Supplemental Information for NRMR MPOs

Integrating Security into Small MPO Planning Activities

John MacGowan
Mark Lofgren
Kimberly Vachal

Rural Transportation Safety and Security Center
Upper Great Plains Transportation Institute
North Dakota State University

August 2008

The contents presented in this report are the sole responsibility of the Upper Great Plains Transportation Institute and the authors.

ABSTRACT

The Rural Transportation Safety and Security Center vision is to promote and enhance the region's transportation safety and security through research, education, and outreach in a partnership with stakeholders. It is a collaborative effort between Upper Great Plains Transportation Institute and the North Dakota Department of Transportation, with funding from the Federal Highway Administration.

Transportation safety and security are critical issues for personal and freight mobility. Security issues are prominent given the large the border area, high-volume commercial traffic corridors, and limited security resources. Our initial challenge with security is to understand the risks and issues that are priorities in rural areas. The Rural Transportation Safety and Security Center will work with stakeholders to conduct research, education, and outreach that will enhance quality of life through safer and more secure rural transportation. This paper is an example of how the Center is fulfilling that goal.

The Cooperative Research Program under the auspices of the American Association of State Highway and Transportation Officials has released a report, NCHRP Report 525, Volume 3 "Incorporating Security into the Transportation Planning Process." The research conducted for this authoritative treatment of the subject was completed in 2004. Since that time, a number of new programs, most notably in the federal government arena have been completed. It is the purpose of this paper is to supplement the information in the NCHRP report with relevant updated information. The information presented should provide a context in which the reader can continue to learn more in the specific areas of interest.

This paper describes the initiatives of the U.S. Department of Homeland Security (DHS) at a fairly high level so that members of Metropolitan Planning Organizations (MPO) can gain an overview understanding of the direction that agency is taking. Similarly, the highway security programs of the U.S Department of Transportation, in conjunction with the DHS, are described. The paper then describes other programs on behalf of other agencies within the federal government, states, and urban areas that have been undertaken.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Just about everything we do depends on transportation. When there is a disruption to transportation flows, whether it is manmade or natural, there are consequences that range from inconvenience to economic loss and even life and death.

During these disruptions, first responders in state and local agencies are on the front line. It is the responsibility of federal officials to work closely with these entities to ensure regional preparedness in coordinating recovery efforts and restoring public confidence. These agencies also work closely with the owners or operators of the nation's transportation infrastructure.[35]

The principle responsibility for transportation security in the United States falls to the U. S. Department of Homeland Security (DHS). The goal of this paper is to develop context for local and regional transportation agencies' need in developing and implementing transportation initiatives based on security. Thus, it is essential to review major DHS security programs and programs shared with the U.S. Department of Transportation.

In addition, activities of key national stakeholder organizations will be explored including the transportation sector's work with the American Association of State Highway and Transportation Officials (AASHTO) and their Special Committee on Transportation Security (SCOTS). In addition, AASHTO provides for security research through the Transportation Research Board (TRB) Cooperative Research Program.

Results of the security research conducted through the Cooperative Research Program have yielded many useful products. Recognizing these efforts, readers should also consult NCHRP Report 525, Volume 3 "Incorporating Security into the Transportation Planning Process." [3] This paper is a supplement to this 2004 publication. For the remainder of this paper, the NCHRP Report 525, Volume 3 will be referred to as "the report." The report was prepared under the direction of a panel of experts and is considered as an authoritative treatment of the subject of integrating security into the planning process.

2. U.S. DEPARTMENT OF HOMELAND SECURITY DIRECTION

The U.S. Department of Homeland Security was created 14 months after September 11, 2001. Just one year later there were three complementary Homeland Security Presidential Directives (HSPD) issued that bear directly on security planning, and together, form the overarching authority for the scheme being developed by DHS. Before introducing the scheme, it is important to understand two precepts of the resulting framework. The first is that it is aimed at national, domestic all-hazard threats and incidents. The second is that it is sized to providing prevention, protection, response, and recovery at the incidents of national significance.

The first directive of interest is HSPD-8, The National Preparedness Goal (the Goal), which is to guide federal departments and agencies, state, territorial, local and tribal officials, the private sector, non-government organizations, and the public in determining how to most effectively and efficiently strengthen preparedness for terrorist attacks, major disasters, and other emergencies. The Interim National Preparedness Goal was released on March 31, 2005.[11] It "establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, state, and local entities."[9] The Goal will guide federal departments and agencies, state, territorial, local and tribal officials, the private sector, non-government organizations and the public in determining how to most effectively and efficiently strengthen preparedness for terrorist attacks, major disasters, and other emergencies. As a result, the public and private sectors will be able to respond to[8]

1. How prepared do we need to be?
2. How prepared are we?
3. How do we prioritize efforts to close the gap?

The second directive of interest is HSPD-5. It is "to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system."[7] It identifies steps for improved coordination in response to incidents. As a result of this, the DHS is coordinating with other federal departments and agencies and state, local, and tribal governments to establish a National Response Plan (NRP) and a major component of that plan, the National Incident Management System (NIMS).[8]

The third directive, HSPD-7, came about in 2003 and established a federal policy for identification and protection of the nation's critical infrastructure and key resources (CI/KR). In response to this, the DHS developed the National Infrastructure Protection Plan (NIPP). The aim of this plan is embraced by and results in a corollary program to the NRP. It is to "Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency." [13]

With the three executive authorities in place, the policy for a major national initiative in treatment of threats from terrorists and all other significant hazards was established. HSPD-8 established the National Preparedness Goal, which is the rallying point for federal, state, local, territorial and tribal governments to come together to agree in concept to the direction the national initiative will

take and to develop a program of mutual agreement under which each jurisdiction can prepare. From there, parallel policy tracks are established: one under HSPD-7 and the National Infrastructure Protection Program and one under HSPD-5 and the National Response Plan. Following this policy fabric, the next step is development of implementation plans and guidance that will cascade to each jurisdiction, public and private. The three program areas should not be taken piecemeal, but rather holistically for an interwoven system of plans, processes, and activities for our nation's defense from terrorism and other national hazards.

2.1 The National Preparedness Goal

The National Preparedness Goal, as it grows and solidifies includes readiness targets, priorities, preparedness standards, and an assessment system for the nation's capabilities. To help balance the potential threat of major events with the resources needed to prevent, respond to, and recover from them, the Goal gives rise to seven national priorities. The priorities fall into two categories: overarching priorities that contribute to development of multiple resources and specific priorities directed at specific target recourses. Achieving the priorities will allow DHS to accomplish its objectives.[17]

The overarching priorities are:

1. Implement the NRP and the NIMS
2. Expand regional collaboration
3. Implement the Interim National Infrastructure Protection

The resource-specific priorities are:

4. Strengthen information sharing and collaboration capabilities
5. Strengthen interoperable communications capabilities
6. Strengthen chemical, biological, radiological, nuclear, and explosive (CBRNE) detection, response and decontamination capabilities
7. Strengthen medical surge and mass prophylaxis capabilities

To aid in the achievement of these priorities, the DHS has decided to utilize a Capabilities-Based Planning approach. That is, planning, under uncertainty to develop capabilities suitable for a wide range of threats and hazards, within a framework of prioritization and choice. Capabilities-Based Planning addresses uncertainty by analyzing a wide range of possible scenarios to identify required capabilities. The Capabilities-Based Planning tools and products under development by the DHS are: [17]

- **National Planning Scenarios**: Planning documents that outline 15 types of terrorist attacks and natural disasters, providing the basis to define prevention, protection, response and recovery tasks, and the capabilities required to perform them.
- **Universal Task List**: A reference tool that provides a list of tasks to be performed by different disciplines at all levels of government to respond to major events.
- **Target Capabilities List**: A list and description of the capabilities needed to perform critical homeland security tasks found in the Universal Task List.

The National Planning Scenarios help to answer the preparedness goal question, "How prepared do we need to be?" They represent a minimum number of scenarios necessary to illustrate the range of potential incidents. They will be used to identify tasks that must be done to prevent, protect against, respond to, and recover from the scenario described incidents as well as the capabilities needed to perform the tasks.

The 15 National Planning Scenarios are shown in Table 2.1.

Table 2.1 National Planning Scenarios

1. (Nuclear) Improvised Nuclear Device	9. (Natural) Major Earthquake
2. (Biological) Aerosol Anthrax	10. (Natural) Major Hurricane
3. (Biological) Pandemic Influenza	11. (Radiological) Dispersal Device
4. (Biological) Plague	12. (Explosive) Improvised Explosive Device
5. (Chemical) Blister Agent	13. (Biological) Food Contamination
6. (Chemical) Toxic Industrial Chemical	14. (Biological) Foreign Animal Disease
7. (Chemical) Nerve Agent	15. Cyber Attack
8. (Chemical) Chlorine Tank Explosion	

Source: Department of Homeland Security[18]

The Universal Task List provides a menu of tasks from all sources that may be performed in major events such as those illustrated by the National Planning Scenarios. Identifying a menu of tasks is the first step toward identifying dependencies and critical tasks among disciplines, entities, and levels of government. Critical tasks are defined as those prevention, protection, response, and recovery tasks that require coordination among an appropriate combination of federal, state, local and tribal governments, private sector, and non-governmental entities during a major event in order to minimize the impact on lives, property, and the economy. Critical tasks, with associated conditions and performance standards, provide the foundation for developing target levels of capability. Also they will serve as the source for learning objectives used in the design, development, conduct, and evaluation of training and exercise events. [19]

At the heart of the preparedness Goal is the Target Capabilities List. It provides guidance on the specific capabilities and levels of capability that federal, state, local, and tribal entities are expected to develop and maintain. Every entity will not be expected to develop and maintain every capability to the same level. The specific capabilities and levels of capability will vary based upon the risk and needs of different types of entities; for example, basic capabilities and levels may be expected of individual jurisdictions, and more advanced capabilities and levels may be expected of groups of jurisdictions or states or the federal government. Currently there are 36 capabilities identified as listed in

Table 2.2 Target Capabilities List

2.2.

Table 2.2 Target Capabilities List

1. Animal Health Emergency Support	19. Isolation and Quarantine
2. CBRNE Detection	20. Mass Care (Sheltering, Feeding, and Related Services)
3. Citizen Preparedness and Participation	21. Mass Prophylaxis
4. Citizen Protection: Evacuation and/or In Place Protection	22. Medical Supplies Management and Distribution
5. Critical Infrastructure Protection	23. Medical Surge
6. Critical Resource Logistics and Distribution	24. On-Site Incident Management
7. Economic and Community Recovery	25. Planning
8. Emergency Operations Center Management	26. Public Health Epidemiological Investigation and Laboratory Testing
9. Emergency Public Information and Warning	27. Public Safety and Security Response
10. Environmental Health and Vector Control	28. Restoration of Lifelines
11. Explosive Device Response Operations	29. Risk Analysis
12. Fatality Management	30. Search and Rescue
13. Firefighting Operations/Support	31. Structural Damage Assessment and Mitigation
14. Food and Agriculture Safety and Defense	32. Terrorism Investigation and Intervention
15. Information Collection and Threat Recognition	33. Triage and Pre-Hospital Treatment
16. Information Sharing and Collaboration	34. Volunteer Management and Donations
17. Intelligence Fusion and Analysis	35. WMD/Hazardous Materials Response and Decontamination
18. Interoperable Communications	36. Worker Health and Safety

Source: Department of Homeland Security[19]

The Target Capabilities List assumes that local jurisdictions have an operational level of required capabilities to address steady state operations and smaller-scale emergencies and disasters. For example, the Target Capabilities List does not address capabilities for routine firefighting, law enforcement services, or seasonal flooding. The Target Capabilities List addresses unique capabilities and incremental resources related to terrorism, very large-scale disasters, or pandemic health emergencies. Establishing the plans, procedures, systems, interagency relationships, training and exercise programs, and mutual aid agreements required to build capabilities for incidents of national significance will enhance performance for all hazards response, regardless of incident size.[18]

Currently, DHS is proposing to array Target Capabilities into tiers. In the national priority, "Expand Regional Collaboration," the term "region" generally means a geographic area consisting of contiguous state, local, and tribal jurisdictions within a planning radius of a high threat urban area. Target levels of capabilities are better met through mutual aid agreements and assistance established under a regional approach because, although all jurisdictions are exposed to some level of risk of a major incident, it is not possible or even desirable to build and maintain full capacity for all capabilities in all communities. [18]

As a result, the assignment of capabilities to tiers provides a framework to determine who is responsible for building and maintaining a capability and what resources are required to perform the critical tasks to meet the performance standards. It also serves as a factor in making allocations of federal preparedness assistance for first responder preparedness.

The tiers structure is designed to provide a common framework and analytical basis for the assignment of target levels to capabilities and capabilities to levels of government. It is not a funding formula. The structure is based on three closely related components: 1) Geographic Groupings, 2) Performance Measures and Objectives, and 3) Capability Classes. [18]

Geographic Groupings. The geographic component of the tiers system assigns individual or groupings of jurisdictions (including cities, towns, and counties) into one of six tier levels based on three factors: 1) total population, 2) population density, and 3) critical infrastructure and other threat indicators. These are considered to be the leading factors of risk. While it is relatively easy to assign a jurisdiction to a grouping under population or density, the critical infrastructure and other threat indicators factor is not a direct input into the tier calculation, but is an additive factor assigned by the DHS to ensure proper accounting of the presence of CI/KR in the jurisdictions. [18]

To provide an example of this system, based on the Fargo-Moorhead MPO's 2006 estimated population (200,000), and its population density (approximately 71 persons per square mile, based on an area of 2,820.64 square miles), they would fall into tier level 5 in **Figure 2.1**.[18] This tier level could be adjusted up or down depending on the presence of significant national level of CI/KR.

Total Pop Grouping	**Points**		**Pop Density Grouping**	**Points**		**Total Points**	**Base Tier Level**
Group 1	100		Group 1	100		91-100	1
Group 2	80		Group 2	80		70-90	2
Group 3	60	**x .50 +**	Group 3	60	**x .50 =**	50-69	3
Group 4	40		Group 4	40		30-49	4
Group 5	20		Group 5	20		10-29	5
Group 6	0		Group 6	0		0-9	6

Figure 2.1 Tier Level Calculation

Knowing the tier a jurisdiction falls into allows entry into the capabilities tier summary tables.A segment of one is shown in **Figure 2.2**.[18] This table indicates the capabilities to target as well as the resources needed for a jurisdiction. The capability is also tied to a full capability description, the expected outcome for execution of the capability, activities performed with the capability, critical tasks to be performed, performance measures, capability elements, other related capabilities, and a listing of reference material.

Common Capabilities		Federal	State	Regional (Intrastate)	Tribal and Local (City/County) Tier						Private Sector	NGO	Citizens
Capability	Resource				1	2	3	4	5	6			
Planning	Planner		X		X	X	X						
	Planning Equipment/Computers		X		X	X	X						
Interoperable Communications	Interoperability Plan	X	X		X	X	X	X	X	X			
	Governance Agreements	X	X		X	X	X	X	X	X			
	Standard Operating Procedures	X	X		X	X	X	X	X	X			
	Technology - System of Systems	X	X		X	X	X	X	X	X			
	Interoperable Communications Technical Assistance Program (ICTAP)Teams	X											
	Continuity of Operations												

Figure 2.2 Capabilities Tier Summary Example

Performance Measures and Objectives. The performance measures and objectives for each capability define how quickly and how well the critical tasks need to be performed. Some performance objectives apply universally across all jurisdictions. Once jurisdictions have been assigned to geographic groupings, it is possible to review the Target Capabilities to identify the critical tasks that they would be responsible to perform and the performance measures and objectives that apply to their group. [18]

Capability Resource Classes. This component assigns resources required to perform the assigned critical tasks to a performance standard. Stakeholder working groups have identified both the resources (personnel, plans, organization and leadership, training, equipment and systems, and exercises) required to perform the critical tasks, as well as the national target levels required to prepare the Nation for incidents of national significance. The capability resources are assigned to the geographic groupings on the basis of risk. [18]

To summarize the DHS preparedness program developed as a result of the Goal, Figure 2.3 provides a better understanding of the relationship of the scenarios, tasks, and capabilities. [19]

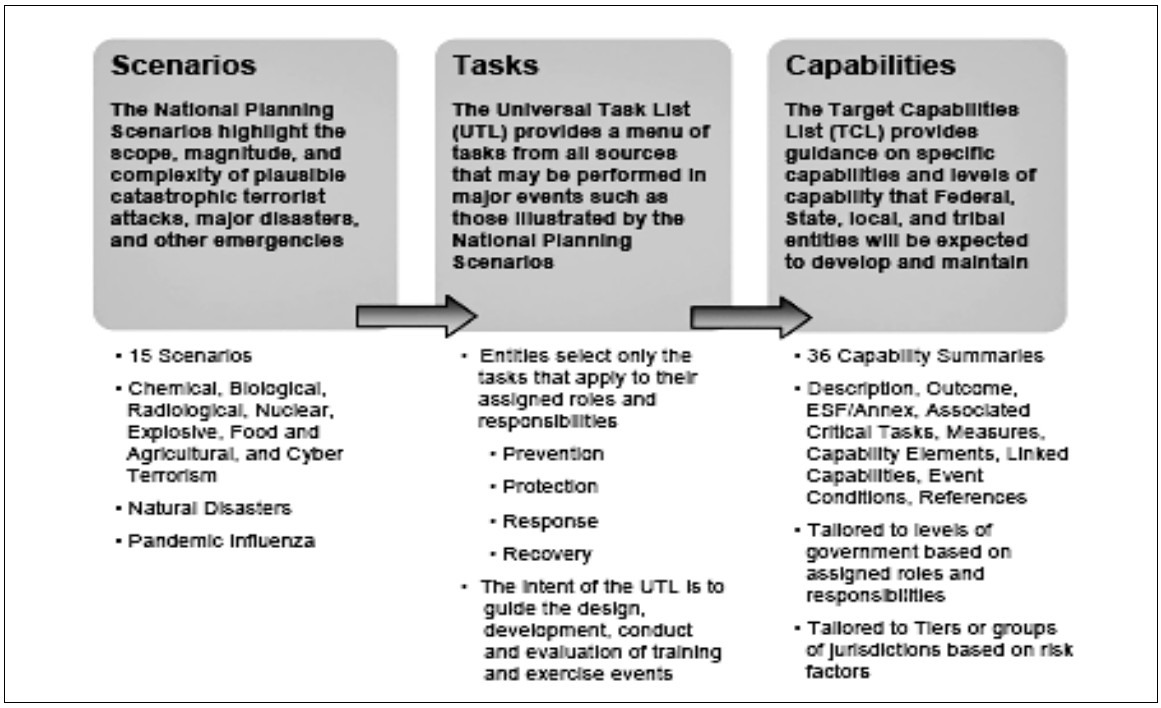

Figure 2.3 Relationships of the Principle Elements of the National Preparedness Goal

2.2 The National Response Plan

The National Response Plan (NRP) uses the National Incident Management System to coordinate and bring together the activities and emergency support from the federal, state, local and tribal government sector as well as non-governmental and private organizations to respond to security incidents. [8] The NRP incorporates best practices from a wide variety of incident management disciplines to include fire, rescue, emergency management, law enforcement, public works, and emergency medical services. The activation of the structures and protocols of the NRP for specific Incidents of National Significance provides mechanisms for the coordination and implementation of a wide variety of incident management and emergency assistance activities. Included in these activities is federal support to state, local, and tribal authorities; interaction with nongovernmental, private donor, and private-sector organizations; and the coordinated, direct exercise of federal authorities, when appropriate. [16]

The definition of Incidents of National Significance is based on four criteria: [16]

1. A federal agency requests the assistance of DHS.
2. State and local resources are overwhelmed and federal assistance has been requested.
3. More than one federal agency has become involved in responding to an incident.
4. The DHS has been directed to assume responsibility for managing a domestic incident by the President.

Key concepts of the NRP can be summarized as follows: [16]

- Systematic and coordinated incident management, including protocols for incident reporting, coordination, alert and notification, mobilization of federal resources, operating under differing threat levels, and integration of crisis and consequence management

- Deployment of federal resources for catastrophic events with state, local, and tribal governments and private entities when possible
- Organizing interagency attempts to minimize damage, restore areas to their previous conditions, and implementing programs to mitigate to future incidents
- Coordinating incident communication, worker safety and health, private-sector involvement, and other common activities associated with incidents
- Organizing relief and support organizations to facilitate the delivery of critical federal resources, assets, and assistance
- Providing mechanisms for coordination, communications, and information sharing in response to threats or incidents
- Facilitating federal support to other federal agencies
- Developing operations, tactical, and hazard-specific contingency plans and procedures
- Providing coordination of interagency and intergovernmental planning, training, exercising, assessment, coordination, and information exchange

The NRP itself comprises four sections:

- The Base Plan, including the concept of operations, structures for coordination, roles, responsibilities, definitions, etc.
- Appendices, the majority of which are a compendium of national interagency plans
- Support Annexes that address nine functional and administrative processes needed to implement the NRP such as financial management, private sector coordination (including National Critical Infrastructure representative – see below), tribal relations, and public affairs
- Emergency Support Functions (ESF) that deal with organizational and administrative functions of the federal agencies responsible for coordinating response and support to states, tribes and other federal agencies

As part of an ongoing process, the NRP is thoroughly reviewed for updating and refinement. Effective May 25, 2007, it is currently undergoing its fifth review cycle.

While the NRP describes in detail, the federal responsibilities and roles in the event of an Incident of National Significance, it explicitly recognizes the role of the State, local and tribal governments and non-governmental entities. It recognizes that police, fire, public health and medical, emergency management, public works, environmental response, and other personnel are often the first responders. However, it makes it clear that in the event of an Incident of National Significance it is the Secretary of Homeland Security, in coordination with other federal departments and agencies, who initiates actions to prevent, prepare for, respond to, and recover from the incident. These actions are taken in conjunction with state, local, tribal, nongovernmental, and private-sector entities. Moreover, in the event that State resources and capabilities are overwhelmed, governors may request federal assistance under a Presidential disaster or emergency declaration. This is why mutual aid agreements among jurisdictions and governmental and non-governmental agencies to expedite responses are so important.

The NRP goes to great lengths to lay out the response organizational structure and the roles and responsibilities of each element. Emergency Support Functions address 15 groupings of public and private sector capabilities that provide support, resources and services needed to respond to incidents and serve as the main operational mechanism for the federal-to-federal and federal to state, local, and tribal governments to provide assistance. ESF #1, for example, addresses the transportation sector organizational structure and response procedures. The U.S. Department of Transportation is designated as the ESF coordinator for the transportation group of capabilities.

As such, it is responsible for the prevention, mitigation, preparedness, recovery, infrastructure restoration, safety, and security of the nation's transportation system. Activities within ESF #1 include: coordinating requests for federal support; reporting damage to transportation infrastructure as a result of the incident; coordinating alternate transportation services; coordinating the restoration and recovery of the transportation infrastructure; performing activities conducted under the direct authority of DOT elements such as air, maritime, surface, rail, and pipelines; and coordinating and supporting prevention, preparedness, and mitigation among transportation infrastructure stakeholders at the state and local levels.[16]

2.3 The National Incident Management System

The National Incident Management System is the bulwark of the NRP's concept of operations and addresses the issue of "common language" among responders in the federal, state, tribal, and local sectors so that common processes, protocols and procedures may be used to coordinate and perform response actions. This will aid in developing a common focus for resources so that great efficiency and speed can be applied in the event of security incident occurrences, either terrorism or natural disaster. [8]

The NIMS is built on the template of the NRP and presents a core set of doctrine, concepts, principles, terminology, and organizational processes for incident management at all levels. It is not intended to be an operational incident management or resource allocation plan. Rather, it requires all federal agencies to adopt the NIMS and use it for their own respective incident management, emergency prevention and mitigation programs and to support actions taken to assist state, local, and tribal entities. Moreover, it is the intention of DHS to have the NIMS be adopted by state and local organizations as a condition for federal preparedness grants, contracts, or other activities.[14]

Most incidents are generally handled on a daily basis by a single local jurisdiction. However, there are occasionally instances when an incident warrants the involvement of several jurisdictions. Such was the case of the St. Valentines Day snow in central Pennsylvania. In this instance on February 13-14, 2007, an expected large winter storm engulfed the central portion of the state, leaving significant snowfall and ice in its wake. The result of this was closure of 150 miles of highways spread over three Interstates, leaving hundreds of drivers and passengers stranded in their vehicles, some for up to 20 hours! Three key state agencies, the state department of transportation (PennDOT), the State Police, and the state emergency management agency (PEMA) failed to adequately prepare, execute, communicate, and coordinate their response resulting in the National Guard and other local responders being called to assist drivers and passengers in need of food and warmth.[15]

In a recent report[33] prepared at the request of the governor and based on numerous interviews, it was found that PennDOT had local staffing issues, inconsistent weather reporting, lack of experience, equipment that had not been maintained, and inadequate public information systems. The State Police had no overall incident command, limiting their ability for a coordinated response over the entire area, relying only on individuals to manage individual incidents. PEMA did not have the agency liaisons they needed after all government operations were shut down in anticipation of the storm. Moreover, they did not implement existing procedures, including those required by NIMS, nor did they notify the governor of the seriousness of the situation until well into the event.

The report[33] made many recommendations aimed at improving the preparedness and response to emergency situations in the future. They recommended clarifying PEMA roles and responsibilities, aggressive adoption and implementation of NIMS, improved information flow, development of alternative routings plans, better maintenances and utilization of technology, better training and exercises, identification of statutes in need of change, and, in general, ensuring a higher priority on emergency preparedness throughout the state.

This is precisely what the NIMS seeks to avoid. The NIMS uses a systems approach to integrate the best processes and methods into a unified framework for incident management. It does this through a core set of concepts, principles, procedures, organizational processes, terminology, and standards requirements applicable to a broad community of NIMS users. The NIMS is constantly trying to achieve a balance of flexibility and standardization in doing this. The NIMS is comprised of six major components to anchor it in the systems approach:[14]

1. *Command and management.* Three organizational structures are used for this. They are the Incident Command System, the Multi-agency Coordination System, and the Public Information Systems.
2. *Preparedness.* Activities under this component include planning, training, exercises, personnel qualification and certification, equipment acquisition and certification, mutual-aid agreements, and publications management.
3. *Resources management*. Standards and requirements are developed to describe inventory, mobilize, dispatch, track, and recover resources for an incident.
4. *Communications and information management.* Elements of this component include incident management communications and information management.
5. *Supporting technologies.* Keeping abreast of improvements in technology in data communications, information management, and data display systems are important to improving incident management.
6. *Ongoing management and maintenance.* In this component, the continuous improvement and refinement of the strategic NIMS is accomplished.

2.4 The National Infrastructure Protection Plan

The NIPP defines the CI/KR protection component for achieving the DHS priorities. Implementing CI/KR protection requires coordination at all levels of government and the private sector. To do this, the NIPP provides the structure and content of each CI/KR sector's plan. This provides a baseline framework for the tailored development, implementation, and updating of 17 interdependent Sector-Specific Plans (SSP), one of which is the Transportation SSP.[13]

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program. Its framework will enable the prioritization of protection initiatives and investments across sectors to ensure the greatest benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing protective programs and initiatives. [13]

Protection includes actions to mitigate the overall risk to CI/KR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other

incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, and implementing cyber security measures, among various others. [13]

The cornerstone of the NIPP is its risk management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk. The risk management framework is structured to enhance CI/KR protection by focusing activities on efforts to: set security goals; identify assets, systems, networks, and functions; assess risk based on consequences, vulnerabilities and threats; establish priorities based on risk assessments; implement protective programs; and measure effectiveness.[13] Detailed application of the risk management framework is embedded in the Sector-Specific Plans (SSP).

The transportation SSP was recently published. Due to the vastness, openness, accessibility and interconnectedness of the U.S. transportation network, the transportation SSP further breaks down specifics into six modal groups: aviation, maritime, mass transit, highway infrastructure and motor carriers, freight rail, and pipeline. The highway transportation system is comprised of the infrastructure, the vehicles, the users, the maintenance equipment, facilities, and controls and communications.[35]

The transportation SSP has three goals and seven attendant objectives: [35]

Goal 1: Prevent and deter acts of terrorism using or against the transportation system.
- Implement flexible, layered, and effective security programs using risk management principles;
- Increase vigilance of travelers and transportation workers;
- Enhance information and intelligence sharing among highway transportation system sector partners.

Goal 2: Enhance resilience of the U.S. transportation system.
- Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability;
- Enhance the capacity for rapid and flexible response and recovery to all-hazards events.

Goal 3: Improve the cost effective use of resources for transportation security.
- Ensure robust sector participation in the development and implementation of public sector programs for the U.S. highway transportation sector;
- Ensure coordination and enhance risk-base prioritization of research, development, resting, and evaluation efforts.

To meet these goals and objectives, the overall transportation SSP begins with risk management where the general framework stops and extends it to a system-based risk management (SBRM) strategy. It is really a strategic framework for making risk-based security and resource allocation decisions and does not directly address operational or tactical plans.

The SBRM is an 8-step processes that defines three foci:
1. On what assets should the focus be placed?
2. How can the risk to those assets be better understood?
3. What countermeasures must be developed to manage the risk?

The 8-step process is illustrated in Figure 2.4.[35]

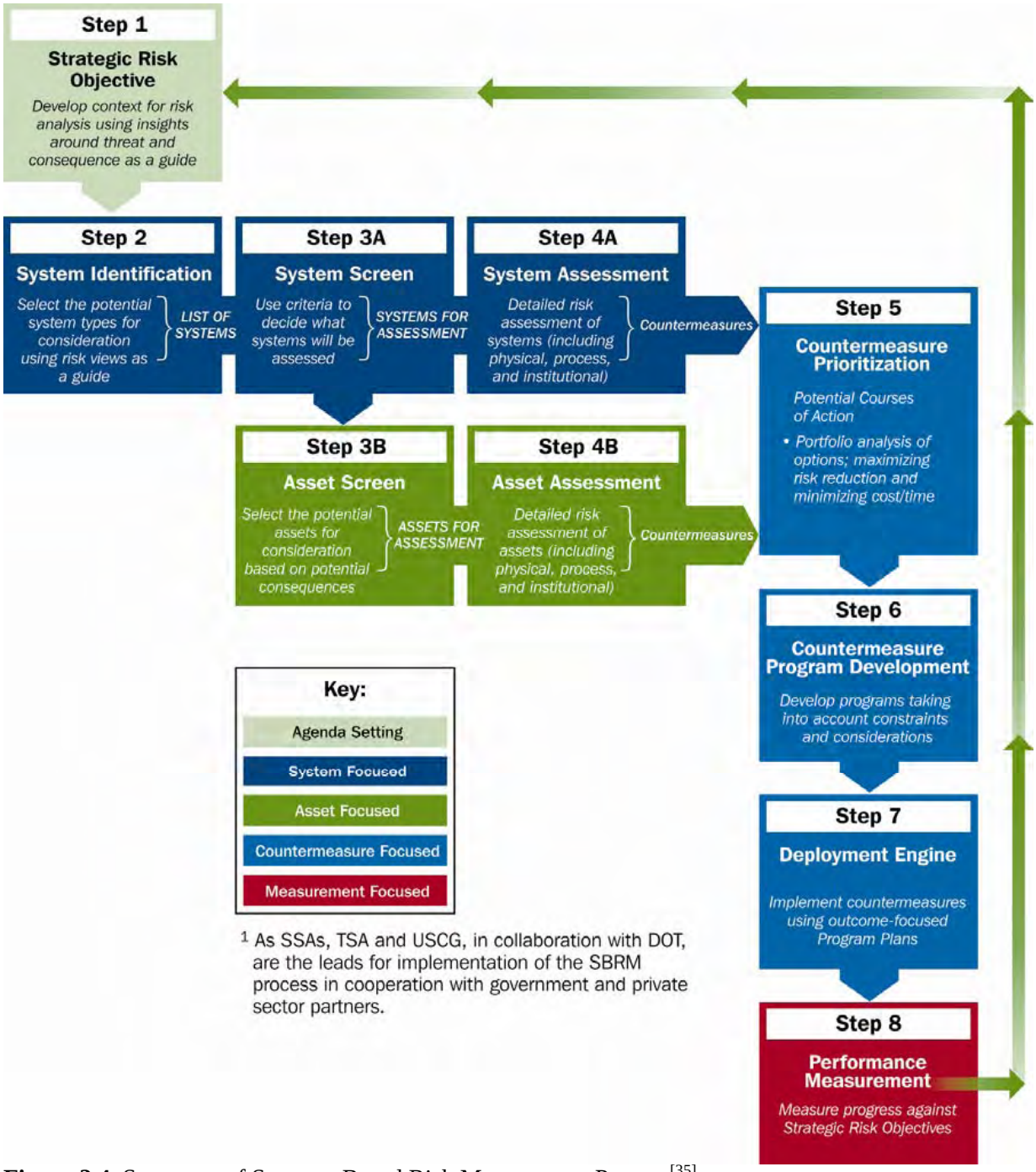

Figure 2.4 Summary of Systems-Based Risk Management Process[35]

As can be seen in Figure 2.4, the SBRM process begins with the identification of strategic risk objectives (SRO) that promote public and private industry leaders to focus on developing a set of asset- and system-based risk management options. The SROs are simply statements that establish specific, measurable, realistic, and attainable targets of required performance for the stakeholders of the system and critical infrastructure when specific risk consequences occur. Every SRO should be focused on a specific outcome and support security countermeasures that will improve the risk posture of the transportation system. [35]

The next step of the SBRM process is to identify the system impacted by each SRO. Because the transportation network is such a large, interdependent and interconnected network the concept of risk views is used. This allows a way of defining a more relevant, scalable, and manageable system. Four risk views are used:

Modal. This is the traditional differentiation of assets by transportation mode (i.e., aviation, maritime, mass transit, highway, freight rail, pipeline).

Geographic. All assets within a geographic boundary (e.g., New York State or the Fargo-Moorhead MPO). This view may be used most often by the sState, local, and tribal government partners.

Functional. The collection of all assets that satisfy a specific supply-chain need (e.g., supplying fuel to the Northeast).

Ownership. The collection of all assets under commonly recognized ownership (e.g., all assets owned and operated by the New York Mass Transit Authority can be evaluated as a system).

Moving forward with the formal development and analysis of a system model, the System Identification step allows a focus on systems that must be considered and those that do not have such a need for a given SRO. For example, an SRO for “improving the ability of the transportation system to withstand the impact of major flooding in the Red River Valley” would be more concerned with the system of interconnectedness of the several impacted modes and less concerned with geography. This step, System Identification, is crucial to subsequent analysis.

The next step, System Screening, is an opportunity to refine the system view to enhance analysis. The result is a model of a network that can be used to test and simulate scenarios that are dictated by the SRO.

The System Assessment step is when the identification and prioritization of risks to the infrastructure owners and operators occurs. This is when the SRO vulnerabilities countermeasures are identified and evaluated. This process is accomplished in three tasks:

1. Analyzing the system performance under candidate countermeasures;
2. Assessing candidate countermeasure effectiveness; and
3. Developing a list of effective countermeasures.

The System Screen and System Assessment steps are repeated for each system view for each SRO. The objective of this analytical process is to identify the most critical assets for a given SRO and to develop countermeasures to reduce the risk to those assets.

The Countermeasure Prioritization step involves developing a decision framework, typically working groups of experts, to examine how countermeasures can be packaged so that they are complementary and not counterproductive. Then the countermeasure packages are ranked by effectiveness in achieving the SRO.

The next step, the Countermeasure Program Development step, is to organize the packages of countermeasures into balanced and focused programs that can be refined for implementation and gain the buy-in from stakeholders and decision makers. The result is realistic and strategic countermeasure programs that address each SRO.

The last two steps, the Deployment Engine and the Performance Measurement steps, are to place the programs into reality through the planning and budgeting process. Then follow up with performance measures that track deployment progress and lend themselves to a continuous improvement process.

The NIPP defines the organizational structures that provide the framework for coordination of CI/KR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through private sector and government coordinating councils that are established for each sector. DHS also works with cross-sector entities established to promote coordination, communications, and best practices sharing across CI/KR sectors, jurisdictions, or specifically defined geographical areas.[13]

2.5 Summary of DHS Direction

The DHS, in response to Presidential directives 5, 7, and 8, is developing programs to provide further guidance to states and urban areas for understanding and aligning their prevention, protection, response, and recovery activities within the context of three major programs: the National Preparedness Goal, the National Response Plan and the National Infrastructure Protection Plan. This federal framework, while strategic at its core, risk as a function of threats, vulnerabilities, and consequences, should guide the states and urban areas in achieving their goals and objectives for securing the transportation system against all-hazard threats.

Figure 2.5 is presented to tie together many concepts presented above. [19] To aid in this, the influence of HSPD-8 is given as an example.

2.6 FY 2007 DHS Grant Program

The DHS grant program is both large and complex with many different programs, each of which has its own requirements. Table 3 presents an overview of the nature and scope of the grants and assistance available from the Department of Homeland Security and its agencies, the Federal Emergency Management Directorate (FEMA) and the Transportation Security Administration.

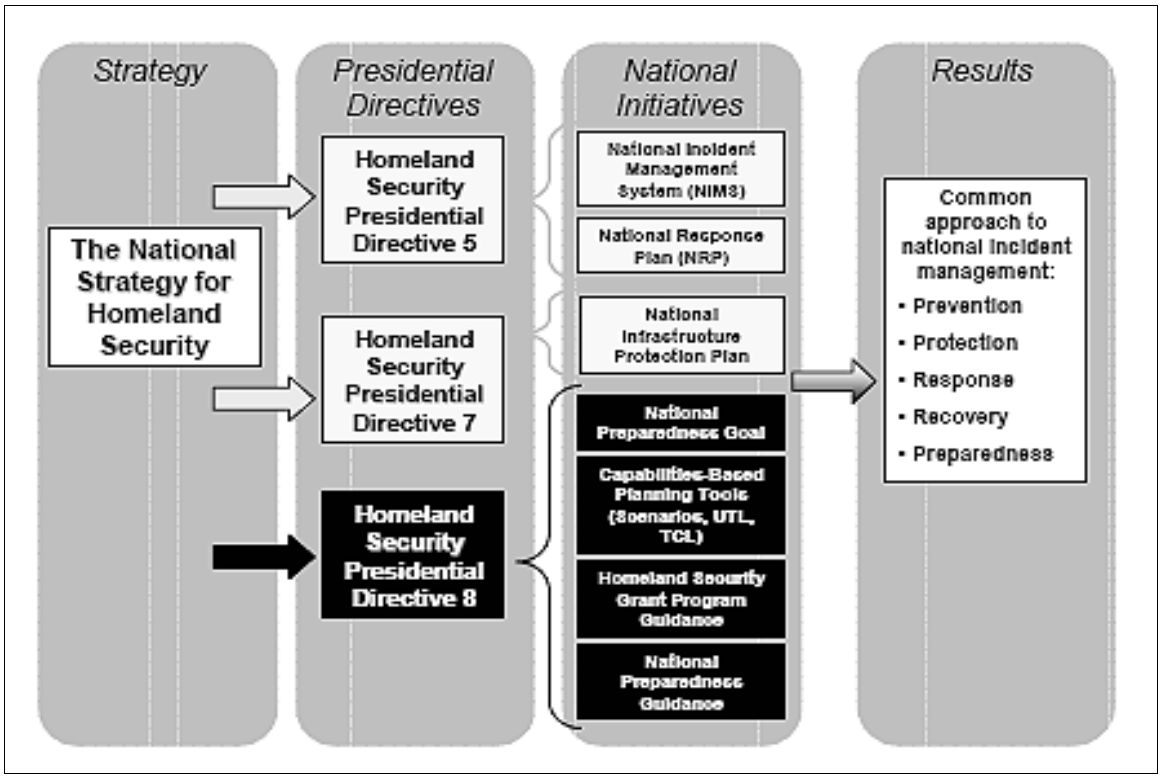

Figure 2.5 DHS Program in Context

At a minimum, DHS asks states and urban areas to ensure that their strategies are regularly reviewed and updated to address the four mission areas (prevent, protect, respond, recover) and reflect the seven National Priorities. It is important to note that it is not a requirement to provide an individual goal and objective for each mission area and priority; states and urban areas are asked to show, however, how their goals and objectives align with these priorities. DHS recognizes that each state and urban area has unique needs and capabilities and the strategies should reflect these attributes. Therefore, strategies should continue to include additional goals and objectives that reflect specific state and urban area priorities. [20]

The current State and Urban Area Homeland Security Strategies address 2004, 2005, and 2006, and are mostly terrorism focused. In updating their strategies, states and urban areas evolved their strategies to address not only terrorism, but a broad range of other threats and hazards, founded on a capabilities-based planning approach. Currently, states and urban areas are developing enterprise-wide homeland security strategies for 2007, 2008, and 2009 that reflect integration and collaboration to support the establishment of the National Preparedness System and realization of the National Goal. [20]

Table 2.3 Overview of the DHS Grants and Assistance Program for 2007[10]

Program	Eligibility	Description	Funding $ Millions	Application Date
DHS Grants & Training				
Homeland Security Preparedness Technical Assistance Program	Entities that can deliver services to SLTTs*	Address current areas of greatest concern in support of the National Preparedness Goal		7/09/07
• Enhance Grant Management Technical Assistance service			$0.3	
• Best Practice Support Technical Assistance service			$0.25	
• Critical Asset Assessment Technical Assistance service			$0.75	
Urban Areas Security Initiative (UASI) Nonprofit Security Grant Program	46 Designated Areas (None in ND; Twin Cites in MN)	Support for target hardening activities for 501(c)(3) nonprofit organizations deemed at high-risk of potential international terrorist attack	$24	6/22/07
Commercial Equipment Direct Assistance Program	First Responders	Support for equipment and training that will improve ability to respond to a major incident.	$33.7	5/29/07
Competitive Training Grant Program	SLTTs and others	To develop and deliver innovative training programs addressing high priority national homeland security training needs in one of the following five focus areas: • Public communications • Executive leadership of homeland security programs • Intergovernmental coordination and planning • Managing homeland security risks • Legal issues in preparation, response, and recovery	$29.1	5/4/07
Infrastructure Protection Program	State, local and private industry	For a range of preparedness activities, including strengthening infrastructure against explosive attacks, preparedness, planning, equipment purchase, training, exercises, and security management and administration costs.	$445.2	3/6/07
• Transit Security Grant Program	UASI areas	To support the work of public transit agencies that operate rail and bus networks.	$171.2	
o Ferry Security Supplement	19 Systems in 14 Regions	To support the work of public transit agencies that operate larger ferry networks.	$7.83 ($5.8 from the Transit Security Program and $2.03 million from the Port Security Program)	
• Port Security Grant Program	Owners/Operators of Federally regulated terminals and facilities	To enhance security at 136+ high threat ports in the country	$202.3	
• Intercity Bus Security Grant Program	Owners/Operators of fixed route intercity bus transportation	To create sustainable, risk-based efforts for the protection of critical port infrastructure	$11.6	

• Trucking Security Program	American Trucking Associations	For the Highway Watch program to continue as a sustainable national program to enhance security and overall preparedness on our nation's highways	$11.6	
• Buffer Zone Protection Program	UASI areas	To build security and risk-management capabilities at the state and local level to secure critical infrastructure including chemical facilities, nuclear and electric power plants, dams, stadiums, arenas and other high-risk areas	$48.5	
Homeland Security Grant Program	SLTTs and others	To prevent, respond to, and recover from a weapons of mass destruction (WMD) terrorism incident involving chemical, biological, radiological, nuclear, and explosive (CBRNE) devices and cyber attacks.	$1666.5	4/5/07
• Urban Areas Security Initiative	UASI areas	For unique planning, equipment, training and exercise needs of high-threat, high-density urban areas.	$ 746.9	
• State Homeland Security Program	States and Territories	To build capabilities at the State and local levels through planning, equipment, training, and exercise activities	$ 509.2	
• Law Enforcement Terrorism Prevention Program	Law enforcement and public safety communities	To support critical terrorism prevention activities, including establishing and enhancing fusion centers and collaborating with non-law enforcement partners, other government agencies and the private sector.	$ 363.8	
• Metropolitan Medical Response System Program	124 specific cities (does not include F-M)	To support local preparedness efforts to respond to all-hazards mass casualty incidents	$ 32.0	
• Citizen Corps Program	States and Territories	To bring community and government leaders together to coordinate community involvement in emergency preparedness, planning, mitigation, response and recovery	$ 14.6	
Emergency Management Performance Grant	States and Territories	To sustain and enhance state and local emergency management capabilities	$194	12/29/06
FEMA Grants and Assistance Programs				
Disaster-Specific Assistance Programs				
• Community Disaster Loan Program	Designated Disaster Localities	Provides funds to any eligible that has suffered a substantial loss of tax and other revenue	Variable	As Needed

• Fire Management Assistance Grant Program	SLTTs	Assistance for the mitigation, management, and control of fires on publicly or privately owned forests or grasslands, which threaten such destruction as would constitute a major disaster.	Variable	As Needed
• Hazard Mitigation Grant Program	SLTTs and others	To implement long-term hazard mitigation measures after a major disaster declaration.	Variable	As Needed
• Public Assistance Grant Program	Designated Disaster SLTTs and others	To alleviate suffering and hardship resulting from major disasters or emergencies	Variable	As Needed
• Reimbursement for Firefighting on Federal Property	Designated SLTTs and others	Provides reimbursement only for direct costs and losses over and above normal operating costs.	Variable	As Needed
Hazard Related Grants and Assistance Programs				
• Community Assistance Program, State Support Services Element	States	To provide technical assistance to communities in the National Flood Insurance Program (NFIP) and to evaluate community performance in implementing NFIP floodplain management activities	Variable	Varies Regionally
• Flood Mitigation Assistance Program	States and localities	To reduce or eliminate the long-term risk of flood damage to buildings, manufactured homes, and other structures insurable under the NFIP	$31	2/28/07
• National Dam Safety Program	States	For strengthening dam safety programs.	$3.2 +/-	11/30/06
• National Earthquake Hazards Reduction Program	States	To reduce the risks to life and property resulting from earthquakes	$0.9	Varies
• National Flood Insurance Program	States, localities and individuals	To purchase insurance as a protection against flood losses in exchange for State and community floodplain management regulations that reduce future flood damages.	Not Available	Varies
• Pre-Disaster Mitigation Program	SLTTs	For hazard mitigation planning and the implementation of mitigation projects prior to a disaster event	Not Available	Varies
• Repetitive Flood Claims Program	States and localities	To reduce or eliminate the long-term risk of flood damage to structures insured under the NFIP that have had one or more claims for flood damages, and that can not meet the requirements of the Flood Mitigation Assistance (FMA) program for either cost share or capacity to manage the activities.	$10	2/28/07

National Preparedness				
• Emergency Management Performance Grant	SLTTs	For the development, maintenance, and improvement of state and local emergency management capabilities.	$165.8	Varies
• Homeland Security Grant Program	See above	See above	See above	See above
• Infrastructure Protection Program	See above	See above	See above	See above
Non-Disaster Programs				
• Chemical Stockpile Emergency Preparedness Program	SLTTs	To protect the people of certain communities in the unlikely event of an accident involving this country's stockpiles of obsolete chemical munitions	Not Available	Varies
• Comprehensive Environmental Response, Compensation, and Liability Act	SLTTs and others	To improve capabilities associated with oil and hazardous materials emergency planning and exercising.	Not Available	Varies Regionally
• Cooperating Technical Partners	SLTTs	For technical assistance, training, and/or data to support flood hazard data development activities	$59	Varies
• Emergency Food and Shelter Program	Private-Nonprofit community and government organizations	Supplements the work of local social service organizations within the United States, both private and governmental, to help people in need of emergency assistance.	$153	Varies
• Map Modernization Management Support	SLTTs	To supplement, not supplant, ongoing flood hazard mapping management efforts by the local, regional, or State agencies.	$7.3	Varies
• Superfund Amendments and Reauthorization Act	First Responders	For training in emergency planning, preparedness, mitigation, response, and recovery capabilities associated with hazardous chemicals	Not Available	Varies
TSA Grants and Assistance Program				
Intercity Bus Security Grant Program	See above	See above	See above	See above
Transit Security Grant Program	See above	See above	See above	See above
Ferry Security Supplement	See above	See above	See above	See above
***SLTTs are State, Local, Tribal and Territories**				

3. U. S. FEDERAL HIGHWAY ADMINISTRATION DIRECTION

Since the Highway Act of 1962, the U.S. Federal Highway Administration (FHWA) has been directed by the U.S. Congress to establish "a continuing and comprehensive transportation planning process carried out cooperatively by state and local communities." Over the past several enacted reauthorization laws, as explained later in this report, the requirements for metropolitan planning organizations have become more specific. In its most recent surface transportation legislation Congress defined security considerations in the context of "increase the safety and security of the transportation system for motorized and non-motorized users."

The 2005 Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), Title VI – Transportation Planning and Project Delivery, Section 6001 (a) included this language to direct MPOs to specifically address security in their planning activities:

''(d) SCOPE OF PLANNING PROCESS.—
(1) IN GENERAL.—Each State shall carry out a statewide transportation planning process that provides for consideration and implementation of projects, strategies, and services that will—
(A) support the economic vitality of the United States, the States, nonmetropolitan areas, and metropolitan areas, especially by enabling global competitiveness, productivity, and efficiency;
(B) increase the safety of the transportation system for motorized and nonmotorized users;
(C) increase the security of the transportation system for motorized and nonmotorized users;
(D) increase the accessibility and mobility of people and freight;
(E) protect and enhance the environment, promote energy conservation, improve the quality of life, and promote consistency between transportation improvements and State and local planned growth and economic development patterns;
(F) enhance the integration and connectivity of the transportation system, across and between modes throughout the State, for people and freight;
(G) promote efficient system management and operation; and
(H) emphasize the preservation of the existing transportation system."

Subsequently, this reference to security was codified, verbatim in 23 CFR 450.306(a)(3).[4] *(emphasis added)*

Furthermore, 23 CFR 450.322 (h) provides additional language for the mandate:
The Metropolitan Transportation Plan should include ….. ***"(as appropriate) emergency relief and disaster preparedness plans and strategies and policies that support homeland security (as appropriate) and safeguard the personal security of all motorized and non-motorized users."***

In November 2006, U.S. Department of Transportation (USDOT) Inspector General noted that one of the 10 top management challenges facing the USDOT in 2007 is "Responding to National Disasters and Emergencies – Assisting Citizens and Facilitating Transportation Infrastructure Reconstruction." [5] The Inspector General pointed out that under the National Response Plan [see more on this under the U.S. Department of Homeland Security (DHS)], the USDOT has the lead role for coordinating transportation support in the event of natural or manmade disasters. Two key focus issues for mitigating the effects of future disasters by the USDOT are:

1. Clarify roles and responsibilities given expanded mission requirements;

2. Ensuring continued vigilance in protecting taxpayer funds spent for relief and recovery efforts.

This designation means that the USDOT, through its operating administrations (e.g. FHWA), is responsible for developing the capability for the movement of people and goods in times of disaster relief. To achieve this directive, the USDOT must work with other federal agencies as well as state and local governments to define missions, chains of command, and lines of communication and provide resources for that inter and intra agency coordination.

It is highly probable that when the new 23 CFR 450 is in place, guidance regarding security in planning will be forthcoming from FHWA. That guidance will most likely be a continuation of the groundwork they have already established in the areas of risk assessment, critical infrastructure protection, and safety planning. The USDOT focus in security planning fits well within the overarching national security vision being implemented by the DHS. An initial step in transportation-based security initiatives is an internal assessment of the acting agency. The self-assessment checklist came about as a result of some assumptions: [6]

1. DOTs and highway operators have limited experience with intentional disruptions to their systems;
2. DOTs and highway operators have limited resources to develop and maintain the necessary added responsibilities of protecting themselves from intentional disruptions;
3. DOTs and highway operators may need to be dependent on other state or federal agencies to learn of threats to their systems.

The FHWA further believes that DOTs and highway operators, in order to form a security program, need to:[6]

1. Determine their risks;
2. Develop inter- and intra-agency relationships;
3. Define roles and responsibilities needed to cope with intentional disruptions;
4. Develop a strategic and tactical approach to security.

In order to do these things, the FHWA proposes that the essential elements of a security plan include:[6]

1. Establish management support for a viable security program;
2. Create a mechanism by which security measures can be planned, designed, and engineered into new projects;
3. Establish a tactical and strategic approach to protecting and communicating sensitive information;
4. Develop a panoply of management and operations practices, relationships, training, and exercises that are needed to cope with intentional disruptions;
5. Enable the mobilization of appropriate response for continuity of operations; and
6. Implement appropriate pre-determined and pre-established alternatives and measures for post-event recovery.

While the FHWA works to institutionalize the security planning and disaster mobility, it remains cognizant of the larger framework that is being designed and implemented by the DHS. In fact, several products developed by the FHWA are key in the contributing to the overall risk-based security programs and countermeasures being coordinated for the transportation sector by the DHS and its Transportation Security Administration.[35]

Between May 2002 and June 2005, the FHWA sponsored 30 regional workshops on Transportation Operations Preparedness and Response across the United States. The purposes of these workshops were to increase awareness, enhance working relationships, identify areas for improvement, and provide information for guidance material at the national level. The result was a report [21] listing the best practices in seven categories:

- Interagency Coordination and Communication (15)
- Emergency Operations (31)
- Equipment (12)
- Intelligent Transportation Systems (9)
- Mutual Aid (9)
- Threat Notification, Awareness, and Information Sharing (25)
- Policy (8)

The numbers following each category indicates the number of best practices identified for all of the workshops. In addition to these best practices, the FHWA Emergency Transportation Operations program maintains a list of resources. [36]

In addition to these initiatives of the FHWA, the Federal Motor Carrier Safety Administration (FMCSA), as part of their regular compliance reviews of motor carriers, conducts educational security discussions with carriers of hazardous material that do not require a security plan and compliance reviews of plans for hazardous material carriers that are required to have a plan. In addition, they are conducting research in routing of hazardous material loads.[35]

4. OTHER U. S. GOVERNMENT ORGANIZATION DIRECTION

In another area of the federal government, the Department of Health and Human Services, working closely with the DHS, has developed a Cities Readiness Initiative (CRI). This is a program to aid cities in increasing their capacity to deliver medicines and medical supplies during a large-scale public health emergency, such as a bioterrorism attack, a nuclear accident, or disease outbreaks such as pandemic influenza.[22]

The Strategic National Stockpile (SNS) has large quantities of medicine and medical supplies to protect the American public if there is a public health emergency (terrorist attack, flu outbreak, and earthquake) severe enough to cause local supplies to run out. Once federal and local authorities agree that the SNS is needed, medicines will be delivered to any state in the United States within 12 hours. [23]

The Strategic National Stockpile has been expanded, and the states' cities have been planning for receipt, warehousing, and dispensing of medicines and medical supplies. The next logical step is to enhance preparation for a major public health emergency by creating unified plans that encompass all levels of government. This is the CRI. Clear and measurable goals are being determined by the cities and agencies involved. During the pilot test phase, gaps in planning were identified and closed.[22] The CRI focus for FY 2007 is to begin having at least one CRI in every state. For example, Fargo-Moorhead (North Dakota/Minnesota) is to be the location of the North Dakota CRI.[24]

The objectives of the CRI are four-fold:[24]

1. Create and sustain the capacity to provide antibiotics to the Metropolitan Statistical Area's entire population within 48 hours of the decision to do so.
2. Integrate command and control of state and local emergency operations systems to allow for effective communications.
3. Institute a public information system to direct, mobilize, and continually inform the public about mass antibiotic dispensing.
4. Ensure security measures to protect people, locations, and critical assets involved in the distribution and dispensing of antibiotics.

The CRI is designed to significantly improve the operational capability of 72 large metropolitan areas to receive, distribute and dispense SNS assets. Each designated city should be able, in the wake of a bioterrorism event for which antibiotics are an appropriate countermeasure, to provide such prophylaxis to the entire population within 48 hours of the time.[24]

5. THE AMERICAN ASSOCIATION OF STATE HIGHWAY AND TRANSPORTATION OFFICIALS DIRECTION

The transportation sector is working with the American Association of State Highway and Transportation Officials (AASHTO). AASHTO's Special Committee on Transportation Security (SCOTS) is responsible for advocating a secure transportation system by coordinating and collaborating with AASHTO members and other agencies and professional organizations. SCOTS membership includes three members (one voting member) from each member state. SCOTS has coordination interfaces with other AASHTO standing committees and subcommittees, such as the Standing Committees on Aviation, Highways, Public Transportation, Planning, Research, Rail Transportation, and Water, as well as subcommittees on Highways, Bridges and Structures, and Systems Operation and Management.

The role of the Transportation Research Board (TRB) in aiding federal agencies in providing information to state DOTs and MPOs to focus on consideration of security in transportation planning is well documented in the reports of the National Cooperative Highway Research Program (NCHRP) and the Transit Cooperative Research Program (TCRP). In fact, the report to which this paper is a supplement is a prime example. In addition to this, since September 11, 2001, 86 security-related projects have been authorized in the Cooperative Research Programs. Fifty-six of these projects have been completed; 20 projects are in progress; and 10 projects have contracts pending or are currently in development. To date, over $11 million of formally coordinated security-related research has been undertaken by the Cooperative Research Programs.[37]

Research undertaken by the NCHRP Project 20-59 panel and the TCRP Project J-10F panel is highly regarded. Table 4 identifies the reports published under their direction. [34] Volume 7, System Security Awareness for Transportation Employees must be ordered separately from the Transportation Research Board as it is in the form of a compact disk containing an interactive, multimedia training course.

Table 5.1 NCHRP Reports 525: Surface Transportation Security

Volume 1: Responding to Threats: A Field Personnel Manual (12/6/2004)
This volume includes a draft template that contains basic security awareness training in a workbook format that can be redesigned as a pamphlet, glove-box brochure, or other user-specific document. This NCHRP manual emphasizes noticing and reporting behavior that may be part of the planning stages of an event, and explains how an increased level of attention on the part of all employees can deter criminal and terrorist plans prior to implementation.

Volume 2: Information Sharing and Analysis Centers: Overview and Supporting Software Features (1/27/2005)
This volume examines how to organize and share security threat information across transportation organizations.

Volume 3: Incorporating Security into the Transportation Planning Process (5/24/2005)
This volume examines the status, constraints, opportunities, and strategies for incorporating security into transportation planning at the state and metropolitan levels. The report also examines security-

Table 5.1 NCHRP Reports 525: Surface Transportation Security

related projects in state and metropolitan priority programming decisions.

Table 5.1 (continued)

Volume 4: A Self-Study Course on Terrorism-Related Risk Management of Highway Infrastructure (6/10/2005)
This volume is designed to provide a general background in terrorism-related risk management for highway infrastructure. The report is also designed to assist bridge and structures engineers and managers in identifying critical highway assets and their potential vulnerabilities, developing possible countermeasures to prevent or ameliorate threats to such assets, and determining the capital and operating costs of such countermeasures. This volume of NCHRP Report 525 is presented in PowerPoint and portable document format (pdf) on CRP-CD-55.

Volume 5: Guidance for Transportation Agencies on Managing Sensitive Information (6/21/2005)
This volume provides basic information on identifying and controlling access to sensitive information.

Volume 6: Emergency Transportation Operations (9/8/2005)
This volume supports development of a formal program for the improved management of traffic incidents, natural disasters, security events, and other emergencies on the highway system. It outlines a coordinated, performance-oriented, all-hazard approach called "Emergency Transportation Operations" (ETO). The guide focuses on an enhanced role for state departments of transportation as participants with the public safety community in an interagency process. There is also available TRB's National Cooperative Highway Research Program (NCHRP) Web-Only Document 73: Emergency Transportation Operations: Resources Guide for NCHRP Report 525, Volume 6 is a resources guide on emergency transportation operations (ETO) containing bibliographical material that may be useful to readers of NCHRP Report 525, Volume 6.

Volume 7: System Security Awareness for Transportation Employees (6/13/2006)
This volume is a CD-based interactive multimedia training course designed to help transportation employees, supervisors, and managers define their roles and responsibilities in transportation system security, recognize suspicious activities and objects, observe and report relevant information, and minimize harm to themselves and others. Course modules focus on system security, reducing vulnerability, suspicious activity, suspicious objects, top priorities, and preparation.

Volume 8: Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies (11/18/2005)
This volume is designed to assist transportation agencies in evaluating and modifying existing operations plans, policies, and procedures, as called for in the National Incident Management System.

Volume 9: Guidelines for Transportation Emergency Training Exercises (5/1/2006)
This volume is designed to assist transportation agencies in developing drills and exercises in alignment with the National Incident Management System. The report describes the process of emergency exercise development, implementation, and evaluation. In addition, the available literature and materials to support transportation agencies such as state departments of transportation, traffic management centers, and public transportation systems are described.

Table 5.1 (continued)

Volume 10: A Guide to Transportation's Role in Public Health Disasters (5/26/2006)
This volume examines development of transportation response options to an extreme event involving chemical, biological, or radiological agents. The report contains technical information on chemical, biological, and radiological threats, including vulnerabilities of the transportation system to these agents and consequence-minimization actions that may be taken within the transportation system in response to events that involve these agents. The report also includes a spreadsheet tool, called the Tracking Emergency Response Effects on Transportation (TERET), that is designed to assist transportation managers with recognition of mass-care transportation needs and identification and mitigation of potential transportation-related criticalities in essential services during extreme events. The report includes a user's manual for TERET, as well as a PowerPoint slide introduction to chemical, biological, and radiological threat agents designed as an executive-level communications tool based on summary information from the report.

Volume 11: Disruption Impact Estimating Tool--Transportation (DIETT): A Tool for Prioritizing High-Value Transportation Choke Points (5/31/2006)
This volume includes information on DIETT as well as installation instructions and a user guide. DIETT is an electronic analytical tool that calculates direct transportation and economic impacts (costs) of an event that precludes the use of a TCP, and it prioritizes TCPs on the basis of these criteria. DIETT does not calculate replacement costs. Using DIETT's prioritized sets of outputs, along with other risk information, decision makers will be able to better focus their capital resource, security, and emergency-preparedness planning.

Volume 12: Making Transportation Tunnels Safe and Secure (2/1/2007)
This volume is designed to provide transportation tunnel owners and operators with guidelines for protecting their tunnels by minimizing the damage potential from extreme events such that, if damaged, they may be returned to full functionality in relatively short periods. The report examines safety and security guidelines for owners and operators of transportation tunnels to use in identifying principal vulnerabilities of tunnels to various hazards and threats. The report also explores potential physical countermeasures; potential operational countermeasures; and deployable, integrated systems for emergency-related command, control, communications, and information.

6. DIRECTIONS OF METROPOLITAN PLANNING ORGANIZATIONS

Institutional Challenges. In a paper[25] published prior to much of the DHS work described above, Dr. Michael D. Meyer makes a strong case for integrating and coordinating security/disaster planning activities within the MPOs. The paper points out that notwithstanding the widely varying and complex planning process framework of MPOs in the United States and because of the MPOs role as a forum for cooperative decision making in a metropolitan area, and its responsibility for allocating financial resources to improving the performance of the transportation system, the MPOs do have a role to play in security/disaster planning. The role of the MPO in security/disaster planning is largely dependent on its history, previous responsibilities, or influence on operations strategies.

Dr. Meyer outlines various potential roles for MPOs in security planning, and points out this will vary for each. MPOs can be a valuable asset in managing disaster, therefore, it is important to take a proactive approach by creating and implementing a strategic plan. Meyer concludes that the MPO "… has a critical role to play." as a medium for collaboration, as a financial resource for planning, and as a resource for transportation system analysis. [25]

7. SUMMARY

This paper is intended as a supplement to the NCHRP report[3] on incorporating security into the transportation planning process. The material present here is largely meant as updated material only made available since the publication of that excellent report. The overarching authority outlined in this report is based largely on all-hazard incidents of national significance. The degree to which this is scalable to the MPO is a function of the size of the Metropolitan Statistical Area, the density of population, and the degree to which infrastructure and processes in the area are at risk. Also, it is a function of the degree to which the MPO has experienced natural or manmade incidents.

REFERENCES

1. Parnell, Henry, *A Treatise on Roads*, Longman, Green, Orme, Brown, Green, and Longman, London, 1833.

2. Kuylash, Damian J., *Transportation and Society*, Transportation Planning Handbook, Institute of Trasnportation Engineers, Washington, DC, 1999.

3. Dornan, Daniel L. & Maier, M. Patricia, *Incorporating Security into the Transportation Planning Process*, NCHRP Report 525: Surface Transportation Security, Volume 3, NCHRP Project 20-59, Transportation Research Board, Washington, DC, 2005.

4. *Statewide Transportation Planning; Metropolitan Transportation Planning; Final Rule*, Federal Register, Volume 72, Number 30, Government Printing Office, Washington, DC, February 14, 2007.

5. Scovel, Calvin L., *DOT's FY 2007 Top Management Challenges, Report Number PT-2007-004*, Memorandum to the Secretary and Deputy Secretary, USDOT, Washington, DC, November 15, 2006.

6. Duffy, Kevin A., Science Applications International Corporation to Gerner, John, FHWA, *Attributes of an Effective State Highway Assets Security Program* – White Paper, McLean, VA, 2006.

7. *Homeland Security Presidential Directive 5*, Accessed on March 25, 2007, at http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html

8. *HSPD-8 in Context: the NRP, NIMS, and the Goal*, Fact Sheet, Department of Homeland Security, Washington, DC, 2004.

9. *Homeland Security Presidential Directive 8*, Accessed on March 25, 2007, at http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html

10. DHS Office of Grants and Training FY2007 Programs accessed on March 26, 2007, at http://www.ojp.usdoj.gov/odp/grants_programs.htm

11. *HSPD-8 Overview*, Accessed on March 26, 2007, at http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm

12. *Homeland Security Presidential Directive 7*, Accessed on March 26, 2007, at http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

13. *National Infrastructure Protection Plan*, Department of Homeland Security, Washington, DC, 2006.

14. *National Incident Managemnt System*, Department of Homeland Security, Washington, DC, 2004.

15. Rendell, Edward G., Press Release: *Rendell Team says Snow Storm Response Hampered by Problems in Preparation, Execution, and Communication*, Pennsylvania Governor's Office, February 21, 2007.

16. *National Response Plan*, Department of Homeland Security, Washington, DC, 2004.

17. *A Common Starting Point: The National Priorities*, Fact Sheet, Department of Homeland Security, Washington, DC, 2004.

18. *Target Capabilities List*, Draft Version 2.0, Department of Homeland Security, Washington, DC, September, 2006.

19. *Interim National Preparedness Goal*, Department of Homeland Security, Washington, DC, March 31, 2005.

20. *State and Urban Area Homeland Security Strategy*, Department of Homeland Security, Washington, DC, July 22, 2005.

21. Houston, Nancy (Booz Allen Hamilton), *Best Practices in Emergency Transportation Operations Preparedness and Response: Results of the FHWA Workshop Series*, Federal Highway Administration, Washington, DC, December 2006.

22. *Cities Readiness Initiative (CRI*), Accessed March 13, 2007 at http://www.bt.cdc.gov/cri/

23. *Strategic National Stockpile*, Accessed March 13, 2007 at http://www.bt.cdc.gov/stockpile/

24. *Cooperative Agreement Guidance for Public Health Emergency Preparedness: Program Announcement AA154 - 2006 (Budget Year 7)*, Accessed March 13, 2007 at http://www.bt.cdc.gov/planning/coopagreement/pdf/fy06announcement.pdf

25. Meyers, Michael D., *The Role of the Metropolitan Planning Organization (MPO) In Preparing for Security Incidents and Transportation System Response*, Georgia Institue of Technolog, 2004, Accessed on February 17, 2007, at http://www.planning.dot.gov/Documents/Securitypaper.htm

26. Lofgren, Mark and Vachal, Kimberly, *Integrating Security Into Small MPO Planning Activities: Case Study Analysis for NRMR MPOs*, Rural Transportation Safety and Security Center, Upper Great Plains Transportation Institute, 2008.

27. Cambridge Systematics, Inc., *Security and Emergency Preparedness in the Transportation Planning Process: Oregon Department of Transportation Case Study*, Federal Highway Administration, Washington, DC, September 30, 2004.

28. Cambridge Systematics, Inc., *Security and Emergency Preparedness in the Transportation Planning Process: San Diego Association of Government*, Federal Highway Administration, Washington, DC, September 30, 2004.

29. Kennedy, Rachel, *Public Safety and Homeland Security White Paper*, San Diego Association of Governments, San Diego, CA, July 21, 2006.

30. Cambridge Systematics, Inc., *Security and Emergency Preparedness in the Transportation Planning Process: OKI Regional Council of Government,* Federal Highway Administration, Washington, DC, September 30, 2004.

31. Cambridge Systematics, Inc., *Security and Emergency Preparedness in the Transportation Planning Process: The Houston-Galveston Area Council,* Federal Highway Administration, Washington, DC, September 30, 2004.

32. PBS&J and Battelle, *Houston Region ITS Strategic Plan,* Houston-Galveston Area Council, Houston, TX, May 2003.

33. James Lee Witt Associates, *Independent Report on the Mid-February 2007 Winter Storm Response for the Commonwealth of Pennsylvania,* Office of the governor of the Commonwealth of Pennsylvania, Harrisburg, PA, March 27, 2007.

34. Transportation Research Board, National Cooperative Highway Research Program Report 525 *Surface Transportation Security,* Volumes 1-6 and 8-12 may be found at: http://trb.org/news/search_news.asp?q_aw=NCHRP+Report+525&q_ep=Surface+Transportation+Security+&q_sw=&q_nw=&allsubjects=on&subjectradio=0&BlurbTypes=2&day=0&Lower_Date=&Upper_Date=&s=1&st=1&Submit1=Find+Blurbs

35. *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* Department of Homeland Security, Washington, DC, May 2007.

36. *Emergency Transportation Operations,* Resources from the Federal Highway Administration for each of the ETO components are available at: www.ops.fhwa.dot.gov/opssecurity

37. *Security Research Status Report,* Information on the Transportation Research Board Cooperative Research Program Security-Related Research is available at: onlinepubs.trb.org/onlinepubs/dva/CRP-SecurityResearch.pdf