Transportation Security and Emergency Response
Professional Capacity Building Initiative

Strategic Plan

Final Draft Report

Prepared for

Federal Highway Administration
United States Department of Transportation

and

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

by

Volpe National Transportation Systems Research Center
Research and Innovative Technology Administration
United States Department of Transportation

January 7, 2006
Transportation Security and Emergency Response
Professional Capacity Building Initiative
Strategic Plan

Table of Contents

I. Executive Summary ........................................................................................................1

II. Understanding Security And Emergency Response Demands on States ....2
    A. Typical duties of a state DOT .................................................................................. 2
    B. Agencies with overlapping responsibilities ......................................................... 3
    C. Security agencies .................................................................................................... 4

III. Findings on State Needs re Security and Emergency Response ...............4
    A. AASHTO SCOTS 2001 Survey .............................................................................. 4
    B. AASHTO SCOTS Training Subcommittee 2002 Survey ........................................... 5
    C. TRB/AASHTO 2003 survey ................................................................................... 5
    D. Volpe Center needs assessment and resources analysis, 2004 ............................... 6

IV. Overview Of An Integrated Professional Capacity Building Initiative....10
    A. The concept of professional capacity building ..................................................... 10
    B. PCB toolkit ............................................................................................................ 10

V. Strategic Plan For A Security/Emergency Response PCB Initiative .......14
    A. Goal of this initiative ............................................................................................ 14
    B. Objectives ............................................................................................................. 14
    C. Implementation principles .................................................................................... 15
    D. Priorities and learning objectives for the PCB initiative ...................................... 16
    E. Multi-year plan ...................................................................................................... 23
    F. Year one actions .................................................................................................... 25
I. Executive Summary

This document presents a strategic plan for professional capacity building (PCB) that will help state departments of transportation (DOTs) meet their obligations for transportation security and emergency response. The plan was developed by the U.S. Department of Transportation’s Volpe National Transportation Systems Center, working closely with the American Association of State Highway Transportation Officials (AASHTO) and the Transportation Research Board (TRB), and supported by the Federal Highway Administration.

Section II discusses the challenges that state DOTs now face. While demands associated with transportation security are relatively new, they overlap considerably those associated with natural disasters. State DOTs want to take advantage of this overlap where possible, such that they can make maximum effective use of existing processes and resources. Thus, this plan treats security and emergency response as related needs, with opportunities for integrated solutions.

Section III summarizes relevant research on state needs. State DOTs want training and other resources on a variety of topics, including inter-agency coordination, evacuation planning, operational methods to secure facilities, vulnerability assessment, and incorporating security into plans and studies. Research also indicates that few resources now exist to address these needs.

Section IV provides an overview of professional capacity building. The concept of PCB is to supply tailored, targeted and timely help by offering an integrated set of resources—including, but not limited to, training. Section IV includes a “PCB toolkit” that summarizes commonly used resources, their advantages and disadvantages, and approximate implementation costs.

Section V presents a multi-year plan to achieve the following goal: **provide state DOTs with a trusted, reliable, and reasonably comprehensive source of information and assistance for their security and emergency response needs.** The plan outlines learning needs for each of 17 topics, spanning five areas. It offers recommendations for addressing those needs over a three-year period. Finally, it provides a detailed set of actions for year one, summarized as follows:

- **Establish a steering committee and technical working groups comprised of partners and stakeholders.** (page 25)
- **Support a series of regional workshops on emergency response coordination.** (page 25)
- **Support development and delivery of a seminar designed for executive-level staff, with a goal of elevating transportation's role in security/emergency response.** (page 26)
- **Conduct seminars on implementing a security/emergency response program.** (page 27)
- **Conduct peer exchanges on addressing security in transportation operations.** (page 27)
- **Support a technical advisory team to provide assistance in identifying critical assets and assessing their vulnerability, and pilot this approach with one state DOT.** (page 28)
- **Research and publish information on design methods for facilities security.** (page 28)
- **Deploy a searchable database of training and other PCB resources.** (page 29)

Clearly, the Federal Highway Administration has a leading role to play. However, the success of this initiative will depend on support and participation from all critical stakeholder interests.
II. Understanding Security And Emergency Response Demands on States

A. Typical duties of a state DOT

To understand the challenges that security and emergency response present for state departments of transportation, it is useful to review their purpose and structure. While there is no “typical” state DOT, there are many functions that are common to all. Generally, a state DOT’s mission is to provide transportation systems and services that are safe, efficient, cost effective, economically vital, accessible, and inter-modal, to ensure the mobility of people and goods, and enhance and/or preserve economic prosperity and the quality of life. The state DOT can be responsible for planning, designing, constructing, operating, and maintaining state facilities in all modes of transportation, including travel by air, water, and land. A state DOT often has primary responsibility for:

- Planning and design of transportation infrastructure,
- Contract administration,
- Materials design and testing,
- Environmental planning and compliance,
- Property acquisition,
- Fiscal programming and cost accounting,
- Enforcement of vehicle weight and dimension laws,
- Highway, bridge and rest area maintenance,
- Public transportation and rail programs and planning,
- General aviation airport planning,
- Highway traffic safety, and
- State Police/Patrol.

One area of responsibility, transportation system security, presents relatively new challenges for state DOTs. Security as it relates to a state DOT has many facets. A DOT needs to consider the following: its assets can be a target of attack, they can be the means of an attack, and they can be instrumental in providing a means for response to an attack and recovery from an attack. Because of these factors, the state DOT needs to plan for all phases of security including deterring, detecting, responding to, and recovering from an attack. During response and recovery operations, there are only minimal differences between responding to an attack and responding to other events that affect the transportation system. Because of the minimal differences in response and recovery operations between an attack and other disruptive events, an “all hazards” approach to planning is both reasonable and effective. Such an approach allows security and emergency management to be combined where appropriate.

Developing plans to deter, detect, respond to, and recover from disruptive events is something that requires the participation of all of a DOT’s staff. However, the responsibilities of each employee differ with his function in the organization and position within that function. The requisite knowledge, skills and abilities will vary as well. Therefore, any program designed to provide knowledge, skills and abilities for employees of a state DOT in the areas of security and
emergency management must take into account the different requirements of the target audiences. The basic areas and subsidiary job functions are as follows:

**Executive**
While each state is different, typical positions include a Secretary of Transportation, an Executive Director, Transportation Commissioners, and Advisory Committee members.

**Planning**
In planning, typical positions include a chief planner or manager, transportation planners, modelers, and engineers.

**Programming and Contracting**
In programming and contracting, typical positions include a capital planning or budget manager, budget analysts, acquisitions, procurement, or contracting officers, and legal staff.

**Engineering and Construction**
In the engineering and construction area, typical positions include chief engineer, civil and structural engineers, district and field engineers and inspectors.

**Operations and Maintenance**
In the areas of operations and maintenance, typical positions include district and field engineers, inspectors, maintenance managers, and maintenance crews.

There are agencies beyond a state DOT that are involved in an “all hazards” approach to security and emergency response. Depending on the nature of an event, federal, state, and local agencies each have a role to play. A state DOT interfaces with other agencies in two ways regarding security and emergency response. First, there are the agencies that the state DOT has interrelated responsibilities with during the planning, response and recovery phases of an event. Second, the state DOT must coordinate with agencies that provide input and information primarily for threats to security.

**B. Agencies with overlapping responsibilities**

The state DOT interfaces with agencies falling into the following groups:
- law enforcement (national, state, county and local police);
- emergency responders (fire, emergency medical services, hazardous material mitigation);
- government coordinating agencies (state emergency management agency [state EMA], Federal Emergency Management Agency);
- other government agencies (local governments - city and county, planning organizations, department of health); and
- private industry (construction contractors, private transportation providers).

Depending on the nature and the scale of the event some or all of these organizations can play a role in the state DOT’s actions. A state DOT’s role in the response to an incident may only be to
provide support to “first responders” during the initial phase of an event. In other cases, the state DOT’s training and expertise place it in a leading role. In a third scenario, different agencies lead as event circumstances shift. Working this out at the scene of an event can cause delays and confusion. Differing priorities and missions can cause participants to attempt to meet their agency’s mission to the detriment of the best overall solution. This can be overcome through cooperative planning and understanding of each participating agency’s mission and capabilities.

C. Security agencies

In addition to agencies involved in response and recovery, there are agencies that provide input and information primarily for threats to security. Their duties bring them into contact with state DOTs and create needs for coordination. These agencies include those involved in national security such as:

- the Department of Homeland Security,
- the Federal Bureau of Investigations,
- the Central Intelligence Agency,
- state police/patrol, and
- major metropolitan police.

These institutions collect, validate, and analyze information on potential threats. They pass on, through appropriate channels, information about active threats. Usually, the state police/patrol and other major metropolitan police departments have intelligence units. These intelligence units coordinate with their national counterparts. Additionally, these state and local police intelligence units keep track of local and regional threats.

III. State Needs in Security and Emergency Response

This strategic plan responds to a well-established need for building the capacity of state DOTs to address security and emergency response demands. Section III reviews the survey and needs assessment work which is the foundation of the strategic plan.

A. AASHTO SCOTS 2001 Survey

In 2001, the Special Committee on Transportation Security (SCOTS) of the American Association of State Highway and Transportation Officials (AASHTO) conducted a survey of transportation security issues. The survey identified security training as an emerging need of state DOTs, a finding which led to the creation of the SCOTS Training Subcommittee.
B. AASHTO SCOTS Training Subcommittee 2002 Survey

In 2002, the newly created SCOTS Training Subcommittee sponsored a telephone and electronic mail survey of 28 state DOTs. The 2002 survey focused on current practices, needs, and potential resources for security training. The results are detailed in *State DOTs’ Transportation Security Training Needs: A Briefing Report for AASHTO’s Transportation Security Task Force.*

**Current training**

While 70% of DOTs reported that they provide some security and emergency management training in-house, its scope is limited. Most offerings are in identifying hazardous materials and controlling spills, and emergency response training, which focuses on recovery and restoration of operations for non-terrorism-related issues. The target audience is generally limited to maintenance workers. Training not done in-house is usually done through a State EMA; Federal sources are not widely used. According to the report, a few states—California, Georgia, Oregon, Pennsylvania, Utah, and Washington—offer more advanced training than is typical of state DOTs.

**Needs**

State DOTs need security training, and the federal support to provide it. 70% of respondents said they had assessed or were assessing their training needs, but were hindered in expanding training by shortages of funding, staff, and expertise. 60% wanted federal input and support on how to develop training, with specific attention to “train-the-trainer” approaches.

Two training topics were considered to be “critical needs”: terrorism awareness training and tailored pre- and post-terrorism event emergency response planning. The former would include information on how to be alert for suspicious incidents, people, packages, and vehicles, and how to protect key facilities.

**Resources**

As noted above, many states provide some type of in-house training already, although they lack the resources to create full-fledged security training programs. Some states also reported that they looked to State EMAs for training, while others reported using FEMA classes, universities, and transportation associations.

C. TRB/AASHTO 2003 survey

In a 2003 joint TRB/AASHTO survey of all 50 states, security training again rose to the top of state technical assistance needs. Funding to support transportation security was also of critical concern, as 86% of respondents reported that they do not have sufficient funds. A strong

---

1 Prepared by TransTech Management, Inc., August 2002
majority (94%) reported they were using an “all hazards” approach to dealing with security. Most (54%) are providing training relating to transportation security and critical infrastructure protection, and 84% are participating in Incident Command System training, nearly all through EMAs.

The states surveyed indicated their “top three” priorities in a few areas relevant here. It should be noted that although the range of answers is fairly wide, technical assistance for training continues to be a top priority.

Top 3 transportation security priorities:
- Bridges (assess vulnerabilities, harden, surveillance) (16 states)
- Infrastructure protection (prevent, mitigate) (15 states)
- Highways (assess vulnerabilities, identify targets (13 states)
- Training and exercises for workers (11 states)
- Funding (cost-effectives of measures/ benefit-cost tradeoffs) (9 states)
- Communications (interoperability) (8 states)
- Continuity of ops (7 states)

Top 3 transportation security concerns needing research and sharing:
- Incorporate security into project planning (including checking contractors) (10 states)
- Communications (10 states)
- Training (9 states)
- Threat information (quality, timeliness, means of communication) (9 states)
- Funding (equipment, asset hardening, measuring effectiveness) (9 states)
- HAZMAT (routing, ID, response prep) (6 states)

Top 3 areas for security tech assistance:
- Training and exercises (21 states)
- Communications, including interoperability (16 states)
- Methods for hardening facilities/assets (15 states)
- Vulnerability assessments (7 states)
- Surveillance (6 states)
- Funding (5 states)

D. **Volpe Center needs assessment and resources analysis, 2004**

At the direction of the FHWA Office of the Administrator, the Volpe Center conducted research on the security and emergency response needs of FHWA staff and FHWA stakeholders, including state DOTs. The Center also collected data on existing training and comparable resources.
The needs assessment centered on interviews with 40 individuals (in-person and on the telephone) from the FHWA, state departments of transportation, metropolitan planning organizations, and industry associations. The information was synthesized, resulting in the identification of target audiences, their security and emergency management PCB needs, and required knowledge, skills and abilities.

**Major findings from the needs assessment**

- Those that were interviewed reported that they are unclear about how security-related responsibilities are distributed among agencies at the federal level.

- Interviewees also emphasized that stakeholders of surface transportation typically do not have a great deal of influence in strategic action on security.

- Representatives from State DOTs were emphatic in saying that they could make good use of technical assistance and guidance—and that they are not looking for directives.

- Interviewees routinely noted that they are looking to the FHWA to provide leadership and assistance. Core capabilities that interviewees hope to see developed in the agency include:
  - Providing leading-edge research
  - Supporting tailored training
  - Developing up-to-date guidance
  - Delivering technical assistance
  - Coordinating information exchange
  - Supplying information on funding

- The areas where state DOTs indicated they most need to build their capability are:
  - *Building awareness of security demands* – defining what security means, what is being expected of the agency, analysis of critical links of the transportation network, whether redundancy needs to be built in;
  - *Developing and implementing programs* – what a security program is, how it is different or the same as other hazards, how it fits in with what the DOT already does, how it fits with operations, planning design and maintenance;
  - *Working with other agencies* – expectations that other agencies have of a state DOT and what the DOT can do within its areas of responsibility to meet those expectations;
  - *Assessing network vulnerabilities* – how a DOT should look at security costs, and how to look at the value of assets in relationship to ongoing emergency services, evacuation, response and recovery efforts;
  - *Incorporating security into planning* – how to design projects for security versus all other typical project requirements;
Detecting, deterring, and mitigating threats – understanding the concepts of detection and deterrence, the DOT’s role versus that of law enforcement/national security organizations, what a DOT should do for mitigation;

Hardening facilities – understanding which facilities need to be hardened, and becoming familiar with methods for hardening them;

Planning for evacuation – some states need remedial help on this topic; others are exploring how to apply what they know for natural disasters to the area of security.

Analysis of currently-available resources

A number of institutions and interests now offer training or other professional capacity building help in the area of security and emergency response. These are discussed briefly in the following paragraphs. The Volpe Center’s research on relevant available training is then summarized.

The Federal Government is the dominant source of training and other assistance. Traditionally, this type of training has been focused on the law enforcement and first responder communities. The Federal Transit Administration (FTA) has developed many courses related to security, but they were originally designed for transit. Other Federal agencies such as the National Institutes of Health (NIH), the Army Corps of Engineers and the Department of Energy (DOE) each have courses that are related to but not directly relevant for state DOTs. The National Transit Institute has a series of security-related courses, which are oriented to transit needs.

State and local governments also have developed training, tailored to their own needs and contexts. That training has focused on basic awareness, and has tended to be directed to the law enforcement and first responder communities.

Colleges and universities that have law enforcement programs have security and emergency management training, but it focuses on areas that are tangential to transportation. Colleges and universities with transportation programs are beginning to add security to their curricula but have limited security-related course offerings.

Finally, the National Academy of Science (NAS) Transportation Research Board (TRB) operates both the National Highway Cooperative Research Program (NCHRP) and the Transit Cooperative Research Program (TCRP), which received jumpstart funding for security research after the terrorist attacks in September 2001. Sponsored research may produce material that can be used for training or other professional capacity building resources. Additionally, as part of its research, TRB and the cooperative research programs run meetings and workshops. However, due to the nature of the organization these are not offered in an ongoing and sustained way.
The Volpe team collected data on training now available in the areas of security and emergency response. That research focused on training that is offered regularly and repeatedly from well-publicized sources, in contrast to training such as workshops that are somewhat ad hoc and occur only once. And the research focused on well-publicized sources; it therefore understates training that is developed and provided by various state DOTs. However, discussions with a sample of state DOTs, and prior survey work conducted by AASHTO and TRB suggests that such state DOT training is limited in general and, where it is provided, focuses on just a few topics. Volpe’s data collection supports several major conclusions that provide guidance for this PCB effort.

- There is room to diversify and improve the methods used for helping state DOTs build their professional capacity.
- There are many security and emergency management training resources, but relatively few focus on surface transportation.
- Of the courses that include some material relevant to security issues, few address in whole or in part the issues identified as priorities by state DOTs. Most offerings cover one of the following subjects:
  - Incident Command, Incident Management, or Unified Command;
  - Basic security awareness;
  - Handling of chemical, nuclear, radiological, and biological events; and
  - Global and geo-political aspects of Homeland Security.
- Training is often not tailored to state context, demands, constraints.
- Much existing training is not practical for states, due to duration, travel, and schedule.
- Available information provides little or no direction on how an agency can begin to integrate security and emergency response strategies into its organization, particularly in support of its day-to-day functions.
- There is no single, central clearinghouse for security and emergency management resources.
- Valuable data and information on security and emergency management exist, but are largely unavailable because much is classified.

The next two sections apply insights derived from the foregoing research. In section IV, the concept of professional capacity building is outlined, and a “PCB toolkit” presented. Section V then provides the heart of this document, a strategic plan for building the professional capacity of state DOTs in the areas of security and emergency response.
IV. Overview Of An Integrated Professional Capacity Building Initiative

A. The concept of professional capacity building

State DOTs need help building the knowledge, skills, and abilities of their staff across a wide variety of areas relating to transportation security and emergency response. Moreover, they do not need to simply enable staff to obtain the knowledge, skills, and abilities, but to maintain and adapt them as circumstances and demands shift. Layered over this need is the reality that states vary widely in their circumstances and requirements, but all tend to have limited capacity to offer or maintain new professional development resources. They also have limited means to support costly delivery of training or other resources to their staff.

These are the assumptions on which this professional capacity building initiative is founded. State DOTs need help that is made available in ways that are:

- tailored to the varying needs of different audiences;
- targeted in delivery so that they reach the right people;
- timed so that they are of maximum impact;
- made easily accessible to the many state and local professionals who have limited travel funding;
- flexible so that they can be adapted as circumstances change; and
- cost-effective, so that reach (and, hopefully, impact) can be maximized.

A capacity building effort would be an important complement to the regulatory approach of the DHS. Overall, the goal is to foster an effective and adaptive workforce. The “adaptive” element is important, as we want a workforce that can adjust as circumstances and needs change. As this goal might suggest, capacity building is about more than training. It supplies tailored, targeted and timely help, and this is accomplished in part by offering an integrated set of resources—including, but not limited to, training.

B. PCB toolkit

The following are tools that could comprise a complete professional capacity building toolkit. Successful federal programs in ITS, transportation planning, roadway safety, freight planning, and environmental competency use some or all of these tools.

- Training – In-depth learning in a topic area with multiple learning objectives, typically in an extended (more than one day) session. Could be face-to-face in a classroom setting, in real time by video or other electronic means, or self-paced via the Internet.
• **Scan** – Travel by representatives of multiple organizations to 2 or more peer agencies to observe and receive information. Usually 3-5 days and long-distance travel.

• **Peer exchange** – In-person session where experts from one group or organization visit their counterparts at another organization to share experiences, tools, and insights. Focus is typically on a well-defined topic, with the goal of developing a plan for action to address known challenges. Duration is typically 1-2 days.

• **Workshop** – Face-to-face session enabling participants to not only learn but also apply principles and/or tools to real-world challenges. This could include tabletop or field exercises. Duration would often be less than one day, but could be longer.

• **Seminar** – Short (typically 1-3 hours) session, either in person or remote, where material is communicated primarily one way, but with some (limited) opportunity for question and answer. This form of PCB could include attending conference panels.

• **Information-sharing** – Includes development and delivery of information, typically via websites or other means that would allow users to visit at their own pace and select the information that best meets their needs. Includes case studies, databases, listserves, fact sheets, and more. Could also include short, oral briefings to executives or others.

• **Technical assistance** – Short-term help with targeted questions or service needs. This could include support for conducting tabletop or field exercises, or completing threat and vulnerability assessments.

Tables on the following pages provide additional details on each of these tools, including tradeoffs, implementation timelines, and approximate costs.
## Implementation Tools for Capacity Building Programs

<table>
<thead>
<tr>
<th>Tool</th>
<th>Strengths</th>
<th>Weaknesses</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **Training**      | • Provides in-depth treatment of multiple learning objectives  
                   • Can be done either in person (preferred) or at a distance                                                                                                                                         | • Costly to develop  
                   • Long lead time required  
                   • May require travel  
                   • Commitment of staff time to participate  
                   • In-person delivery requires minimum number of participants  
                   • Timing of delivery may not match timing of need                                                                                                                                                    | • 9 months – 1 year  
                   • $125-$175,000 to develop, pilot, and deliver                                                                                                                                                    |                |
| **Scan Tour**     | • Collects and synthesizes effective practices  
                   • Enables learning through direct, real-time observation  
                   • Presents lessons learned  
                   • Supports networking of peers                                                                                                                                  | • Requires extensive data collection/research  
                   • Logistically-intensive                                                                                                                                                    | • Up to one year  
                   • $50-$70,000                                                                                                                                                                              |                |
| **Peer Exchange** | • Enables sharing of cutting-edge practices among peers  
                   • Can provide targeted technical assistance  
                   • Encourages local and regional coordination  
                   • Enables peer networking                                                                                                                                                                                  | • Impacts relatively few (participants)  
                   • Impact may depend on follow-up tracking  
                   • Focuses on one topic  
                   • May require travel funds                                                                                                                                                    | • 3 to 5 months  
                   • $15-25,000 per event                                                                                                                                                    |                |
<table>
<thead>
<tr>
<th>Tool</th>
<th>PRO</th>
<th>CON</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workshop</td>
<td>• Allows for group discussion of topics</td>
<td>• Requires host location, facilitator, and travel funds</td>
<td>• 3 to 6 months</td>
</tr>
<tr>
<td></td>
<td>• Encourages brainstorming and recommendation development</td>
<td></td>
<td>• Cost varies based on location, number of travelers, days of event ($20-50,000)</td>
</tr>
<tr>
<td></td>
<td>• Creates networking opportunities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Addresses needs and goals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seminar</td>
<td>• Can serve as a roundtable discussion</td>
<td>• May require high-speed web access</td>
<td>• 4 to 6 weeks</td>
</tr>
<tr>
<td></td>
<td>• Can reach a large audience</td>
<td>• Tends to treat topics more superficially than other methods</td>
<td>• $5,000 or less per seminar</td>
</tr>
<tr>
<td></td>
<td>• Can be done via web</td>
<td>• Less interactive than a workshop or peer exchange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can be archived for reference or re-broadcast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information-Sharing</td>
<td>• Can provide a centralized location for information, databases, on-line forums and other tools</td>
<td>• Requires maintenance</td>
<td>• 1 to 3 months for development</td>
</tr>
<tr>
<td></td>
<td>• Provides up-to-date information on events, training</td>
<td>• Relatively passive resource, so impact is difficult to gauge</td>
<td>• $10-$15,000 for website development</td>
</tr>
<tr>
<td></td>
<td>• Always available to a wide audience</td>
<td>• May require high-speed web access</td>
<td>• $30-$45,000 for annual site maintenance</td>
</tr>
<tr>
<td></td>
<td>• Can serve many users with low marginal costs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Assistance</td>
<td>• Flexible: can be tailored to project- and-agency-specific needs</td>
<td>• Requires access to sometimes-specialized expertise</td>
<td>• Once the program is developed, lead time is minimal</td>
</tr>
<tr>
<td></td>
<td>• No or short lead time, depending on the nature of the problem</td>
<td>• May require travel</td>
<td>• Cost varies widely, but will tend to be less than most other elements</td>
</tr>
<tr>
<td></td>
<td>• Impact on actions can be significant and measurable</td>
<td>• Difficult to disseminate results to a wider audience</td>
<td></td>
</tr>
</tbody>
</table>
V. Strategic Plan For a Security/Emergency Response PCB Initiative

A. Goal of this initiative

To a significant extent, the challenges state DOTs now confront as they strive to meet their security and emergency response demands share one aspect: uncertainty. There are multiple and increasing expectations being imposed on states. This in itself creates uncertainty. The situation is exacerbated by the many agencies involved both in providing for security and emergency response, and in communicating expectations or requirements. Not surprisingly, there are also many sources of training, information and resources, which necessarily vary widely in accessibility and quality. Just knowing what those resources are and how to obtain them is daunting to most potential users. Finally, there is the simple fact that the state DOTs vary widely in circumstances, creating some confusion about how to define standards and establish resources that can be of maximum value.

In all, there is a need for a trusted, reliable, and reasonably comprehensive resource for information and assistance. This plan is designed to achieve the goal of providing such a resource. That goal will be best realized if this effort is supported and implemented by all critical stakeholder interests, and conceived as a coherent, well-integrated whole.

B. Objectives

To achieve the goal described above, this PCB initiative should be organized around the following objectives:

1. **Establish and maintain partnerships.** As noted above, state DOTs will benefit most from a reasonably comprehensive and well-integrated effort. This can only be achieved with the involvement of multiple stakeholder interests, not only during planning, but also throughout implementation of this initiative.

2. **Provide a one-stop shop for identifying and linking to resources.** There are many organizations providing training, information and other resources. Target audiences need help identifying those organizations and easily accessing resources.

3. **Help users filter resources, so that they access support that is most effective and appropriate.** With the many sources, there is also great variation in quality and usefulness – great value would be added by helping users filter what is available.

4. **Enable members of the communities of interest to work with one another.** Audiences for this PCB initiative are dispersed, vary widely in circumstances and demands, and have relatively limited ability to travel. At the same time, they have clearly articulated a desire to communicate with and learn from one another. This PCB initiative can add enormous value to the extent that it facilitates that communication, by collecting
and providing central access to contact information, providing technical support to electronic communications (e.g. a listserv), and supporting travel where appropriate.

5. **Develop and disseminate information.** Given that many of those that need help are uncertain about requirements and about who does what, a capacity building effort should include development and dissemination of information and direction.

6. **Collect, synthesize, and disseminate effective practices.** Some agencies are doing good things in the name of security – a PCB program can add value by finding these examples, synthesizing them, and providing easy access to that information.

7. **Support development and delivery of courses.** Though this plan stresses the importance of providing resources in a variety of formats to match the varying needs and circumstances of state DOTs, traditional training should remain a core resource. Partners to the initiative should plan to support the development of curricula and course materials, as well as delivery. It is likely that the National Highway Institute (NHI) and, perhaps, the National Transit Institute (NTI) would be important contributors.

C. **Implementation principles**

To achieve the above objectives, this PCB initiative will follow the principles described below:

1. **Build on the FHWA’s recognized leadership role.** Highways are recognized to be a critical component in implementing the national security agenda. Interviewees for the Volpe needs assessment consistently noted that state DOTs and others are looking to the FHWA for guidance on security and emergency response. As the leader in the design, construction and continued operation and maintenance of the national highway system, the FHWA is ideally positioned to have an active role in the advancement of a national security and emergency response agenda.

2. **Partner to design, steer, and implement the PCB initiative.** There are many potential partners for a capacity building effort. A number of professional associations and educational organizations have developed security oriented courses, training and technical assistance. The FHWA already works closely with most or all of these associations and organizations in other areas. The creation of partnerships needs to be strengthened for security and emergency management. This collaboration must be done to minimize redundancy as well as deliver the knowledge and skills needed by transportation professionals. Potential partners include:
   - The Office of Domestic Preparedness (ODP),
   - The Transportation Security Agency (TSA),
   - The Office of Information Analysis and Infrastructure Protection (IAIP),
   - The Department of Defense (DOD) Technical Support Working Group (TSWG),
   - The Federal Emergency Management Administration,
   - American Association of State Highway and Transportation Officials (AASHTO),
   - The National Highway Institute, and
   - The National Transit Institute.
3. **Use existing technical information and tools.** A considerable amount of technical information (including DOD classified information) is available and usable for advancement for this initiative. Leveraging this opportunity includes encapsulating information in the form of easily digestible outreach materials, and releasing case studies, lessons learned, and effective practices.

4. **Build on the success and resources of established PCB programs.** Existing programs provide a model for development of this PCB initiative. The FHWA has established PCB programs (including for ITS and transportation planning) that provide a model for determining the most effective delivery methods. These programs have had great success with websites, technical advisories, and peer-to-peer networks.

5. **Where possible, adapt existing training.** While there is relatively little known training that is ready for use by state DOTs on their most important needs, certain training exists that could be adapted for states. In addition, it is likely that at least a few states have tried to provide training—or other help—to their staff. Those efforts too could be adapted for use more broadly.

6. **Explore alternatives to traditional classroom training.** Given that state DOTs are constrained in their ability to either fund training or the travel that might be required, one operating principle of this initiative should be to leverage technology so that staff can receive training in ways that are flexible and cost-effective.

**D. Priorities and learning objectives for the PCB initiative**

The Volpe Center worked with AASHTO, TRB, and a sample of state DOTs to prioritize the observed needs of state DOTs. Volpe presented a sample of state DOTs with a list of the knowledge, skills, and abilities (KSAs) that prior research showed to be of some importance to state DOTs. The DOTs were asked to sort each KSA into one of four tiers of importance: those for which training or other PCB resources are urgently needed, those for which it is important to provide resources, those where training or other help may be needed at some point, and those for which no PCB effort is required. The resulting priorities were then sorted into clusters by the Volpe Center. Finally, these results were reviewed with members of the AASHTO Special Committee on Transportation Security, and with the Transportation Research Board’s Surface Transportation Security Research Panel (NCHRP Project 20-59). The five clusters and associated topics are summarized in the following table. The stars indicate the relative need for PCB resources, where three stars represent an urgent need, two stars an important need, and one star a need to be addressed at some time.

Based on all of the foregoing research and analysis, Volpe has developed recommendations for providing PCB resources to address state DOT needs for security and emergency response. Those recommendations begin with learning objectives that should be associated with each KSA topic area. These objectives do not presume any particular method of resource delivery (e.g. training versus technical assistance). It should be noted that these are offered as preliminary

---

2 Respondents were California, Florida, Idaho, Illinois, Minnesota, Missouri, New York, Virginia, and Wisconsin.
objectives. They will likely need further refinement in coordination with partners and stakeholders providing technical input.

| Positioning the DOT to respond to a disaster |  |
| Coordinating with other institutions and agencies | ⭐⭐⭐ |
| Enhancing inter-agency communications | ⭐⭐⭐ |
| Planning for evacuation | ⭐² |
| Building a security/emergency response program |  |
| Elevating transportation's role in security/emergency response | ⭐⭐⭐ |
| Implementing a security/emergency response program | ⭐⭐⭐ |
| Obtaining funding for security/emergency response | ⭐² |
| Integrating security throughout agency | ⭐ |
| Using operations to enhance security/emergency response |  |
| Operational methods to secure facilities | ⭐⭐⭐ |
| Monitoring facilities/assets for indicators of threat | ⭐² |
| Processes/resources for maintaining continuity of operations | ⭐² |
| Managing sensitive information | ⭐ |
| Engineering and construction for security/emergency response |  |
| Design methods for facilities security | ⭐⭐⭐ |
| Identifying critical assets and assessing vulnerability | ⭐⭐⭐ |
| Hardening assets for recovery from blast & contamination | ⭐² |
| Risk assessment methodologies | ⭐ |
| Transportation planning for security/emergency response |  |
| Incorporating security strategies in plans and studies | ⭐⭐⭐ |
| Roles for MPOs in security planning processes | ⭐ |

1. Positioning the State DOT to Respond to a Disaster

1.1. Coordinating with all partners (⭐⭐⭐) – The overall objective for this topic is to help state DOTs develop more effective working relationships with their counterparts in Federal, state and local agencies who have some role in event response. PCB resources should support learning:

- the importance of establishing relationships with first responders, emergency management professionals, and others at local, state, regional, and federal levels,
- the benefits of those relationships, and the costs of failing to establish relationships,
- typical roles and responsibilities of the various partners in emergency response,
- how an “all hazards” approach influences coordination with partners,
how to ensure that other agencies’ expectations are reasonable and realistic based on items like: DOT work rules, DOT assets, and DOT skills,
- tools and techniques for establishing relationships and using them to achieve effective coordination,
- the role of private companies, non-governmental organizations and others in both planning and management of security and emergency response

1.2. **Enhancing inter-agency communications (★★★)** – A major and ongoing challenge to effective emergency response is reliable communication between agencies, at and between levels of authority. This is in part a technology challenge, but in part one of organization and process. PCB resources should support learning:
- how to specify the benefits of effective communications, and the costs of ineffective communications,
- factors that contribute to effective communications (including technology, organization, and protocols),
- technological challenges and possible remedies,
- strategies for anticipating and offsetting communications issues through organizational innovations
- the relationship between communications during routine operations and during security or natural disaster events.

1.3. **Planning for Evacuation (★★)** – Hurricanes Katrina and Rita revealed the importance of having an effective plan for mass evacuation of residents, and transportation’s vital role in that plan. PCB resources under this topic should support learning:
- strategies for coordination and communication with other agencies for the actual evacuation (i.e., staffing the route),
- planning for evacuees’ needs once evacuated,
- how to manage route planning and related issues e.g., fuel deployment, en route medical services, removal and storage of disabled vehicles etc.,
- how to determine where to preposition supplies,
- how to coordinate with destination locations,
- how to coordinate with other agencies (police, fire, road side service etc.),
- how to plan evacuations spanning more than one state.

2. **Building a Transportation Security/Emergency Response Program**

2.1. **Elevating transportation's role in security/emergency response (★★★★)** – In the research leading to this strategic plan, state DOTs (and other stakeholders) emphasized that the function and importance of transportation to security and emergency response is still not well-understood or appreciated. State DOTs, in particular, need help articulating what might be called the “business case” for putting resources behind an integrated security and emergency response program. Thus, PCB resources under this topic should support learning:
- how to explain transportation’s role in the economy, in supporting
evacuation, in supporting post incident response and post incident recovery

- explain why the security of the surface transportation systems is important to the state and region
- the benefits of being proactive with security, and risks of inaction
- the relationship between strategies for security and for emergency response
- critical factors for success in establishing a program for security and emergency response

2.2. **Guidelines for implementing a security/emergency response program (★★★★)**

- States are struggling with how to meet their obligations for addressing threats to security without overwhelming their resources. They also want to avoid “reinventing the wheel”; that is, they want to adapt existing resources and strategies for emergency response wherever possible. States are simultaneously attempting to better integrate different functions across the agency. For example, there is increasing interest in linking planning with operations, so that the long-term requirements associated with operations are anticipated during the planning phase. With all of this in mind, training or other PCB resources should aid in learning:
  - parameters of an “all hazards” approach to security and emergency response,
  - similarities and differences between events of natural and malevolent origin, for each phase of the event life cycle (deter, detect, respond, recover)
  - critical areas of focus for implementing a security plan, including security at asset locations, security for employees, cyber security, and security of sensitive documents,
  - organizational models for a comprehensive security and emergency response program,
  - strategies for incorporating security and emergency response considerations into existing processes for planning, engineering, and operations.

2.3. **How to identify funding sources (★★)**

- State DOTs (along with metropolitan jurisdictions and others) continue to be concerned about what they perceive as a mismatch between increasing expectations on them to provide for security and available funding to support their security efforts. PCB resources targeting this concern should support learning:
  - major public sources of funding at federal and state levels
  - strategies for working with the private sector,
  - how to leverage the relationships among security, emergency response, operations, and economic development to maximize access to funding programs,
  - partnership opportunities within and between states.

2.4. **Methods for integrating security into all aspects of an agency (★)**

- While basic awareness of security-related demands among transportation professionals has improved significantly over the past several years, there is still a need to increase and update that awareness. PCB resources should help organizations look at how their employees need to change their way of thinking and acting so
that security becomes second nature. PCB resources should support learning:
- how security considerations vary by function within the typical state DOT,
- strategies for building an internally coherent and integrated approach to communicating essential principles of awareness throughout the organization,
- professional development practices for maintaining and updating security awareness

3. Using Operations to Enhance Security and Emergency Response

3.1. Operational methods to secure facilities (★★☆) – State DOT operations are at the center of both security and emergency response needs. On a day-to-day basis the operations, inspections, and maintenance staff are in position to detect and, possibly, deter security threats. They will also provide much of the human resources required to respond to and recover from the transportation impacts of an emergency event of any kind. States are therefore very interested in how to provide for security-related needs through operations. PCB resources should support learning:
- how to specify the ways that operations affects security and emergency response,
- how to apply that specification to job descriptions and work processes,
- how to create facility inspection guidelines that include assessing vulnerability of critical components
- strategies for leveraging ITS systems and transportation management centers to address security and emergency response,
- how to develop operational security plans for staffed facilities (levels of security for different areas; badging for staff, contractors, visitors at administration facilities and construction sites; deploying a security force; and, use of other assets like traffic control centers in security operations)

3.2. Monitoring facilities and assets for threats and vulnerabilities (★★) – One of the areas where the difficulty in distinguishing transportation’s responsibilities from public safety’s responsibilities is most evident is in monitoring of facilities for threats to security. Most state DOT staff do not enforce the law, yet are often closest to the facilities and infrastructure that may be targets of violent acts. PCB resources need to support learning:
- how to scope the responsibilities of the DOT with respect to monitoring and threat detection
- key knowledge and skills that staff need to possess,
- tools that can make monitoring more efficient and effective,
- strategies and standards for instituting professional development practices
- possible coordination needs, including with those responsible for adjacent facilities or assets (e.g. chemical plants, dams, etc.) that may have security/emergency response implications.

3.3. Processes and resources for maintaining continuity of operations (★★☆) – No matter what type of incident occurs, a state DOT cannot assist in the recovery if
it does not have continuing operations. From the simplest instruction issued to complex issues of payroll, contracting, regulation, and waivers of regulation, a state DOT needs to be able to have continuity of operations. PCB resources developed need to support participants’ learning:
• how to determine what are critical operations,
• how they can be maintained during a security or emergency management event,
• what is necessary to support the operations.

3.4. **Managing sensitive information** (★) – Historically and under many state laws, State DOTs have shared many of the documents that they have developed freely with the public. However, some of these documents can provide insight into security vulnerabilities of the organization and its assets. It is often necessary to provide some of these documents to those outside of the department for contracting and other reasons. PCB resources would include the following learning objectives:
• guidance on approaches to managing access to critical engineering and operations documents,
• Security necessary for security plans, emergency response plans and continuity of operations plans,
• guidance for protecting documents that need to be included for purposes of contract bids (e.g., facility and asset blueprints),
• descriptions and examples taken from real world best practices as well as federal law involved in the safeguard of sensitive material and documents.

4. **ENGINEERING AND CONSTRUCTION FOR SECURITY AND EMERGENCY RESPONSE**

4.1. **Design methods for facilities security** (★★★) – PCB resources for this topic should focus on “vertical” assets, i.e. primarily buildings owned or operated by the state DOT. Resources should support learning about the following issues related to structural design:
- how to categorize different types of facilities in terms of security implications,
- how to assess operational and maintenance implications of design decisions,
- methods for making trade-off decisions between capital and operating/maintenance expenditures,
- how design can enable rapid recovery and continuity of operations.

4.2. **Identifying critical assets and assessing vulnerability** (★★★) – State DOTs and other transportation agencies continue to struggle with how to identify critical assets and assess their vulnerability. Among the learning objectives that a PCB initiative could support are:
- how to document how a state DOT's assets (e.g., bridges, tunnels, overpasses etc.) are used in a local as well as regional and national context
- becoming familiar with different methods for assessing vulnerability
- identifying standards that may be recommended for defining criticality and vulnerability
- identifying stakeholder agencies and mastering methods for coordinating with them to define criticality and assess vulnerability.

4.3. **Hardening assets for recovery from blasts and contamination (★★) –** State DOTs either control or are a major stakeholder in major infrastructure—bridges, tunnels, intermodal connectors—that is a likely target for attack or is potentially vulnerable to crippling damage from a natural disaster. Thus, there is considerable interest in methods for hardening those assets to withstand impacts and recover quickly. This PCB initiative can add value by supporting learning of:

- the latest research on blast resistance of materials and structural designs,
- methods and tools for assessing blast resistance,
- how different types of materials used in construction react to chemical, biological or radiological (CBR) agents,
- how location of assets and design may unintentionally incorporate potential vulnerabilities

4.4. **Risk assessment methodology (★) –** Risk assessment is complex. There are a number of different methodologies, there are a variety of factors to consider when developing a risk assessment and there are several complicated formulas for calculating risk. In addition to the variety of methodologies and inputs used in risk analysis, there are a number of different methods that different federal, state and local agencies use and in some cases require. The learning objectives for this topic would include:

- information on risk assessment methodology,
- methods different Federal Government organizations recommend/require
- what methods state DOTs have used,
- what experiences different states have had in conducting risk assessments

5. **Transportation Planning for Security and Emergency Response**

5.1. **Incorporating security strategies into plans and studies (★★★★) –** From major construction projects to normal operations, state DOTs must develop studies and plans. Historically, these plans and studies have not considered security. However, it is always less expensive and much more efficient to incorporate security into a project or study at the beginning. The cost of not incorporating security in the planning and study phase can increase the final cost of a project significantly. Learning objectives in this PCB area can include:

- considerations for meeting the increased security/emergency management roles that transportation networks are being asked to perform,
- minimizing the risk of network disruption,
• the use of the transportation network for evacuation,
• the use of the transportation networks for event response

5.2. Possible roles for MPOs in security planning (★) – Transportation projects begin with planning. Metropolitan Planning Organizations develop the Transportation Improvement Plan (TIP) for their metropolitan region. Since including security early in the planning process is one of the keys to a successful security program it is important for both MPO staff and state DOT staff to understand how security can be incorporated in the planning process. A PCB program would include the following learning objectives:
• MPO planning process,
• how security can be incorporated into the MPO planning process,
• how security will impact the transportation improvement plan (TIP),
• how security will fit into the process to develop a TIP,
• impacts on the state-wide transportation improvement plan (STIP).

E. Multi-year plan

With these broadly-framed learning objectives in mind, we have provided four types of recommendations for each topic:

1. Phasing – Each topic is sorted into one of three phases, according to how soon PCB resources should be deployed. Most of the urgent topics are recommended for action in year one. Remaining topics are recommended for action in years two and three.

2. Target audience – Each topic is aligned with one or more target audiences, corresponding to generic functions of a state DOT. This indicates to which specific audiences training or other assistance on a specific topic should be targeted.

3. Level of competency – While multiple audiences may be the target of PCB for a single topic, not all of those audiences will necessarily need to become competent to the same level. For some, it is enough to have basic awareness sufficient to communicate in general terms about the topic. Others will need understanding of the topic, such that they could ask appropriate questions and direct the work of others. A few will need mastery, such that they could not only communicate about the topic and direct the work of others, but could complete technical tasks related to the topic.

4. PCB resource type – For each combination of topic and state DOT audience, we have recommended certain types of PCB resources. These tend to correlate with competency level. For example, those needing mastery of a topic should have access to more direct, in-depth assistance than those needing only awareness. This enables tailoring of resource delivery to the particular responsibilities and accessibility of state DOT personnel.

The matrix on the following page summarizes our recommendations, and represents the overview of a multi-year action plan for building the capacity of state DOTs to address their security and emergency response needs. Details for year one are provided thereafter.
# Overview of Multi-Year Plan for Building State DOT Capacity in Security/Emergency Response

<table>
<thead>
<tr>
<th>Topic Area</th>
<th>Executive Level</th>
<th>Engineering/Construction</th>
<th>Operations/Maintenance</th>
<th>Planning</th>
<th>Programming/Procure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Year One</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordinating with other institutions and agencies</td>
<td>Event response</td>
<td>W'shop, Scan</td>
<td>W'shop, Scan</td>
<td>Peer, Sem</td>
<td></td>
</tr>
<tr>
<td>Elevating transportation's role</td>
<td>Building a program</td>
<td>W'shop, Scan</td>
<td>W'shop, Scan</td>
<td>Peer, Sem</td>
<td></td>
</tr>
<tr>
<td>Implementing a security/emerg response program</td>
<td>Building a program</td>
<td>W'shop, Scan</td>
<td>W'shop, Scan</td>
<td>Peer, Sem</td>
<td></td>
</tr>
<tr>
<td>Operational methods to secure facilities</td>
<td>Operations</td>
<td>Scan</td>
<td>Scan</td>
<td>Scan</td>
<td>Scan</td>
</tr>
<tr>
<td>Design methods for facilities security</td>
<td>Design/Engineering</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Identifying critical assets, assessing vulnerability</td>
<td>Design/Engineering</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td><strong>Year Two</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhancing inter-agency communications</td>
<td>Event response</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Planning for evacuation</td>
<td>Event response</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Funding for security/emergency response</td>
<td>Building a program</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Monitoring for indicators of threat</td>
<td>Operations</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Maintaining continuity of ops</td>
<td>Operations</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Hardening assets</td>
<td>Design/Engineering</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Incorporating security in plans and studies</td>
<td>Planning</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td><strong>Year Three</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managing sensitive information</td>
<td>Operations</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Integrating security throughout agency</td>
<td>Building a program</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Risk assessment methodologies</td>
<td>Design/Engineering</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
<tr>
<td>Roles for MPOs in security planning</td>
<td>Planning</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
<td>Scan, Sem, Info</td>
</tr>
</tbody>
</table>

Train - Training  
Peer - Peer Exchange  
Info - Info Dissemination  
Tech - Technical Assistance  
Scan - Scan tour  
W'shop - Workshop  
Sem - Seminar  

<table>
<thead>
<tr>
<th>Mastery</th>
<th>Understanding</th>
<th>Awareness</th>
</tr>
</thead>
</table>

Security/Emergency Response PCB Strategic Plan - DRAFT  
24
F. Year one actions

1. Identify partners for overall support and establish a resource plan.

FHWA and AASHTO should reach out to potential partners for this initiative, including:
- FHWA Office of Infrastructure and Office of Operations
- Department of Homeland Security (DHS) Office of Domestic Preparedness (ODP), and Transportation Security Agency (TSA);
- Department of Defense Technical Support Working Group (TSWG);
- Federal Transit Administration (FTA)

Part of this action should be to identify sources of financial and other support and initiate activities to obtain support. Opportunities include FHWA research programs, DHS grant programs, and pooled-fund studies. Activities could thus include conducting research to explore these and other opportunities, writing grant proposals, and coordinating participation for pooled-fund studies.

2. Establish a steering committee and technical working groups comprised of partners and stakeholders.

The FHWA and AASHTO should work together to establish a steering committee for this PCB initiative. In addition to the above, probable members include:
- AASHTO
- Volpe Center
- FHWA Office of Professional and Corporate Development
- Representatives of state DOTs (for technical working groups)

In addition to communication via electronic mail and telephone, the Steering Committee should be convened on one or more occasions to discuss, modify as needed, and ratify both a guiding mission and set of objectives for this PCB initiative. The Committee would also review and revise, as needed, the first-year plan of action, and coordinate the formation of technical working groups. These groups would be charged with providing technical input to specific actions, and with assisting in data collection and outreach where needed and appropriate.

3. To address the topic of coordination among state DOTs and others for effective emergency response, organize and support a series of regional workshops.

Each workshop would bring together transportation agency management and security personnel; local police and fire personnel responsible for emergency management coordination; emergency medical services and hospital disaster relief coordinators; state
and local government emergency management coordinators; and federal law enforcement and national security agencies. Each workshop will be designed to:

- help transportation and emergency response agencies work together to prepare and protect their community with coordination, communication, planning and practice of safety and security measures;
- increase participant awareness of the critical processes, issues, and activities that arise during and following an emergency, and of possible approaches for addressing these challenges;
- provide participants with a better understanding of the roles played by each agency and begin the process of developing the plans, tools and relationships necessary to respond effectively in an emergency situation;
- enhance working relationships among personnel from multiple organizations responsible for emergency preparedness and response; and
- identify areas for transportation emergency response planning and readiness.

There are two very successful models that can guide planning for and implementation of this series. In 2002, the FHWA Office of Operations sponsored approximately 10 workshops on emergency transportation operations and response. Between 2002 and 2003, the FTA Office of Safety and Security sponsored 22 regional “Connecting Communities” workshops hosted by transit agencies. Workshops for security and emergency response should be developed by adapting appropriately from the experience with these two models.

4. **To address the topic of elevating transportation's role in security/emergency response, support development and delivery of a seminar designed for executive-level staff.**

The objective of the seminar would be to enable participants to articulate the importance of having a program that addresses the security and emergency response capacity of the surface transportation network, and to specify at a strategic level the major elements of such a program. Issues would likely include the following:

- Benefits of being proactive with security and risks of inaction
- Relationship between security and emergency response
- Critical factors for success in establishing a program
- Organizational and resource models for such a program

The seminar would be delivered in under 2 hours, comprising three segments:

- A lecture to provide information on the core issues outlined above.
- One or two case studies based on state DOTs who have successful programs.
- Discussion

This seminar can be conducted either in-person, ideally as part of a regional or national conference, or via webinar. Delivery costs are comparable for either method. Existing material that provide a model for this concept and materials for its development include
the pooled-fund study of the Pennsylvania DOT (PennDOT) Transportation Security Strategy (Volpe Center, 2004); and (b) the FTA Security Design Considerations.

5. To address the topic of implementing a security/emergency response program, develop effective practices case studies and conduct a series of webinars to review the studies.

All state DOTs have some form of security and emergency response program in place. States that regularly experience hurricanes have evacuation plans, California has plans to deal with earthquake precipitated emergencies, states in the north have plans in place for winter weather emergency response, states in the plains and Midwest have tornado response plans and a number of state DOTs all across the country have developed security related response programs. It will benefit the state DOTs, and the nation, to capture this knowledge base in a series of case studies showing what works for an individual state DOT. Additionally, cross-cutting studies comparing what has worked under different circumstances would be beneficial.

To present this information to the state DOTs, two methods would be used. First, the studies themselves would be posted for distribution on the web. Second, a series of webinars would be conducted to review the case studies and present the results of the cross cutting studies. The webinars would have participation not only from the authors of the case studies and the cross-cutting studies but also would include as presenters representatives from the studied state DOT.

6. To address the topic of operational methods to secure facilities, support a series of peer exchanges, each involving three or four state DOTs.

The Volpe needs assessment showed that states are very interested in connecting with and learning from each other. They would like to receive technical and financial support for direct exchange of ideas and experiences. We recommend a series of peer exchanges among state DOTs, focused on the topic of operational methods for security. Typically, one agency would host two to three others on site. The guests would make presentations on their experiences addressing a particular challenge. All participants would then brainstorm possible actions the host agency can take to address its challenges.

The topic of operational methods to enhance security is ideally suited to the peer exchange format. Agencies can easily summarize and illustrate their practices, and the face-to-face format allows for control of access, so that the security of potentially sensitive information is not compromised. Each exchange could be run over the course of two days. We recommend a two-phase approach, with executive-level staff involved on day one, and managers and other staff on day two. Each exchange would yield a written summary that—appropriately screened for sensitive content—could be made available to the wider state DOT community via a website. Another product could be a contact list comprising exchange participants, so that states could better network with colleagues.
The FHWA and FTA Offices of Planning co-sponsor a peer exchange program as part of the Transportation Planning Capacity Building (TPCB) Program, with technical and logistical support provided by the Volpe Center. The TPCB peer program provides a known and very successful model for this PCB initiative.

**7. Support a technical advisory team to provide on-request assistance in identifying critical assets and assessing their vulnerability, and pilot this approach with one state DOT.**

The technical advisory team would be comprised of between two and four specialists from the FHWA, supplemented as necessary by experts from the Volpe Center or private-sector contractors. The team would function in a way similar to certification review teams, but in the spirit of providing technical assistance, not regulatory oversight. The team would provide advice on how to inventory assets, and on how to assess vulnerability of high priority assets. Materials could include checklists, methods, and tools that states can utilize.

Teams would work with the host agency to develop an agenda, would be on site for 2 to 3 days, and would then develop a report for use by the host agency. An option for this recommendation would be to also generate a report for use by other agencies. In year one, we recommend piloting this team concept with one state DOT. Such an effort might be supported by a pooled-fund study, similar to the PennDOT Transportation Security Strategy project (see recommendation #5).

**8. To address the topic of design methods for facilities security, research and publish information on methods and procedures.**

This effort would compile and present information for state DOTs on both the methods and procedures for securing facilities. The document would provide information on all of the different types of facilities that a state DOT could own. The document would also provide information on facilities for which a state DOT is often responsible. The model for this effort is the Federal Transit Administration’s *Transit Security Design Considerations*, which has been very well-received. The proposed document would also build upon the research conducted by the National Highway Cooperative Research Program and the Transit Cooperative Research Program of the TRB, as well as research by FHWA and others. Since security is an evolving field, and to ensure that users needs are considered, technical working groups would be formed to provide input into the document during its development.

An option we recommend for consideration is to develop a pair of training classes, one for executives and one at a technical level, which would present the material in the guidance document. In addition, the technical level training class would provide some scenario-based case studies and/or tabletop exercises to provide an interactive learning environment. The material presented in both the document and the classes will provide
state DOT employees with a foundation that will allow them to incorporate security into
facility design.

9. **Deploy a searchable database of training and other resources.**

Establishing this database will respond to a strongly-voiced need of states, who need a
reliable, central source of information on where to find training. It will also quickly
establish a presence for this PCB initiative. The database should be hosted on a website
that will become the central site for the initiative.

Volpe has compiled a preliminary database. The TRB’s Transportation Education and
Technology Transfer Committee has also compiled research on this subject. AASHTO
has established a platform that could host the database. Additional work would include
updating information on existing database entries, adding new entries to better represent
state-level offerings, refining the database structure to make it more “user-friendly”,
programming the database for use on a website.

**Concluding notes regarding implementation**

In the table on the following page, we summarize the 9 actions proposed for the first year. We
also show a recommended timeframe for completing implementation of each action. This is
based on an assumed start date of February 1, 2006.

Note that while the actions are presented in numeric sequence, this plan assumes that
implementation will proceed simultaneously on multiple actions. How this would be
accomplished should be addressed by the steering committee. Regardless, the list of first-year
actions is ambitious.

This strategic plan is designed to address the needs of those institutions that are most
immediately involved in transportation system security and emergency response—state
departments of transportation. However, an important implication of the foregoing research and
recommendations is that the success of this effort will depend on the Federal Highway
Administration. In particular, the technical expertise resident both at headquarters and in the
division offices will be essential. One of the steering committee’s first activities should be to
assess the current capacity of the FHWA to play this critical role in implementation of these
recommendations. Depending on the outcome of that assessment, some of the recommendations
may need to be implemented first with FHWA management and staff as participants. This would
amount to a “train the trainer” phase of effort.
<table>
<thead>
<tr>
<th>ACTION</th>
<th>WHEN TO COMPLETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify partners for overall support and establish a resource plan.</td>
<td>February-March, 2006</td>
</tr>
<tr>
<td>2. Establish a steering committee and technical working groups.</td>
<td>March-April, 2006</td>
</tr>
<tr>
<td>3. To address the topic of coordination among state DOTs and others for effective emergency response, organize and support a series of regional workshops.</td>
<td>August-December, 2006</td>
</tr>
<tr>
<td>4. To address the topic of elevating transportation's role in security/emergency response, support development of a seminar designed for executive-level staff.</td>
<td>September 2006</td>
</tr>
</tbody>
</table>
| 5. To address the topic of implementing a security/emergency response program, develop effective practices case studies and conduct a series of webinars to review the studies. | Case studies – July, 2006  
Webinars – Oct – Nov 2006 |
| 6. To address the topic of operational methods to secure facilities, support a series of peer exchanges, each involving 3-4 state DOTs. | November, 2006 – February, 2007 |
| 7. Support a technical advisory team to provide on-request assistance in identifying critical assets and assessing their vulnerability, and pilot this approach with one state DOT. | Pilot in June, 2006            |
| 8. To address the topic of design methods for facilities security, research and publish information on methods and procedures. | December, 2006                 |