Homeland Security and State Departments of Transportation

Maintaining Strategic Direction for Protecting America’s Transportation System

Issued by:

American Association of State Highway and Transportation Officials
Special Committee on Transportation Security

January 2006
Acknowledgments

This study was requested by AASHTO and conducted as part of National Cooperative Highway Research Program (NCHRP) Project 20-59. The NCHRP is supported by annual voluntary contributions from the state Departments of Transportation. Project 20-59 is intended to fund quick response studies on behalf of the AASHTO Special Committee on Transportation Security. The report was prepared by Joe Crossett of TransTech Management, Inc. Project 20-59 is guided by a panel that includes David S. Ekern, David P. Albright, John M. Contestabile, Frank Day, Ernest R. "Ron" Frazier, Lee D. Han, Polly L. Hanson, Randell H. "Randy" Iwasaki, Gummada Murthy, Mary Lou Ralls, Ricky D. Smith, Jeff Western, and Mark Wikelius. Liaisons include Steven L. Ernst, Michael Taborn, Valerie Briggs, Robert D. Franz, Paul Golden, Greg Hull, Anthony R. Kane, Jack Legler, Vincent P. Pearce, Matthew D. Rabkin, Kerry Thomas, and Joedy Cambridge. The project was managed by S. A. Parker, CRP Senior Program Officer.

Disclaimer

The opinions and conclusions expressed or implied are those of the research agency that performed the research and are not necessarily those of the Transportation Research Board or its sponsors. This report has not been reviewed or accepted by the Transportation Research Board's Executive Committee or the Governing Board of the National Research Council.
Table of Contents

State DOTs - Guardians of Transportation Infrastructure and Mobility......................... 1
  1.1. Understanding the Threat to Transportation ........................................................... 2
  1.2. Highlights of DOTs’ AASHTO-Led Activities ...................................................... 3
  1.3. State DOTs’ Partners .......................................................................................... 4
  1.4. White Paper Structure ....................................................................................... 4

Protection of Critical Transportation Assets................................................................. 5
  2.1. Risk Assessment ............................................................................................... 5
  2.2. Counter Measure Development and Deployment ............................................... 6

Emergency Management Support to First Responders .................................................... 8
  3.1. Mobilizing Emergency Transportation Operations ............................................. 8
  3.2. Recovery of Transportation Infrastructure .......................................................... 10

Critical Gaps and Needs.................................................................................................. 11
  4.1. Interagency Coordination .................................................................................. 11
  4.2. Funding Needs .................................................................................................. 11
  4.3. DOT Organizational Structures ......................................................................... 11
  4.4. Technology ....................................................................................................... 12
  4.5. Communications ............................................................................................. 12
  4.6. Training, Drills, and Exercises .......................................................................... 12
  4.7. Information Sharing .......................................................................................... 13
Section 1.0

State DOTs - Guardians of Transportation Infrastructure and Mobility

Deadly and unprecedented terror attacks on infrastructure in the United States and Western Europe, including bombings on London’s subway system and Madrid’s commuter rail network, as well as the World Trade Center/Pentagon attacks, have forced state department of transportation (DOT) leaders to reassess their agencies’ security needs. Among DOTs, the top priorities that have emerged include better protection of critical transportation infrastructure and ensuring adequacy of emergency management capabilities.

Four years on from the attacks of 9/11 that provoked this new level of scrutiny, and after considerable investment of time and money by DOTs and their partners, this White Paper offers a mid-course review of how DOTs are continuing to refine and enhance approaches to homeland security and the needs they have in two critical areas:

- **Critical Transportation Infrastructure Protection.** Unlike natural or accidental emergency situations, terrorist attacks are deliberate acts that may be prevented or deterred.

  DOTs are now challenged to ensure that the infrastructure they own and operate is adequately protected against terrorism; a responsibility that requires new skills such as risk management as well as partnerships with the law enforcement and intelligence communities and additional resources. In every state, a handful of transportation infrastructure assets are sufficiently vulnerable to attack and/or critical to society and to the economy that they merit extraordinary measures of protection.

- **All Hazards Emergency Management Support.** DOTs have always been primed to support public safety and first responder agencies when potentially deadly devastation is inflicted by natural or accidental emergencies, such as hurricanes, floods, truck crashes, fires or chemical spills.

  Transportation agencies now find that refinement of the same support roles, such as their Intelligent Transportation System capabilities for incident management can help prepare for, respond to, and recover from terrorist attacks on the nation’s transportation systems, or other targets. “All hazards” emergency management has become a by-word at many DOTs for guiding their homeland security efforts – but keeping abreast of fast-moving developments in emergency management practices often proves challenging.

The ways DOTs now address transportation security are different from four years ago. Emergency management and critical infrastructure protection are no longer unfamiliar terms, and advanced preparedness planning, sophisticated emergency transportation operations, improved coordination with public safety and law enforcement agencies, and counter measures that protect critical infrastructure are on every DOT’s agenda.

The purpose of this White Paper is to provide a big picture perspective on the multiple directions in which transportation-related security policy is heading at the state DOT level. This analysis will help DOT policy makers identify next steps for

---

1 The need for a White Paper was first discussed by AASHTO’s Special Committee on Transportation Security at its January 2005 meeting. A request for the paper was made during the June 2005 SCOTS meeting.
ensuring DOTs are fully prepared to prevent future attacks and respond to emergencies, and how to obtain resources to support these needs.

1.1. Understanding the Threat to Transportation

Transportation is a vital part of the nation’s social and economic fabric. It ensures workers get to their jobs, goods and services reach their destinations, and people stay connected. Blanket protection by state DOTs of all transportation assets, however, is neither feasible nor warranted.

Collectively, state DOTs have primary responsibility for building and operating most of the busiest highways, bridges, and tunnels in the United States, which together constitute more than 1.8 million lane-miles of highways. DOTs are also multimodal agencies whose responsibilities often include passenger and freight rail, public transit, water ports, ferries and aviation.

Every day, vehicles travel about five billion miles on state DOT-owned roads. About 90 percent of all freight by value is shipped around the United States by truck, and businesses rely on a “just-in-time” economy in which a single unexpected incident can have significant effects. The weeklong shutdown of all sea- and airports following September 11, for example, is estimated to have resulted in economic losses as great as the $50 billion World Trade Center costs.

The apparent scale and redundancy of the nation’s transportation system gives a false sense of security, but in many parts of the country that system is straining to keep up with the transportation demands of communities and the economy. A Blue Ribbon Panel convened by American Association of State Highway and Transportation Officials (AASHTO) and the Federal Highway Administration (FHWA) in 2003 suggests there are about 1,000 bridges across the country where substantial casualties and economic disruption would result from isolated attacks.

The costs of failure to prepare for a terrorist attack that affects the nation’s transportation infrastructure or relies on that infrastructure for emergency response, in terms of loss of life and economic disruption, could be catastrophic. The FHWA/AASHTO Blue Ribbon Panel concluded that economic and replacement costs for loss of a single critical bridge or tunnel could exceed $10 billion.

The threat of terrorism poses new challenges for state DOTs. In 2003, eighty percent of DOTs surveyed said they had incurred additional costs to improve transportation.

State DOTs and Terror – An Example: On September 11, 2001, the emergency management capabilities of several state DOTs in the New York and Washington, DC regions were tested in previously unimaginable ways. Highways, bridges, and tunnels; transit systems; and pedestrian facilities in these areas were turned into evacuation routes and a way for emergency response teams to reach incident scenes. Virginia DOT’s high-tech Traffic Management Center in Arlington, VA was even transformed into the incident command headquarters for emergency responders after American Airlines flight 77 hit the Pentagon.

State DOTs were able to act swiftly on September 11 because they were already equipped to meet the challenges of responding to and recovering from the devastation caused by natural and man-made disasters. When incidents such as hurricanes, wildfires, earthquakes, or major traffic crashes threaten safety and mobility, DOT personnel and equipment are part of response and recovery activities.

Their sophisticated traffic management systems help keep traffic moving, their information systems help keep communications flowing, and their construction expertise helps speed recovery.


4 FHWA, Recommendations for Bridge and Tunnel Security, 2003
security. According to a national needs assessment for ensuring transportation infrastructure security that was published in 2002, overall security costs for DOTs are expected to reach at least $10.5 billion during the six-year TEA-21 reauthorization period. More training, equipment, infrastructure hardening, and research for DOTs is vital, yet only 1 percent of the Department of Homeland Security’s fiscal year 2004 $247 million research and development budget is dedicated to supporting highway-related initiatives. Eventually, no security counter measures funding went to highways.

1.2. Highlights of DOTs’ AASHTO-Led Activities

AASHTO’s 21-member Special Committee on Transportation Security (SCOTS) in its Task Force form was established immediately after 9/11/01 and reports directly to AASHTO’s President. SCOTS’ vision is to be “the voice and resource for state DOTs to improve transportation security across all modes.”

Working together under the auspices of AASHTO’s Special Committee on Transportation Security, state DOTs and their partners have undertaken a wide variety of activities over the last four years. SCOTS has sponsored National Cooperative Highway Research Program (NCHRP) research of over $6 million on development of guides, research, training and workshops for AASHTO members. It is also a unifying force among DOTs and their partners at FHWA for raising the profile of homeland security issues in transportation and for forging partnerships with other groups engaged in security activities. Highlights of completed NCHRP/SCOTS/FHWA-sponsored activities include:

- Two surveys of state DOTs’ approaches to transportation security (2001 and 2003);
- Transportation and Security Research Priority Setting Workshops (April 2002 and February 2003);
- Survey of State DOTs’ Security Training Needs (August 2002);
- AASHTO Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (2002);
- AASHTO Guide to Updating Highway Emergency Response Plans for Terrorist Incidents (2002);
- National Needs Assessment for Ensuring Transportation Infrastructure Security (2002);
- FHWA Emergency Preparedness Workshops – 30 two-day workshops around the country consisting of a case study analysis and a terrorism exercise (2002-2005);
- AASHTO/FHWA Emergency Response Workshops (2003);
- FHWA Bridge and Tunnel Vulnerability Assessment Workshops (2003);
- AASHTO/FHWA Recommendations for Bridge and Tunnel Security - Blue Ribbon Panel on Bridge and Tunnel Security (September 2003);
- FHWA/Volpe Institute Disaster Case Studies Series (New York/Washington DC, Baltimore Train Fire, East Coast Blackout, Northridge Earthquake) (2004);
- AASHTO brochure on Protecting America’s Roads, Tunnels, and Bridges – The Role of State DOTs in Homeland Security (2005);

---

6 Ham, D. and Lockwood, S., National Needs Assessment for Ensuring Transportation Infrastructure Security. 2002
• NCHRP Guidance for Transportation Agencies on Handling Sensitive Information (2005)
• NCHRP/National Transit Institute’s training course and CD-ROM System Security Awareness for Transportation Employees (2005); and
• A very significant effort currently underway is the development of a multimodal transportation infrastructure risk management guide (NCHRP final report due Aug 2006).

This list is just a sampling of the activities in which AASHTO and SCOTS have been closely involved. DOTs also are closely involved with numerous other efforts, both within their own states and in partnership with Federal agencies.

1.3. State DOTs’ Partners

Partnership has emerged as a common theme among all state DOTs’ homeland security initiatives. Partnership is at the heart of effective emergency management activities and it is also a vital part of critical infrastructure protection.

The partnerships DOTs are entering into address issues like transfer of best practices, joint training, information sharing, interoperable voice and data communications, combined research, and multi-agency funding approaches.

State DOTs’ partners in homeland security include the US Department of Transportation, the US Department of Homeland Security (including the US Coast Guard, the Federal Emergency Management Agency, and the Transportation Security Administration), Federal intelligence agencies, the US Department of Defense, Federal law enforcement agencies, public transit agencies, railroad operators, airport operators, trucking associations, port authorities, bridge and tunnel operators, state emergency management agencies, local and state public health and safety authorities, and local and state law enforcement and first responders.

1.4. White Paper Structure

The remainder of the White Paper describes the state of the practice for state DOTs’ critical infrastructure protection activities (Section 2) and emergency management practices (Section 3). This is followed by identification of a set of critical gaps and needs (Section 4).
Section Two

Protection of Critical Transportation Assets

Terrorist attacks differ from natural and accidental disasters because they are intentionally perpetrated acts that could possibly be prevented or deterred. The heightened threat of terrorism has required DOTs to pay much closer attention to the risk of malevolent attacks against assets they build, maintain, and operate, and/or the users of those assets.

Experts fear attacks that destroy or damage transportation infrastructure. The principal threat against transportation infrastructure assets is explosive attacks on key links such as bridges, interchanges, and tunnels. Safe, continuous movement of people and goods could also be jeopardized by use of incendiary devices, handheld cutting devices that sever bridge components, release of chemical or biological agents in tunnels.

Blanket protection by state DOTs of all transportation assets is neither feasible nor warranted. Most of the nation’s transportation system is characterized by features, such as physical robustness, ease of replacement, system redundancy, and limited potential for mass casualties that make it a relatively unappealing terrorist target.

Some individual transportation facilities are critical to protect and may be attractive targets for terrorists. These include facilities where users are concentrated in small areas; or that span large natural barriers such as rivers, bays or mountains; or that serve unique regional or national transportation and economic functions; or that have a symbolic role.

The cost of counter measures for even a handful of transportation infrastructure assets is high. AASHTO’s 2002 National Needs Assessment for Ensuring Transportation Infrastructure Security estimates state DOTs’ capital and operating budget needs for protecting critical assets at $2.5 billion between 2002 and 2008. This estimate will be refined and updated during 2006.

Protection of critical transportation assets includes 1) identification of critical assets, and assessment of their vulnerability to attack/potential consequences of attack; and 2) development and deployment of suitable counter measures. Each of these components is discussed in this section.

2.1. Risk Assessment

As owner-operators of transportation assets, state DOTs must determine the need for counter measures, if any, via a comprehensive risk management assessment of asset criticality, vulnerability, and potential consequences that helps identify assets which, if attacked, have the greatest risks for undesirable outcomes.

Transportation agencies are becoming adept at the process of assessing the vulnerability and criticality of their transportation assets. This assessment is based on an integrated analysis of the data collected on critical/key assets/activities, realistic and credible threats, and known or specifically identified vulnerabilities. It often requires coordination with the law enforcement and intelligence community. AASHTO’s 2002 Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection provides a helpful resource on this topic. In 2006 an updated AASHTO guide on risk management will be completed.

Vulnerability assessment methods range in complexity from highly subjective approaches that rely primarily on the good judgment of knowledgeable and experienced individuals to detailed scientific approaches involving structural analyses and testing. Historically, risk assessments related to
highways have focused on natural and unintentional technological disasters where reasonable estimates of destructive forces can be quantified and engineering designs can be developed consistent with perceived risks to critical infrastructure, people and property.

Terrorism presents an “asymmetric” threat – one in which terrorists either employ surprise and relatively low-cost weaponry to inflict catastrophic damage on large populations and property, or threaten actions that cause fear and panic. Vulnerability to these threats is much more difficult to assess and is often based on assumptions about the capability and intent of terrorist organizations. The best counter measures for these threats may involve access control, surveillance, monitoring, standoff barriers, and other procedural or technical approaches rather than improving structural integrity of the asset through costly engineering design and construction.

All DOTs have access to, and according to the most recent (2003) survey data from AASHTO, a large majority (84 percent) are using AASHTO-sponsored guidance on vulnerability/criticality assessment and risk management to determine the extent and nature of threats to their state’s transportation system. Based on the results of these analyses, they are developing counter measure techniques to detect and prevent attacks on critical infrastructure and minimize damage in the event they occur.

2.2. Counter Measure Development and Deployment

DOTs develop and deploy counter measures as a result of needs identified in risk management assessments. In many instances, counter measures are developed and deployed in coordination with other partners, including law enforcement and public safety agencies. Counter measures are intended to deny, deter, detect or defend against attacks. Deterrent and detection measures work by creating a greater likelihood that potential aggressors will be caught and may even be deterred from attacking an asset. The effectiveness of deterrence varies with the aggressor’s sophistication, the asset’s attractiveness, and the aggressor’s objective.

Defensive measures work by protecting an asset from aggression by delaying or preventing an aggressor’s movement toward the asset or by shielding the asset from weapons and explosives. Both deterrent and defensive counter measures commonly take the form of site-work, building/structure, and detection elements:

- **Site-work elements** include the area surrounding a facility or an asset. They can include perimeter barriers, landforms, and standoff distances that delay aggressors from gaining access by using tools in a forced entry, prevent an aggressor’s movement toward an asset, and/or protect the asset from the effects of tools, weapons, and explosives. For transportation assets they may include elimination of parking areas beneath bridges, restrictions on ingress and egress routes from adjacent areas, or additional lighting.

- **Building and structure elements** are measures directly associated with design of facilities and structures. They may include installation of locks, caging, and various types of fencing locations where placement of explosives would affect points of structural integrity and vulnerability, as well as protection of the structural integrity of key members against collapse by strengthening key substructure members and blast shielding.

- **Detection elements** sense an act of aggression, assess the validity of the detection, and communicate the appropriate information to a response force. A detection system must provide
all three of these capabilities to be effective. Detection elements include closed-circuit television, regular vehicle checks, motion detectors, alarms, and weapon and explosive detectors, including chemical and biological weapon detection technologies. This element can also include guards used to support this equipment or to perform similar functions.

Any of these counter measures may be added during asset retrofits or during new construction/reconstruction. Many key counter measure issues relating to highway structures are in the early stages of research. Current military and engineering judgment indicates that complete protection of key structural elements is neither feasible nor cost-effective. The overall practical objective of various security measures is, therefore, not to provide full protection, but to discourage terrorist attack through visible security and reduced vulnerability, as well as to minimize damage to critical facilities in the event of an attack.

**Conclusions**

State DOTs are making headway in critical infrastructure protection. Sophistication of risk management practices is growing and should be encouraged. Sharing of information with law enforcement and intelligence agencies remains a concern. Further research is needed on the effectiveness and applicability of different counter measures. In addition, DOTs must make greater efforts to integrate asset protection with broader transportation planning efforts, such as identification of long-term transportation capacity needs. Adequacy of resources to meet implementation needs remains a concern. Section Four discusses specific needs in detail.
Section Three

Emergency Management Support to First Responders

The primary functions of emergency management include protection and preservation of life, property, evidence, and the environment wherever possible during any emergency event. State DOTs generally do not lead emergency management efforts, but they can, and often do play a vital support role to first responder, public safety, and law enforcement partners, before (emergency preparedness), during (emergency response), and after (recovery) emergencies. Of course, in the event that an emergency directly affects transportation infrastructure owned by a DOT, their role may include greater leadership, particularly in recovery efforts.

DOTs are often perceived by others as public works agencies with limited support capabilities. Public safety and emergency management agencies, meanwhile, may not understand how to assess an emergency situation in terms of its likely impacts on the transportation system. Likewise, some technical resources – such as advanced surveillance systems possessed by state DOTs – are not well known to the public safety community. Training, drills, and exercises can help improve coordination and understanding among emergency management agencies and DOTs.

Emergency management is not a new responsibility for DOTs. Because states’ transportation networks are vulnerable to disruption caused by a variety of events including traffic incidents, weather, construction, and natural disasters, DOTs have ramped-up their “all hazards” emergency management capabilities to ensure coordinated and speedy emergency response and recovery regardless of the type of emergency.

State DOTs’ distributed personnel, incident response training, and statewide communications networks are particularly valuable for both security-related and other emergency response efforts. A 2002 study, however, estimates state DOTs’ capital and operating budget needs for enhanced emergency management will total $8 billion between 2002 and 2008. This estimate will be refined and updated during 2006.

The attacks of Sept 11, 2001 were a catalyst for intensive and nationwide efforts led by the Department of Homeland Security to revisit, revise, and reinvigorate multi-agency emergency management efforts. In this ongoing process, emergency management practices, procedures, and protocols that accommodate the threat of terrorist attacks as well as natural disasters are constantly evolving. For many state DOTs, just keeping pace with these changes can be challenging,

Transportation agencies’ primary emergency management support skills and resources fit within two broad categories: 1) mobilization of emergency transportation operations to respond to events both on and off the transportation system, and 2) recovery of transportation infrastructure. Each of these components is discussed in this section.

3.1. Mobilizing Emergency Transportation Operations

Emergency transportation operations (ETO) facilitate first responders’ activities. Mobilization of emergency transportation operations by DOTs and their partners involves assembling and organizing resources, including people, equipment, facilities, communications systems, expert technical support, and public information systems and protocols. It is a process that requires that the right people will deploy appropriate resources at the correct time.

Effective ETO mobilization requires a partnership of local, regional, state, and
federal agencies. Joint preparedness training is important, while during response and recovery voice and data communications must be interoperable, and information must be shared.

Emergency transportation operations approaches vary widely among regions. In most states, however, DOTs usually have some or all of the following responsibilities:

- Assistance in determining viable routes to, from, and within disaster areas and regulation of use of those networks for movement of people, equipment, and supplies;
- Coordination with Emergency Operations Centers to implement detours and diversion routes for potentially affected areas of the transportation system;
- Assessment of transportation infrastructure condition and closure of unsafe components;
- Assistance with evacuation of persons from immediate peril;
- Transportation of equipment, personnel, and supplies for supporting emergency activities, and provision of any highway clearances and waivers needed to speed up such movements;
- Provision of transportation-related resources such as vehicle repair facilities, fleet parking, and storage areas to be used for servicing, refueling, parking, and storage of emergency vehicles;
- Helping keep freight moving through or around an area and helping EMS vehicles move where needed;
- Provision of general traffic management assistance including posting of temporary signing, portable variable message signs, temporary traffic controls, one-way systems, barricades, detour routings, and vehicular traffic flow data and information from permanent and temporary monitoring sites;
- Dispatch of operations personnel to incident scenes (Service Patrols/Incident Response Teams) to: secure the incident scene; provide emergency medical aid; support fire, rescue and emergency medical services in their operations; relocate or remove vehicles and debris from the roadway; assist stranded motorists and others on the roadway; provide for emergency traffic control; and initiate longer-term traffic control for approaching traffic and affected areas;
- Coordinated operation of the transportation system to address incident impacts. (This could include lowering of freeway speed limits through use of dynamic message signs or variable speed limit signs, modification of ramp metering rates or signal timing to slow the flow of traffic, and use of flashing beacons and Highway Advisory Radio to issue public warnings and advisories.);
- Coordination with other transportation agencies via state-wide/multi-state incident monitoring systems to provide direct updates to traveler information Internet sites. Many TMCs are also now connected to regional, state and even multi-state systems which identify incidents, delays, road closures, emerging conditions, and accidents;
- Use of traffic management centers operated by DOTs in many larger cities that offer electronic technology such as traffic cameras, ramp monitoring, and roadway sensors, to monitor and manage traffic;
- Design and implementation of alternate transportation services to temporarily replace transport capacity lost to disaster damage; and
- Provision of information for the public about issues such as road closures, infrastructure damage, debris removal,
and restoration activities via contacts with radio, television and other commercial media and use of technologies such as highway advisory radio, 511 travel information, variable message signs, and Internet web pages.

3.2. Recovery of Transportation Infrastructure

As the story begins to leave the headlines, disaster recovery efforts are usually just starting for major incidents where infrastructure damage is severe. If transportation facilities are targeted or they experience ancillary damage, a stiff economic toll may be exerted if they are closed to traffic, particularly when alternate routes are not readily available. In such instances, pressure to rebuild quickly is often intense.

As emergency management activities switch from response to recovery, state DOTs continue to play either a key supporting role or a leading role if transportation facilities have been damaged. Recovery of transportation infrastructure helps communities reestablish economic and social vitality. State DOTs oversee hundreds of infrastructure construction projects every year. Their access to heavy equipment and contracting capabilities make them uniquely qualified to lead or support infrastructure reconstruction efforts. In most states, DOTs usually have some or all of the following responsibilities:

- Restoration of critical transportation routes and facilities;
- Issuance of permits required to repair/restore utility lines or pipes that are immediately adjacent to, or run over or under state highways; and
- Provision of needed equipment and/or technical assistance in support of the restoration of critical public works.

Conclusions

Emergency management is a topic that requires integration among many diverse players. State DOTs are aware of this, however, significant room for improvement remains to integrate processes, training, communications, and technology. Further research in these areas would be beneficial to advance the field of knowledge. In addition, guidelines and tools are needed to aid in the design, development, and implementation of a range of training drills and exercises to improve DOTs’ emergency management capabilities. While funding is important, strengthening of partnerships is also critical. Section Four discusses specific needs in detail.
Section Four

Critical Gaps and Needs

Despite the progress that DOTs have made in homeland security over the last four years, many important issues must still be addressed. In this section, a series of critical gaps and needs in state DOTs’ homeland security efforts are identified.

4.1. Interagency Coordination

Despite the growing focus on coordinated emergency management and infrastructure protection, DOTs frequently still have arms-length relationships with law enforcement, intelligence agencies, and public safety agencies that have first responder responsibilities. Alternatively, DOTs primarily depend on informal person-to-person relationships established at the field level.

In many states, opportunities to consider common issues, and to share responsibilities, training, resources, and information are sometimes missed and DOTs frequently lack meaningful involvement in the management of emergencies.

Continued effort is needed to improve understanding of state DOTs’ responsibilities, particularly in the area of emergency management, and to ensure they are well integrated with those of first responders, law enforcement, and public safety agencies. Likewise continued efforts are needed to strengthen communications, information sharing and training among agencies.

4.2. Funding Needs

Security-related activities are placing new financial burdens on State DOTs, who are struggling to meet emergency management and infrastructure protection priorities.

Traditional transportation funding sources are simply insufficient to meet basic system preservation, operations, and expansion needs, much less address new security-related costs. Only a small subset of security-related funding sources are designed to address the specific security needs faced by state DOTs. Other funding programs are designed with an emphasis that overlaps state DOT interests, but are sources for which state DOTs may only be eligible to receive funds as a collaborator with another agency. Sorting through and identifying the appropriate funding sources and fulfilling the application process can be a daunting task.

Recent DHS strategy has been to focus distribution of all funding resources on a single comprehensive approach to domestic incident management, known as the National Response Plan (NRP). Recognizing that each state has a key role in the NRP, DHS has increasingly been allocating funds to each state based upon a formula that considers population, threat, and other factors. To increase their chances of receiving funds, state and local responders must align grant requests with federal priorities and those of their state emergency management plans.

4.3. DOT Organizational Structures

Many DOTs consider security activities an ancillary responsibility for units with other primary responsibilities, such as intelligent transportation systems (ITS), traffic operations, or maintenance. For example, at many DOTs, emergency transportation operations (ETO) are conducted as a fragmented, part-time reactive activity at the district level with responsibilities divided among maintenance, traffic operations units, traffic management center (TMC) management, and ITS project staff. This generally compromises the quality of leadership and reporting accountability for
emergency management within DOTs. As a result, DOT contributions may not be consistently and fully integrated into statewide emergency management plans. To fulfill their mobility mission, many DOTs will have to upgrade the position of homeland security beyond their often fragmented, part-time and reactive character.

4.4. Technology

Application of technology within DOTs for security purposes is limited and based principally on safety service patrols, regional public safety call and computer-aided dispatch (CAD) centers and the modest coverage of ITS surveillance, detection, and communications systems. Only 25 percent of the freeway network in the 78 largest metro areas is covered by systems that allow monitoring of traffic conditions and communication with users in the event of an incident or emergency. Nationwide expansion and enhancement of ITS systems is required to support homeland security needs. Personal protective equipment is not systematically available for transportation employees who work on or around critical facilities.

4.5. Communications

Communications interoperability refers to the capability for agencies to talk with one another by radio on demand and in real time. Many states are now developing state-of-the-art radio communications networks for first responders, including law enforcement and fire personnel, emergency medical services (EMS) workers, and other public health professionals.

In 2004, ninety four percent of DOTs surveyed cited communication interoperability as a major concern. DOT personnel lack appropriate communications interoperability with other emergency responders. Today’s emergency communications are lacking in terms of interoperable flexibility. The inefficiency in communications is a major source of delay in rapid response and quick resolution of incidents and emergencies. The need for interoperable interagency communications is widely acknowledged, but represents an expensive challenge in many regions.

4.6. Training, Drills, and Exercises

According to an AASHTO survey completed in 2002, a large majority of DOTs surveyed (about 80 percent) had not made major changes to their in-house training activities since September 11th to include broader security-related concerns. About 70 percent of state DOTs surveyed indicated they were reassessing, or had already reassessed their training needs. Shortages in funding, staff, or expertise; however, have hindered the ability of most states’ DOTs to expand improve security training capabilities.

Comprehensive security training should include both emergency management preparedness activities to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies, and training in infrastructure protection. DOTs particularly need to develop training activities that are multimodal and scalable and that include transportation employees, other responders, and other affected entities. Training should be delivered via classroom settings, video/web, and simulated exercises and administered not just to maintenance workers but also executive management. Specific topics identified by DOTs include:

- **Risk Assessment & Counter Measure Evaluation** - Methodologies for identifying and protecting critical infrastructure, equipment, and systems, including evaluation of the consequences of facility loss, techniques for data collection, and retrieval of relevant records;
• **Critical Infrastructure Protection** – Guidance on reporting suspicious activities, surveillance of key facilities, protecting computer networks/data, DOT buildings and human resources, legal issues;

• **Emergency Preparedness, Response and Recovery Planning** – Approaches for improved traffic management and operations, inter-agency coordination, hardening targets, quick-turnaround repairs, recovery and restoration of normal operations.

• **Media and Public Information** – Directions on activities such as controlling information flow, protecting secure information, and alerting the public, etc.

Integrated training activities, such as tabletop exercises with other agencies to test emergency response and recovery capabilities are important.

### 4.7. Information Sharing

Information-sharing protocols for each significantly different emergency type (weather, security, planned event) are not uniformly developed and often involve different units within responder and supporting agencies. For example, traffic management center/computer-aided dispatch (TMC/CAD) integration benefits may be obvious but only a few regions are yet moving in this area. Traffic management center protocols for both rapid and appropriate response and effectively informing the public have been developed in only a few regions. An integrated approach to a broader range of hazards also introduces other technology issues. These involve the need for cooperation among the emergency management community and public safety and transportation entities, more shared real-time information, rapid access across public data sources and data types, and a need to develop access to special expertise on an on-call basis.

### Conclusions

DOTs have made a great deal of progress on improving transportation-related security in the last four years. Despite their efforts, critical gaps remain and must be addressed. This White Paper sets the stage for DOTs to continue to develop a coordinated response to homeland security.