. Such training can foster a security-conscious workforce, and training employees to be watchful for potential problems in critical infrastructure can significantly increase overall security. A survey of DOTs echoes this sentiment, stating, "State DOTs need to strengthen terrorism awareness training…State DOTs are weakest in the area of terrorism awareness training, which includes threat assessment and risk management training."[49]

The National Cooperative Highway Research Program (NCHRP) is in the process of developing a manual for DOT field personnel about responding to threats and being aware of suspicious activity; this manual will be available soon through TRB. Additionally, some DOTs have developed terrorism awareness training programs of their own. Oregon DOT (ODOT) has created a presentation entitled "Terrorism Awareness for ODOT Employees" for all of their employees. Similarly, Illinois DOT has created a "Response Handbook for Incidents, Disasters, and Emergencies (RHIDE)." Other DOTs have developed and published brochures to raise the awareness level of their employees regarding terrorism incidents. The brochures alert employees on what they should look for and what to do if they notice any suspicious activity.[50]

I.2 Provide supplemental security training, based on job responsibilities.

An additional recommendation is that staff members should receive supplemental security training tailored to specific job responsibilities, so they are better prepared for the particular types of situations they are likely to face. This goal should be approached in a manner that maximizes the ability of staff to prepare for and respond to a range of attacks or emergencies (as opposed to a general emergency situation), to minimize detrimental impacts.

One area of specialized training recommended by many sources is first responder training, including the use of personal protection equipment for biological, chemical, and radiological hazards. Most transportation agencies lack the training and proper personal protection equipment to be first responders in many hazardous situations, although they are often put in that role.[51] "The history of terrorist incidents suggests the need for more attention to the protection of first responders including their ability to recognize threat types so as to avoid hazards, and to avail themselves of personal protection equipment, hazard detectors, and decontamination facilities. Terrorist access to a wider range of weapons indicates the need to consider a wider range of hazards."[52]

States are addressing the issue of first responder training in a number of ways. One DOT has implemented all-day first responder training for new employees and an annual half-day refresher course for existing employees. Another state plans to train its frontline people on how to use the protective suits it is acquiring.

Another type of training commonly recommended for state DOTs is unified and incident command structure training. The FHWA regional workshops found that there is a lack of knowledge among DOT staff in many regions about multi-agency and Unified Incident Command (UIC) protocols. Most first responders are well-versed in this, but non-first

responder agencies (such as DOTs) feel additional training is needed if they are to operate as first responders.[53]

In addition to first responder/personal protection training and training in UIC protocols, other types of specialized training mentioned in this research include:

- Pre and post-event emergency response training
- Quick clearance and site management training
- Interagency communications training
- Employee security training
- Response and vulnerability assessment training
- Public information training
- Weapons of mass destruction training
- Hazardous materials training
- IT security training
- Advanced courses for other specializations, such as bridge or tunnel engineers, patrollers, and managers.

Research conducted for AASHTO provides some insight into effective training practices underway in various states:[54]

- Pennsylvania DOT has been noted for its Train-the-Trainer format, which involves the training of District officials who then return to their geographic areas and train District staff.
- California DOT works with a private security firm, the Governor's Office of Emergency Services, as well as the California State Training Institute, and has an internal training division that delivers training to other state agencies and private industry through a number of delivery mechanisms including presentations, simulations, videos and print media.
- Georgia DOT has created a security taskforce in tandem with other state agencies, which helps spread out the costs of creating new security training within the DOT.
- Oregon DOT uses a variety of training formats—classroom settings, video and simulated exercises— to deliver multiple training programs to both maintenance workers and executive management. AASHTO found Oregon to be one of the most innovative state DOTs surveyed in terms of its security training. Oregon is working with federal, interstate, and intrastate agencies to develop a comprehensive security training program.
- Washington DOT has developed an Employee Disaster Response Plan that divides employees up into teams that are responsible for organizing and assisting fellow employees during an emergency. They also have a training program called the Self and Family Preparedness Class that is designed for employees and their families to take action before a disaster so that employees can remain at work when a disaster strikes.

I.3 Perform exercises to test response.

All interviewees and other sources emphasized that exercises are crucial for reinforcing the lessons learned in training and for coordinating effectively with other agencies. Exercises are also a critical method for testing existing plans and determining where gaps may exist.

As a Harvard University report points out, the most effective responses to major incidents have come from people "who have developed a good plan and who exercise it on a regular basis with a variety of scenarios. There are shelves full of plans waiting to be implemented but never tested, even in tabletop or mock exercises."[55] ITE adds, "You discover things in a tabletop exercise which would never be discovered any other way."[56]

Interviewees stressed the importance of performing internal and multi-agency training often. Comprehensive training can include tabletop exercises, functional walk-throughs, and full field exercises. A fundamental goal of wide-scale exercises is to enable agencies to work together. This includes elements such as establishing chain of command, communication and information sharing, and even credential recognition. One source suggests using scenarios that are more complex, which require agencies to figure out how to cooperate effectively under difficult circumstances. Another report states that DOTs can use training to overcome a lack of familiarity with the personnel and procedures of other agencies: "Paper protocols are no substitute for face-to-face familiarity with agency partners where unanticipated circumstances call for quick, on-the-scene cooperative judgments and action. It is clear that joint training and regular exercises are an essential and continuing requirement for maximum effectiveness."[57] Yet another report states that DOTs should learn to work "as a team with other agencies or in a support role rather than being in charge. Exercises help strengthen such relationships and clarify roles."[58, 59]

One DOT has found an innovative way to foster involvement in joint exercises with other agencies. The DOT has a mobile communications center that can be deployed to incident sites. A DOT official said that other agencies always invite the DOT to their training exercises because the agencies want to have the mobile communications center involved and on-site for the exercises.

Endnotes

[1] Appendix A contains a complete list of interviewees and their agencies. The Bibliography lists the documents reviewed for this report.

[2] Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, pg. 3.

[3] The Blue Ribbon Panel on Bridge and Tunnel Security. *Recommendations for Bridge and Tunnel Security*. For the American Association of State Highway and Transportation Officials' Security Task Force. Sept. 2003, pg. 2.

[4] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 12.

[5] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004, pg. 7.

[6] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version, Apr. 2003, 20 pgs.

[7] *Ibid.*, pg. 10.

[8] *Ibid.*, pg. 7.

[9] *Ibid.*, pg. 9.

[10] *Ibid.*, pg. 6.

[11] *Ibid.*, pg. 13.

[12] *Ibid.*, pg. 12. More information about ETIS may be found at http://www.fhwaetis.com.)

[13] Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, pg. 24.

[14] FTA. *The Public Transportation System Security and Emergency Preparedness Planning Guide.* DOT-FTA-MA-26-5019-03-01. Jan. 2003, pg. 46.

[15] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004.

[16] *Ibid.*, pg. 9.

[17] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 11.

[18] Harvard University, John F. Kennedy School of Government Executive Session on Domestic Preparedness. *Beyond the Beltway: Focusing on Hometown Security, Recommendations for State and Local Domestic Preparedness Planning a Year After 9-11*. Sept. 2002, pg. iii.

[19] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004, pg. 9.

[20] Code of Virginia, 2.2-3705: 17, 46, 50, 56, 57, 69; available on-line at <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-3705> and 36-105.3; available on-line at <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+36-105.3>

[21] US Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Cross Cutting Study.* Jan. 2003, pg. vii.

[22] Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, pg. 31.

[23] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004, pg. 9.

[24] Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, pg. 23.

[25] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 15.

[26] *Ibid.*, pg. 12.

[27] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004.

[28] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 5.

[29] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004, pg. 11.

[30] *Ibid.*, pg. 12.

[31] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, 20 pgs.

[32] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004, pg. 12.

[33] *Ibid.*, pg. 12.

[34] *Ibid.*, pg. 12.

[35] Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, pg. 28.

[36] National Cooperative Highway Research Program. *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents.* NCHRP Project No. 20-07, Task 151A. May 2002, pg. 19.

[37] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 5-6.

[38] United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004, pg. 11.

[39] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 12.

[40] *Ibid.*, pg. 11.

[41] *Ibid.*, pg. 7.

[42] National Cooperative Highway Research Program. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* NCHRP Project No. 20-07, Task 151B. May 2002.

[43] Adapted from National Cooperative Highway Research Program. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* NCHRP Project No. 20-07, Task 151B. May 2002, pg. 5.

[44] From National Cooperative Highway Research Program. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* NCHRP Project No. 20-07, Task 151B. May 2002, pg. 22.

[45] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 7.

[46] National Cooperative Highway Research Program. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.* NCHRP Project No. 20-07, Task 151B. May 2002, pg. 7.

[47] National Cooperative Highway Research Program. *National Needs Assessment for Ensuring Transportation Infrastructure Security.* NCHRP Project No. 20-59, Task 5. Oct. 2002, pgs. v-vi with more detail on pages 27-29.

[48] The Blue Ribbon Panel on Bridge and Tunnel Security. *Recommendations for Bridge and Tunnel Security*. For the American Association of State Highway and Transportation Officials' Security Task Force. Sept. 2003, 64 pgs.

[49] TransTech Management, Inc. "State DOTs' Transportation Security Training Needs: A Briefing Report for AASHTO's Transportation Security Task Force." Aug. 2002, pg. 4.

[50] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 11.

[51] *Ibid.*, 20 pgs.

[52] National Cooperative Highway Research Program. *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents.* NCHRP Project 20-07, Task 151A. May 2002, pg. 18.

[53] Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 8.

[54] See for more detail: TransTech Management, Inc. "State DOTs' Transportation Security Training Needs: A Briefing Report for AASHTO's Transportation Security Task Force." Aug. 2002, pgs. 9-12.

[55] Harvard University, John F. Kennedy School of Government Executive Session on Domestic Preparedness. *Beyond the Beltway: Focusing on Hometown Security, Recommendations for State and Local Domestic Preparedness Planning a Year After 9-11.* Sept. 2002, pg. 19.

[56] Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, pg. 27.

[57] National Cooperative Highway Research Program. *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents.* NCHRP Project No. 20-07, Task 151A. May 2002, pg. 18.

[58] Harvard University, John F. Kennedy School of Government Executive Session on Domestic Preparedness. *Beyond the Beltway: Focusing on Hometown Security, Recommendations for State and Local Domestic Preparedness Planning a Year After 9-11.* Sept. 2002, pg. 19.

[59] In one region, the local MPO has taken the lead role in working with various agencies to move forward issues, including emergency response, requiring regional coordination. This is especially helpful since the region includes 114 governments all of which have their own defined local mission. (Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version. Apr. 2003, pg. 12).

Appendix A: Interviewees

State Agencies

Illinois Department of Transportation
- Joe Hill
- Dave Johnson
- Tom Korty

Maryland Department of Transportation
- John Contestabile

Missouri Department of Transportation
- Don Hillis
- Mike Stephenson

New Jersey Department of Transportation
- Kurt Aufschneider
- Harold Neil

Texas Department of Transportation
- Mary Lou Rawls
- Tom Rummel

Virginia Department of Transportation
- Perry Cogburn
- Jim Keck
- Mike McAllister
- Steve Mundol
- Paul Szatkowski

Washington State Dept. of Transportation
- Tom Lentz
- Terry Simmonds

Federal Agencies

FHWA, Office of Operations
- John Gerner
- Vince Pearce

FHWA, Office of Bridge Technology
- Steve Ernst

Transportation Security Administration
- Ash Chatterjee
- Kate Parker
- Stephen Sprague
- James Taylor

Other Agencies

AASHTO
- Tony Kane

Bibliography

American Association of State Highway and Transportation Officials. "Maryland's Reaction and Response to the Events of September 11th – A Case Study." 2002, 6 pgs.

American Association of State Highway and Transportation Officials. *Re-organizing for Transportation Operations*. 1 Dec. 2003, 14 pgs.

American Association of State Highway and Transportation Officials. "Summary of Lessons Learned from Pentagon Attack." 2002, 5 pgs.

American Association of State Highway and Transportation Officials and Federal Highway Administration. *Compilation of Actions Taken by Surveyed Transportation Agencies at Each Level of the Homeland Security Advisory System*. 31 Oct. 2002, 19 pgs.

American Association of State Highway and Transportation Officials Task Force on Transportation Security. *Transportation Security Research: Highway and Bridge Priorities of State Transportation Agencies*. 29 Apr. 2002, 14 pgs.

Albright, D. Principles and Practices for State Transportation Agency Security in Strategic Indirect Warfare. New Mexico Department of Transportation. Sept. 2003, 31 pgs.

Boyd, A., and J.P. Sullivan. "Emergency Preparedness for Transit Terrorism." *TR News.* Volume 208. May-June 2000, 7 pgs.

Boyd, A., and J.P. Sullivan. *Emergency Preparedness for Transit Terrorism*. Transit Cooperative Research Program, Synthesis of Transit Practice 27. 1997, 83 pgs.

Cambridge Systematics. *Asset Management Guidance for Transportation Agencies.* National Cooperative Highway Research Program Project 20-24(11). Nov. 2002, 134 pgs.

Cohen, J.D., and J.A. Hurson. "The State and Local Role in Domestic Defense." *PPI*. Jan. 2002, 9 pgs.

D'Agostino, S. "Securing Emergency Operations." Transportation Management and Engineering. Vol. 9, Num. 1. Jan. 2004, 3 pgs.

Federal Emergency Management Agency. *Capability Assessment for Readiness (CAR).* 1997, 144 pgs.

Federal Emergency Management Agency. Guide for All-Hazard Emergency Operations Planning - Chapter 6, Attachment G (Terrorism). Apr. 2001, 62 pgs.

Federal Emergency Management Agency. State and Local Guide (SLG) 101: Guide for All-Hazard Emergency Operations Planning. Sept. 1996, 279 pgs.

Federal Highway Administration. "Lessons Learned in Emergency Transportation Operations Preparedness and Response." Pre-Publication Version, Apr. 2003, 20 pgs.

Federal Transit Administration. *Critical Incident Management Guidelines.* July 1998, 105 pgs.

Federal Transit Administration. "Federal Transit Administration Transit Threat Level Response Recommendation."

Federal Transit Administration. The Public Transportation System Security and Emergency Preparedness Planning Guide. DOT-FTA-MA-26-5019-03-01. Jan. 2003, 195 pgs.

Federal Transit Administration, Security Design Research Program. "Transit Agency Emergency Communication Needs." DRAFT. 11 Apr. 2003, 27 pgs.

Harvard University, John F. Kennedy School of Government Executive Session on Domestic Preparedness. Beyond the Beltway: Focusing on Hometown Security, Recommendations for State and Local Domestic Preparedness Planning a Year After 9-11. Sept. 2002, 57 pgs.

ITS Cooperative Deployment Network. "The FHWA's Role in Enhancing Surface Transportation Security: A Discussion with Vince Pearce, Public Safety and Security Team Leader, FHWA Office of Operations." *ICDN*. 22 Apr. 2003.

Institute of Transportation Engineers. "Transportation for Emergency Response and Recovery." 2004, 32 pgs.

Jenkins, B.M., and F. Edwards-Winslow. *Saving City Lifelines: Lessons Learned in the 9-11 Terrorist Attacks.* Mineta Transportation Institute. Sept. 2003, 74 pgs.

Jenkins, B.M., and L.N. Gersten. Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. Mineta Transportation Institute. Sept./Oct. 2001.

Mayer-Schönberger, V. "Emergency Communications: The Quest for Interoperability in the United States and Europe." Working Paper. May 2002, 48 pgs.

McCormick, Taylor and Associates. *Communication of Threats: A Guide.* TCRP Report 86, Public Transportation Security Volume 1. Aug. 2002, 50 pgs.

Mercier, C. L. "Terrorists, WMD, and the US Army Reserve." *Parameters*. Autumn 1997, pp. 98-118.

Meyer, M.D. "The Role of the Metropolitan Planning Organization (MPO) In Preparing for Security Incidents and Transportation System Response." DRAFT, University of South Florida. Jan. 2002, 7 pgs.

National Cooperative Highway Research Program. A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. Project 20-07/Task 151B. May 2002, 47 pgs.

National Cooperative Highway Research Program. *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents.* Project 20-07/Task 151A. May 2002, 85 pgs.

National Cooperative Highway Research Program. Emergency Transportation Operations Preparedness and Response Workshops for Statewide Applications: Workshop Follow-Up and Report. Project 20-59/Task 8. Jan. 2004, 47 pgs.

National Cooperative Highway Research Program. *Guide to Emergency Transportation Operations*. Project 20-59/Task 11, Volumes 1 and 2. Oct. 2003, 70 pgs.

National Cooperative Highway Research Program. *National Needs Assessment for Ensuring Transportation Infrastructure Security.* Project 20-59/Task 5. Oct. 2002, 57 pgs.

National Governors Association, Center for Best Practices. "Domestic Preparedness Checklist." 3 pgs.

National Governors Association, Center for Best Practices. “States’ Regional Terrorism Policy Forums.” Jan. 2001.

National Research Council. Improving Surface Transportation Security, A Research and Development Strategy. Washington D.C: National Academy Press, 1999.

O’Neil, D.J. “Statewide Critical Infrastructure Protection: New Mexico’s Model.” *TR News.* Vol. 211. Nov.-Dec. 2000, 4 pgs.

RAND Corporation. Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Dec. 2001, 270 pgs.

Seiple, C. “Consequence Management: Domestic Response to Weapons of Mass Destruction.” *Parameters*. Autumn 1997, pp. 119-34.

The Blue Ribbon Panel on Bridge and Tunnel Security. *Recommendations for Bridge and Tunnel Security*. For the American Association of State Highway and Transportation Officials’ Security Task Force. Sept. 2003, 64 pgs.

The White House. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Feb. 2003, 96 pgs.

TransTech Management, Inc. State DOTs’ Transportation Security Training Needs: A Briefing Report for AASHTO’s Transportation Security Task Force. Aug. 2002, 17 pgs.

United States Department of Homeland Security. *Initial National Response Plan.* 30 Sept. 2003, 14 pgs.

United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis.* DRAFT. Feb. 2004.

United States Department of Transportation, John A Volpe National Transportation Systems Center. *Effects of Catastrophic Events on Transportation System Management and Operations: Cross Cutting Study.* Jan. 2003, 63 pgs.

United States General Accounting Office, Report to the Committee on Appropriations, House of Representatives. *Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments.* May 2003, 27 pgs.