FHWA/IN/JTRP-2007/19

Final Report

**SYNTHESIS OF BEST PRACTICES FOR
TRANSPORTATION SECURITY**

Volume II: Emergency Response

**Rodrigo Vargas
Jon D. Fricker**

January 2009

Final Report

FHWA/IN/JTRP-2007/19

SYNTHESIS OF BEST PRACTICES IN TRANSPORTATION SECURITY

Volume II: Emergency Response

by

Rodrigo Vargas
Graduate Research Assistant

and

Jon D. Fricker
Professor
School of Civil Engineering
Purdue University

Joint Transportation Research Program
Project No. C-36-67VVV
File No. 9-10-73
SPR-2872

Conducted in Cooperation with the
Indiana Department of Transportation
and the
U.S. Department of Transportation
Federal Highway Administration

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the Indiana Department of Transportation or the Federal Highway Administration at the time of publication. The report does not constitute a standard, specification, or regulation.

Purdue University
West Lafayette, IN 47906
January 2009

TABLE OF CONTENTS

	Page
List of Abbreviations.....	vi
Abstract.....	ix
CHAPTER 1 – INTRODUCTION.....	1
1.1 Background.....	1
1.2 Problem Statement.....	3
1.3 Research Objectives.....	6
1.4 Organization of the Report.....	6
CHAPTER 2 – FEDERAL HOMELAND SECURITY EMERGENCY MANAGEMENT	
MEASURES.....	8
2.1 Homeland Security Advisory System.....	8
2.2. National Incident Management System – NIMS.....	10
2.2.1 Command and Management.....	13
2.2.2 Preparedness.....	14
2.2.3 Resource Management	17
2.2.4 Communications and Information Management	22
2.2.5 Supporting Technologies.....	23
2.3 National Response Plan – NRP.....	23
2.3.1 NRP National Structure.....	30
CHAPTER 3 – EMERGENCY MANAGEMENT IN INDIANA.....	36
3.1 State Emergency Management Agency – SEMA.....	38
3.2 Indiana Comprehensive Emergency Management Plan – CEMP	42
3.3 Indiana Counter-Terrorism and Security Council – C-TASC.....	49

	Page
3.4 Indiana Department of Transportation – INDOT.....	51
3.4.1 Emergency Operations Plan.....	53
3.4.2 Lines of Authority and Communication.....	54
3.4.3 Standard Operating Procedures.....	55
3.4.4 Knowledge of Statewide Emergency Management.....	56
CHAPTER 4 – BEST PRACTICES IN EMERGENCY RESPONSE.....	58
4.1 Incident Command System – ICS.....	59
4.1.1 ICS Basic Structure.....	62
4.1.2 Incident Facilities.....	63
4.1.3 Command Function.....	64
4.1.4 Operations Section.....	67
4.1.5 Planning Section.....	70
4.1.6 Logistics Section.....	72
4.1.7 Finance/Administration Section.....	75
4.1.8 Area Command.....	76
4.1.9 ICS and DOTs.....	79
4.2 Communications.....	81
4.2.1 Interoperability.....	82
4.2.2 Information Assurance.....	84
4.2.3 Lines of Communication and Notification Procedures.....	85
4.3 Intelligent Transportation Systems – ITS.....	87
4.3.1 ITS and Emergency Response.....	89
4.3.2 Integration of TMC and EOC.....	92
4.4 Decision Support Systems.....	95

	Page
4.4.1 DSS in Emergency Response.....	100
4.4.1.a. DSS for Emergencies in Industrial Plants.....	100
4.4.1.b. DSS for Response to Hazardous Material Spills.....	104
4.4.2 DSS in State DOTs.....	107
CHAPTER 5 – GUIDELINES FOR THE DEVELOPMENT OF INDOT	
EMERGENCY OPERATIONS PLAN.....	110
5.1 Considerations for Development of an INDOT EOP.....	111
5.1.1 All-hazards approach.....	112
5.1.2 Follow Homeland Security Advisory System.....	112
5.1.3 Integration and Interoperability.....	113
5.1.4 Redundancy and Continuity of Operations.....	113
5.1.5 Personnel Safety.....	114
5.1.6 Compliance with Federal and State Requirements.....	115
5.2 Application of NIMS-ICS for INDOT in Emergency Response.....	117
5.2.1 ICS-type structure for INDOT Districts.....	118
5.2.2 Lines of Communication/Coordination.....	124
5.2.3 Area Command-type Structure for INDOT Central Office.....	127
5.2.4 Lines of Communication/Coordination with INDOT Central Office	
EOC Activated.....	130
5.3 INDOT EOP Structure.....	136
5.3.1 Basic Plan.....	137
5.3.2 Continuity of Operations Plan.....	137
5.3.3 Standard Operating Procedures.....	138
5.3.4 Hazard-specific Plans.....	139

	Page
5.3.5 Protective Measures for Different Levels of HSAS.....	140
CHAPTER 6 – CONCLUSIONS AND FUTURE RESEARCH.....	141
LIST OF REFERENCES.....	144
APPENDIX A – TASKS ASSIGNED TO INDOT BY THE CEMP.....	153
APPENDIX B – SURVEYS.....	161
APPENDIX C - TRANSPORTATION EMERGENCY RESPONSE CHECKLIST.....	169

LIST OF ABBREVIATIONS

9/11	Refers to the terrorist events of September 11, 2001
AASHTO	American Association of State Highway and Transportation Officials
AC	Area Command
AI	Artificial Intelligence
CEMP	Indiana Comprehensive Emergency Management Plan
CIMS	Crisis Information Management Software
COOP	Continuity of Operations
CORTAN	Central Ohio Regional Transportation and Emergency Management
C-TASC	Indiana Counter-Terrorism and Security Council
DHS	Department of Homeland Security
DIC	District Incident Commander
DMS	Dynamic Message Signs
DNR	Indiana Department of Natural Resources
DOJ	Department of Justice
DOT	Department of Transportation
DSS	Decision Support Systems
EMA	Emergency Management Agencies
EMAC	Emergency Management Advisory Council
ENS	Emergency Notification Systems
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
ER	Emergency Response
ES	Expert Systems
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency

FHWA	Federal Highway Administration
FTA	Federal Transit Administration
HPMS	Highway Performance Monitoring System
HS	Homeland Security
HSAS	Homeland Security Advisory System
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IDHS	Indiana Department of Homeland Security
IIMG	Interagency Incident Management Group
INDOT	Indiana Department of Transportation
INS	Incident of National Significance
ISP	Indiana State Police
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
JFO	Joint Field Office
MCC	Mobile Command Center
NGO	Non-governmental Organizations
NIMS	National Incident Management System
NRCC	National Response Coordination Center
NRP	National Response Plan
OSHA	Occupational Safety and Health Administration
RRCC	Regional Response Coordination Center
SEMA	Indiana State Emergency Management Agency

SOP	Standard Operating Procedures
TMC	Traffic Management Center
TRB	Transportation Research Board
TSA	Transportation Security Administration
WMD	Weapons of Mass Destruction

CHAPTER 1 – INTRODUCTION

1.1 Background

The terrorist events of 9/11 highlighted the need for transportation agencies to reconsider their level of preparedness to respond adequately to large-scale incidents. Up to that point, highway emergency response was considered as a local issue and concentrated mainly on natural disasters (AASHTO, 2002a). Departments of Transportation had different stages of preparedness, depending on the levels and types of risks considered, on a region by region basis. In this way, the level of preparedness for response to large scale incidents varied between State DOTs, and depended on the level of risk and the type of potential threats faced by each particular state (Ham, 2004). For the purpose of this research, “emergency response” will be considered as the short-term actions taken immediately after an incident (AASHTO, 2002a).

A basic premise to consider when approaching DOT emergency response is the fact that State DOTs are not lead emergency management players (AASHTO, 2002a). Emergency management is usually a coordinated effort among several Federal, state, local, and private organizations. Each agency is assigned specific functions to perform when responding to an incident. A State DOT is merely one such organization. The responsibilities assigned and the functions State DOTs are expected to perform are assigned in state emergency management plans, following the four components of emergency management: mitigation, preparedness, response, and recovery. However, the means to accomplish each one of these tasks rely on each State DOT's level of preparedness. In this way, prior to 9/11, many State DOTs had developed and implemented Emergency Operations Plans (EOPs) that established all provisions and procedures to follow internally within the state

DOT, as a way to ensure the functions assigned by state emergency management plans were performed efficiently and effectively.

Prior to 9/11, terrorism was considered as a type of emergency, and many state emergency management plans had annexes that addressed special requirements to be faced when responding to terrorist incidents. However, few State DOTs had addressed security or considered terrorism in their internal EOPs and procedures (Ham, 2004).

The events of 9/11 raised the level of awareness and highlighted the need to review and revise existing emergency management practices to include the possibility of large scale terrorist incidents, which may involve the use of Weapons of Mass Destruction (WMD), occurring within US territory. Pre-9/11 DOT emergency response provisions that may have proven to be appropriate for natural disasters may not be adequate within the new terrorist emergency management framework. Potential large-scale terrorist incidents may bring characteristics that may be quite different from that of conventional emergencies (AASHTO, 2002a).

TABLE 1.1 – Similarities and Differences Between Terrorist and Other Emergencies (AASHTO, 2002a)

Similarities	Differences
<ul style="list-style-type: none">• Mass casualties• Damage to infrastructure• With or without warning• Evacuation or displacement of citizens	<ul style="list-style-type: none">• Caused by people on purpose• Will always be treated as crime scenes• May not be immediately recognizable as terrorist incidents.• May not be single incidents• Place responders at higher risk due to WMD and possible planned secondary incidents• May result in widespread contamination of critical equipment and facilities• May have delayed or long-lasting effect• May expand geometrically in scope• May cause strong public reaction

Table 1.1 shows some of the similarities and differences between terrorist emergencies and other large-scale events that necessitate modifications to pre-9/11 emergency plans and procedures. As a result, the response practices in place by many state DOTs for natural disasters and other significant emergencies may require important changes when considering response to a terrorist attack. Table 1.2 presents some of the modifications in emergency response as outlined by AASHTO (2002a).

1.2 Problem Statement

The Indiana Department of Transportation (INDOT) is one of several Indiana agencies that are required to provide support to emergency response efforts for large-scale incidents as required by the Indiana Comprehensive Emergency Management Plan (CEMP). In addition, large-scale emergencies, including terrorist incidents, will always affect the transportation system in some way (AASHTO, 2002a; ITE and FHWA, 2004). Transportation systems can be the target of the attacks due to their importance to the economy. They can also be used as the weapon for perpetrating the attacks, as was the case in the attacks of 9/11. In addition, transportation systems are required to provide proper mobility in the case that evacuation is required, even if the transportation system itself has been affected. Finally, the transportation system is also the means for response personnel to quickly reach the incident site and handle the emergency. In conclusion, there is never a more important time for the transportation system to work at its fullest capability than in the event of an emergency (ITE and FHWA, 2004).

TABLE 1.2 – Characteristics of a Terrorist Incident and Possible Changes in Response (AASHTO, 2002a)

Possible Characteristics of Terrorist Incident	Possible Change in Response
Caused by people on purpose	Law enforcement and national security agencies will play a larger role in a terrorist incident. Coordination and understanding of respective agency roles will be critical. DOT personnel will need to understand the different relationships inherent during or after a terrorist incident.
Will always be treated as crime scenes	Law enforcement agencies will want to control and preserve certain elements of the crime scene, which may affect response by other agencies. DOT personnel need to understand how to effectively work with law enforcement agencies.
May not be immediately recognizable as terrorist incidents	If an incident occurs on or near a highway, DOT personnel may be first or early responders. Basic training in identifying signs and consequences for early recognition of terrorist incidents is needed to take appropriate safety precautions.
May not be single incidents	Consider the possibility of additional terrorist incidents as they respond to an earlier incident(s). DOT personnel need to be trained to consider risks of secondary terrorist incidents
Place responders at higher risk due to WMD and possible planned secondary incidents	Responders may be the actual target of secondary incidents.
May result in widespread contamination of critical equipment and facilities	Geographic areas may need to be quickly closed to all but designated emergency response personnel. Some resources may become unavailable for use if contaminated. If a highway or related facility becomes contaminated, some DOT personnel will need to know how to operate in that contaminated environment.
May have delayed or long-lasting effect	Response resources may be required far beyond those originally anticipated. DOT response resources need to be available but may also need to be protected as the consequences spread.
May expand geometrically in scope	Same as above.
May cause strong public reaction	A comprehensive public information strategy is necessary. Where highways are concerned, state DOT personnel will be expected to provide information, e.g., through variable message signs, to motorists evacuating the area.

INDOT's emergency operations are performed today based on having developed relationships with key individuals in other agencies (e.g., ISP, DNR, SEMA). Based on prior experience, INDOT personnel know what to do and whom to contact, depending on the type of event. Even though this practice may have proved to be effective for INDOT in dealing with common incidents (USDOT, 2003), the new terrorist framework in emergency management and the potential threat of incidents involving WMD pose a significant challenge and may require revising current procedures and developing new practices. For these types of events, agencies with no previous relationship may have to work closely with INDOT, and this new relationship might have to be formed in the wake of a catastrophe. Clearly, this is neither convenient nor desirable. Furthermore, normal contacts within INDOT, as well as those outside the agency, may not be available during an incident, and this has to be accounted for beforehand.

The new terrorist threat on the Nation creates the need for INDOT to review, revise, and update its emergency response capabilities to ensure they are adequate enough in this new operational environment. A wealth of information on transportation security has been produced by public and private organizations that address the new issues transportation agencies need to consider to review and update their emergency response procedures. In addition, Federal initiatives like the National Response Plan (NRP) and the National Incident Management System (NIMS) have to be considered by INDOT to ensure its response procedures are integrated within the larger national and state emergency management framework of operations.

1.3 Research Objectives

The current research focuses on developing a blueprint for INDOT as a guide of best practices for developing Highway Emergency Response Plans. The specific objectives of this research include:

- Summarize the growing literature on transportation security as it pertains to INDOT, to serve as reference for future INDOT transportation security and emergency response efforts, including the development of an INDOT EOP.
- Identify and review current best practices implemented across the country that will help INDOT in future security-related initiatives.
- Develop a set of guidelines to enhance INDOT's emergency response capabilities in the new terrorist framework of operations.
- Develop a set of guidelines for the development of a Highway Emergency Operations Plan for INDOT.

1.4 Organization of the Report

The following report consists of six chapters. Chapter 1 establishes the motivation of the research, the general background of the project, and presents the research objectives. Chapter 2 is a review of Federal homeland security measures undertaken to enhance emergency management in the US, including the Homeland Security Advisory System, the National Incident Management System, and the National Response Plan. Chapter 3 is an overview of emergency management in the State of Indiana, which will serve as a way for INDOT to understand its role in the State emergency management framework of operations. Included in this chapter is also a review of INDOT's current emergency response capabilities as observed in the development of this project. Presented in Chapter 4 is a review of what the research team identified as best practices in emergency response as applicable to INDOT.

Chapter 5 presents a set of guidelines for the development of an INDOT EOP, including some general considerations, the application of the Incident Command System to INDOT as an organizational system for emergency response, and a proposed structure of an EOP that will serve as a reference for the future development of an INDOT EOP. Finally, Chapter 6 presents a set of conclusions and outlines recommendations for future research.

CHAPTER 2 - FEDERAL HOMELAND SECURITY EMERGENCY MANAGEMENT MEASURES

The Homeland Security Act of 2002 established the Department of Homeland Security, with three basic objectives (DHS, 2004d): prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.

Several initiatives have been taken since then to protect America from future terrorist attacks. Homeland Security Presidential Directives 3 (Bush, 2003a) and 5 (Bush, 2003b) dictated some of the most ambitious measures that changed emergency management as established before 9/11. This chapter presents some of the most important initiatives of the Federal government, focusing on those that have affected and will affect the entire emergency management effort in the US.

2.1 Homeland Security Advisory System

The use of advisory systems to centralize and disseminate risk and threat level information has been a common practice of emergency management organizations for decades. Advisory systems not only serve as an efficient way to communicate different risk levels to and among departments and agencies, but are also an effective way to reach the general public.

The new terrorist threat after the attacks of 9/11 highlighted the need to establish a centralized mechanism to communicate homeland security threat levels to the Nation. With this in mind, Homeland Security Presidential Directive-3 (Bush, 2003a) established the Homeland Security Advisory System (HSAS) on March 2002. All Federal departments and agencies are required to adopt the HSAS as their primary threat advisory system. All other existing threat systems must conform to

the HSAS and should be modified accordingly to function under this new system (Bush, 2003a).

The HSAS consists of a series of five-color coded threat levels each corresponding to a specific level of risk, as shown in Figure 2.1. The higher the threat level, the higher the risk from terrorist attacks. Each of these levels has a set of Protective Measures to be adopted by all Federal departments and agencies. Figure 2.1 summarizes the threat level conditions and the set of Protective Measures determined in the HSAS.

Protective Measures established for a certain threat level must also include those of the lower threat levels. For example, Protective Measures for threat level yellow must include those for that threat level as well as those specified for blue and green. In addition, each individual department or agency must identify all additional protective measures it considers necessary to complement those established in the HSAS.

The declaration of each of the threat conditions is performed by the Attorney General in consultation with the Assistant to the President for Homeland Security and the Homeland Security Council Principals based on intelligence information, and can be made for the entire Nation or for a specific geographic area or industrial sector (Bush, 2003a). For example, in August 2004 the threat level was raised from yellow to orange for the financial sector in New York City, northern New Jersey, and Washington D.C., remaining yellow for the rest of the country.

Although the HSAS is directed towards Federal departments and agencies, Homeland Security Presidential Directive-3 encourages State and local entities to adopt the HSAS and implement their own specific Protective Measures as considered appropriate following the threat level established. This enhances interoperability and improves coordination among organizations involved in emergency management. An

Threat Condition	Description	Protective Measures
Severe Condition RED	Declared when there is a severe risk of terrorist attacks.	<ol style="list-style-type: none"> 1. Increasing or redirecting personnel to address critical emergency needs. 2. Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources. 3. Monitoring, redirecting, or constraining transportation systems. 4. Closing public and government facilities
High Condition ORANGE	Declared when there is a high risk of terrorist attacks	<ol style="list-style-type: none"> 1. Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations. 2. Taking additional precautions at public events and possibly considering alternative venues or even cancellation. 3. Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce 4. Restricting threatened facility access to essential personnel only.
Elevated Condition YELLOW	Declared when there is a significant risk of terrorist attacks	<ol style="list-style-type: none"> 1. Increasing surveillance of critical locations. 2. Coordinating emergency plans as appropriate with nearby jurisdictions. 3. Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures. 4. Implementing, as appropriate, contingency and emergency response plans.
Guarded Condition BLUE	Declared when there is a general risk of terrorist attacks.	<ol style="list-style-type: none"> 1. Checking communications with designated emergency response or command locations. 2. Reviewing and updating emergency response procedures. 3. Providing the public with any information that would strengthen its ability to act appropriately.
Low Condition Green	Declared when there is a low risk of terrorist attacks.	<ol style="list-style-type: none"> 1. Refining and exercising as appropriate preplanned Protective Measures. 2. Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures. 3. Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

Figure 2.1 – Homeland Security Advisory System

example of this is the Federal Transit Administration. The FTA has developed a National Transit Response Model (FTA, 2004), an applied version of the HSAS that is specifically directed towards the transit industry. The model is a guide with recommendations to transit companies on particular measures to adopt in each one of the threat levels of the HSAS.

2.2 National Incident Management System –NIMS

In an effort to standardize emergency management in the United States, Homeland Security Presidential Directive – 5 (HSPD-5) directed the Secretary of Homeland Security to develop a National Incident Management System (NIMS). This system was to incorporate a set of concepts, principles and guidelines to be implemented by all Federal, State, and local agencies involved in emergency management, based on best practices from diverse incident management disciplines across the country. The purpose of the NIMS was to provide a consistent nationwide approach for all entities involved to work effectively and efficiently together to prepare for, respond to, and recover from potential incidents (Bush, 2003b).

On March 1, 2004 the DHS released the National Incident Management System (NIMS). The purpose of the NIMS is to standardize emergency management practices across the US in order to assure interoperability and consistency between Federal, State, and local entities involved in emergency response. It was developed in collaboration with emergency management professionals and agencies from diverse fields, and incorporates some of the best practices and principles found in the country today.

Until the NIMS was released, there was no real national standard for emergency management that covered all departments and agencies with incident management responsibilities. The events of 9/11 highlighted the need for such standards, to ensure that all parties would use the same guiding principles when working together during a disaster. This would enhance the level of preparedness and response capability of emergency agencies across the US.

Homeland Security Presidential Directive – 5 (HSPD-5) requires all Federal departments and agencies to adopt the NIMS and to incorporate it in their internal incident management activities, as well as to assist State and local entities during a disaster. It also requests that all State and local agencies adopt the NIMS as a requirement for Federal preparedness assistance beginning in FY 2005. To assist this process of adopting NIMS principles to current emergency management capabilities, the NIMS Integration Center was created by the DHS. The NIMS Integration Center serves as the focal point of all information regarding this new set of standards, including the development of a national program for education and awareness.

The NIMS defines five basic components that compose the national framework for incident management. Each component includes principles and specific mechanisms that should be implemented by emergency organizations once the NIMS is fully implemented. These five components are:

1. Command and management
2. Preparedness
3. Resource management
4. Communications and information management
5. Supporting technologies

2.2.1 Command and Management

The Command and Management component is build upon three basic systems: Incident Command Systems, Multiagency Coordination Systems, and Public Information Systems. ICS and Multiagency Coordination Systems refer to different incident management levels that are activated according to the nature of the event. Public Information Systems, on the other hand, include all the principles, procedures, and processes needed to inform the public appropriately about a large scale incident.

The Incident Command System presented in the NIMS is based on the usual ICS concept used by emergency response professionals for incident management. A more detailed description of the ICS is presented in Section 4.1. The NIMS restates the ICS as the best practice for organizing emergency management at the incident and establishes it as the national standard structure for incident response. Adoption of the ICS by organizations with emergency responsibilities is also the initial requirement for NIMS compliance.

The Multiagency Coordination Systems on the other hand refer to those systems in which resources are integrated into a common organizational unit for overall emergency coordination. Multiagency Coordination Systems include Emergency Operations Centers (EOC) and Multiagency Coordination Entities. Emergency Operation Centers are defined by the NIMS as the physical locations at which coordination of information and resources take place during incident management operations. Multiagency Coordination Entities refer to those organizations established to provide overall guidance and policy coordination. These are especially appropriate in events that involve multiple agencies of multiple jurisdictions in which an overall coordination of activities is required.

2.2.2 Preparedness

The NIMS establishes the need for individual components with emergency involvement to acquire a certain level of preparedness as a way to secure proper incident management operations. All preparedness initiatives in the NIMS are directed towards ensuring integration and interoperability, as well as coordination among the different public and private organizations involved in an incident. These initiatives are grouped into two basic elements: preparedness organizations and preparedness programs.

Any type of group established to design, coordinate, and conduct preparedness activities is defined in the NIMS as a Preparedness Organization. These organizations, whether committees, planning groups, or any other kind of corporation, should meet regularly to establish priorities and coordinate preparedness efforts following the specific needs of the jurisdiction in question. Following NIMS, tasks assigned to Preparedness Organizations include the development and coordination of emergency plans, the integration and coordination of activities among the different parties for interoperability, and establishing priorities for resources that may be required, among others.

The NIMS also outlines a number of initiatives and principles required to ensure incident management preparedness. These initiatives, referred to as Preparedness Programs, include planning, training and exercises, personnel qualification and certification, equipment certification, and mutual-aid agreements. Preparedness programs should follow NIMS standards and protocols as appropriate to ensure proper interoperability when applied to incident response. For completeness of this document, it is important to briefly state the requirements and principles outlined for each one of these.

All planning efforts in emergency management rely on a number of plans as their core of operations. These plans allow emergency responders to establish a set of guidelines and conventions for operations, prior to the event ever happening. The NIMS states that all emergency plans should be focused on being able to set priorities, integrate all entities and functions involved by establishing relationships, and ensure that all communications systems are properly established (DHS, 2004b). It identifies five different types of plans to be developed by jurisdictions: Emergency Operations Plans (EOPs), procedures, preparedness plans, corrective action and mitigation plans, and recovery plans.

EOPs are plans that describe how a specific jurisdiction will respond to an incident, including its organizational structures for emergencies (FEMA, 2004). Procedures plans on the other hand must include all critical information in detail that is needed for emergency response within a jurisdiction, including mechanisms for specific tasks such as notification to appropriate staff, communications operating instructions, and mechanisms for reporting information, among others (DHS, 2004b). Preparedness plans describe all training needs and how these needs are identified, how resources can be obtained through mutual-aid agreements, and the identify the equipment required for the hazards the jurisdiction is most likely to confront (FEMA, 2004). Corrective Action and Mitigation plans are plans to implement procedures based on lessons learned from prior incidents or training and plans that describe all activities to be taken to reduce or eliminate any possible threat, respectively. Finally, recovery plans are those that describe all actions needed to enhance recovery from potential emergency scenarios.

Training and exercises constitute the second set of preparedness programs to be considered by emergency involved organizations. The NIMS states that all emergency personnel implicated in response to an incident must be properly trained

for all-hazards and must participate in realistic exercises to enhance their performance in real-life situations. Exercises allow responders to experience first-hand situations similar to what they may encounter in a real incident. This allows them not only to identify strengths and weaknesses in their response abilities, but is also an opportunity to establish relationships with personnel from other agencies and jurisdictions with whom they do not work regularly. To assist in the standardization of training and exercises for emergency personnel, the NIMS Integration Center should develop a national program for education and training (DHS, 2004b). This center acts as the focal point of all NIMS training requirements to maintain training standardization, and provides support for emergency exercises.

An important element included in the NIMS is the requirement for standardization and certification of personnel. This assures that all emergency response personnel have the minimum knowledge and skills to perform appropriately during an incident. Standards will include training, experience, credentialing, currency, and physical and medical fitness (FEMA, 2004). The NIMS Integration Center is responsible for the development, management, and publication of these standards.

Under NIMS, equipment utilized for emergency response is also required to be properly certified. This not only guarantees an appropriate level of performance of all equipment involved, but also allows for interoperability of the equipment across jurisdictions if the incident requires so.

Incidents that require the intervention of multiple jurisdictions or authorities may present difficulties when collaboration between them is needed and there are no previous arrangements between the parties. The NIMS establishes mutual-aid agreements as a way to avoid these complications and permits that required support between jurisdictions be handled in an effective way in the stages when it is more needed, that is, during the actual response to the incident. Jurisdictions should

identify those entities from which resources may be requested before hand, and establish agreements that enhance their collaboration efforts. These entities may include surrounding jurisdictions, neighboring states, and private organizations from which support may be required.

2.2.3 Resource Management

The third component of the national framework for emergency management deals with the appropriate coordination and management of resources employed for incident response. Resources should move quickly and in the most efficient manner when requested at the site. This, as observed from previous experiences, has been a significant issue for effective incident response (FEMA, 2004).

During an incident, resources for response may come from various sources, depending on the characteristics and specific requirements of the event. Organizations and entities that normally do not operate together may have to allocate and share resources in the most efficient way possible. To enhance this process, the NIMS establishes a set of standards and specific requirements for resource management to be adopted by emergency organizations across the US. These standards, managed by the NIMS Integration Center, will assure interoperability and integration as all entities involved work under the same guidelines.

The NIMS establishes five basic principles for effective resource management, upon which all standard procedures and mechanisms are based. Specific processes to comply with each of these principles are shown in Table 2.1 (DHS, 2004b; FEMA, 2004).

**TABLE 2.1 – NIMS basic principles for effective emergency management
(DHS, 2004b; FEMA, 2004)**

1. Advance Planning	Preparedness organizations work together prior to an incident to develop plans for managing and using resources.
2. Resource identification and ordering	Resource managers use standardized processes and methods to identify, order, mobilize, dispatch, and track resources.
3. Categorizing of resources	Resources are categorized by size, capacity, capability, skill, and other characteristics.
4. Use of agreements	Develop pre-incident agreements for providing or requesting resources.
5. Effective management of resources	Use validated practices to perform resource management tasks systematically and efficiently

The third basic principle deserves further comment, as it is one of the most important concepts outlined in the NIMS.

The basic idea behind the categorizing of resources is to standardize how resources from the various sources are classified in a simple and easily understandable way, to avoid confusion and assure seamless integration during the response efforts.

The process of categorizing resources is called “typing”, and it is performed through a detailed method established by the NIMS called the NIMS Resource Typing System. Based on this system, resources are to be classified using five simple elements that describe their characteristics: category, kind, components, metrics, and type. *Category* refers to the primary function for which a resource is considered most useful. Figure 2.2 shows all possible categories and their respective descriptions. *Kind* refers to a description of the broad class the resource belongs to, such as personnel, equipment, supplies, vehicles, and aircraft. *Components* refer to

Category	Purpose
Transportation	To assist Federal agencies, State and local governments, and voluntary organizations requiring transportation to perform incident management missions following a major disaster or emergency; to coordinate incident management operations and restoration of the transportation infrastructure
Communications	To provide communications support for Federal, State, local, and tribal incident management efforts
Public works and engineering	To assist those engaged in lifesaving, life-sustaining, damage mitigation, and recovery operations following a major disaster or emergency by providing technical advice, evaluation, and engineering services; by contracting for construction management and inspection and for the emergency repair of water and wastewater treatment facilities; supplying potable water and ice and emergency power; and arranging for needed real estate.
Firefighting	To detect and suppress urban, suburban, and rural fires.
Information and planning	To collect, analyze, process, and disseminate information about a potential or actual disaster or emergency to facilitate overall activities in providing assistance to support planning and decision-making.
Law enforcement and security	To provide law enforcement assistance during response and recovery operations; to assist with site security and investigation.
Mass care	To support efforts to meet the mass care needs of disaster victims including delivering such services as supplying victims with shelter, feeding, and emergency first aid; supplying bulk distribution of emergency relief supplies; and collecting information to and for a disaster welfare information system designed to report on victim status and assist in reuniting families.
Resource management	To provide operational assistance for incident management operations.
Health and medical	To provide assistance to supplement local resources in meeting public health and medical care needs following a disaster or emergency or during a potential developing medical situation.
Search and rescue	To provide specialized lifesaving assistance in the event of a disaster or emergency, including locating, extricating, and providing on-site medical treatment to victims trapped in collapsed structures.
Hazardous materials response	To support the response to an actual or potential discharge and/or release of hazardous materials.
Food and water	To identify, secure, and arrange for the transportation of safe food and water to affected areas during a disaster or emergency.
Energy	To help restore energy systems following a disaster or emergency.
Public information	To contribute to the well-being of the community following a disaster by disseminating accurate, consistent, timely, and easy-to-understand information; to gather and disseminate information about disaster response and recovery process.
Animals and agricultural issues	To coordinate activities responding to an agricultural disaster and/or when the health or care of animals is at issue.
Volunteers and donations	To support the management of unsolicited goods and unaffiliated volunteers, and to help establish a system for managing and controlling donated goods and services.

Figure 2.2- Categories used in resource typing system (DHS, 2004b)

the specific elements that comprise the resource. For example, an engine company may be classified as having different components like a pump, hose 1, hose 2, hose 3, a water tank, a ladder, and personnel (DHS, 2004b). *Metrics* refer to the measurement standard used to categorize the resource. The metric used should be convenient enough to describe the capability and/or capacity of the resource to incident management personnel. For example, an appropriate metric for a crane may be the maximum load it can operate. *Types* are used to categorize resources according to their capacity and capability from Type I to Type IV. A Type I resource has a larger capacity than a Type II, III or IV. This way, incident managers can quickly and effectively recognize the resources available for operations and request the best suited for the mission. Figure 2.3 shows an example of a fully typed resource extracted from the NIMS.

Resource: Urban Search & Rescue (US&R) Task Forces					
Category:		Search and Rescue		Kind:	Team
Minimum Capabilities:		Type I	Type II	Type III	Type IV
Component	Metric				
Personnel	Number of People per Response	70 person response	28 person response		
Personnel	Training	NFPA 1670 Technician Level in area of specialty. Support personnel at Operations Level.	NFPA 1670 Technician Level in area of specialty. Support personnel at Operations Level.		
Personnel	Areas of specialization	High angle rope rescue (including highline systems); confined space rescue (permit required); Advanced Life Support (ALS) intervention; communications; WMD/HM operations; defensive water rescue	Light frame construction and basic rope rescue operations; ALS intervention; HazMat conditions; communications; and trench and excavation rescue		
Personnel	Sustained Operations	24-hour S&R operations. Self-sufficient for first 72 hours.	12-hour S&R operations. Self-sufficient for first 72 hours.		
Personnel	Organization	Multi-disciplinary organization of Command, Search, Rescue, Medical, HazMat, Logistics, and Planning.	Multi-disciplinary organization of Command, Search, Rescue, Medical, HazMat, Logistics, and Planning.		
Equipment	Sustained Operations	Potential mission duration of up to 10 days.	Potential mission duration of up to 10 days.		
Equipment	Rescue Equipment	Pneumatic Powered Tools, Electric Powered Tools, Hydraulic Powered Tools, Hand Tools, Electrical, Heavy Rigging, Technical Rope, Safety	Pneumatic Powered Tools, Electric Powered Tools, Hydraulic Powered Tools, Hand Tools, Electrical, Heavy Rigging, Technical Rope, Safety		
Equipment	Medical Equipment	Antibiotics/ Antifungals, Patient Comfort Medication, Pain Medications, Sedatives/ Anesthetics/ Paralytics, Steroids, IV Fluids/ Volume, Immunizations/ Immune Globulin, Canine Treatment, Basic Airway, Intubation, Eye Care Supplies, IV Access/ Administration, Patient Assessment Care, Patient Immobilization/ Extrication, Patient/ PPE, Skeletal Care, Wound Care, Patient Monitoring	Antibiotics/ Antifungals, Patient Comfort Medication, Pain Medications, Sedatives/ Anesthetics/ Paralytics, Steroids, IV Fluids/ Volume, Immunizations/ Immune Globulin, Canine Treatment, Basic Airway, Intubation, Eye Care Supplies, IV Access/ Administration, Patient Assessment Care, Patient Immobilization/ Extrication, Patient/ PPE, Skeletal Care, Wound Care, Patient Monitoring		
Equipment	Technical Equipment	Structures Specialist Equip, Technical Information Specialist Equip, HazMat Specialist Equip, Technical Search Specialist Equip, Canine Search Specialist Equip	Structures Specialist Equip, Technical Information Specialist Equip, HazMat Specialist Equip, Technical Search Specialist Equip, Canine Search Specialist Equip		
Equipment	Communications Equipment	Portable Radios, Charging Units, Telecommunications, Repeaters, Accessories, Batteries, Power Sources, Small Tools, Computer	Portable Radios, Charging Units, Telecommunications, Repeaters, Accessories, Batteries, Power Sources, Small Tools, Computer		
Equipment	Logistics Equipment	Water/Fluids, Food, Shelter, Sanitation, Safety, Administrative Support, Personal Bag, Task Force Support, Cache Transportation/ Support, Base of Operations, Equipment Maintenance	Water/Fluids, Food, Shelter, Sanitation, Safety, Administrative Support, Personal Bag, Task Force Support, Cache Transportation/ Support, Base of Operations, Equipment Maintenance		
Comments		Federal asset. There are 28 FEMA US&R Task Forces, totally self-sufficient for the first 72 hours of a deployment, spread throughout the continental United States trained and equipped by FEMA to conduct physical search-and-rescue in collapsed buildings, provide emergency medical care to trapped victims, assess and control gas, electrical services and hazardous materials, and evaluate and stabilize damaged structures.			

Figure 2.3- Example of a fully typed resource (DHS, 2004b)

2.2.4 Communications and Information Management

During an incident, a vast amount of information is expected to flow among the different parties involved in the response effort, both within the incident response structure, and among the different agencies that need to coordinate activities and share information. One of the most important issues that emergency management agencies have to face when attending an emergency is the adequate and efficient flow of information. It is fundamental that the right information is distributed to the right personnel at the right time. With the new terrorist framework of operations, much effort and attention has been placed on the importance of considering the fact that some of the information shared may be reserved and should not be made available to people who do not need it.

Considering the above, the NIMS establishes the need for a set of standards for communications and information management systems to obtain a common operational picture among the different organizations with emergency management responsibilities (DHS, 2004b). Although little information is available at this time, these standards are to be developed by the NIMS Integration Center sometime in the future, and will consider standards for incident notification and status notification, information systems for sharing information among Federal, State, local, and private organizations, as well as standard specifications of communication systems and technology required to assure interoperability. A national authentication and certification system will also be established to prevent the information shared from falling in the wrong hands. Agencies at all levels will also become part of a National Database of Incident Reports, through the NIMS Integration Center, that will gather all incident reports to support incident management efforts.

2.2.5 Supporting Technologies

The NIMS identifies science and technology as an essential component to implement and adopt efficiently all of the principles and standards proposed. Therefore, it recognizes the need for on-going research and development of technologies and systems for support to emergency management operations under NIMS. Development of new technologies and standards under the NIMS should follow five principles as shown in Table 2.2.

Table 2.2 – Key principles for supporting technologies

Principle	Description
1. Interoperability and compatibility	Systems must be able to work together and should not interfere with one another.
2. Technology support	Enhances incident management and response.
3. Technology standards	Systems and technologies are based on requirements developed through appropriate preparedness organizations, following National standards if required.
4. Broad-based requirements	Needs for new technologies, procedures, protocols, and standards are identified at the field and national level. The NIMS provides a mechanism for prioritization.
5. Strategic planning and R&D	The NIMS Integration Center and the DHS will integrate all incident management science and technology needs of organizations under the NIMS into the National R&D agenda.

2.3. National Response Plan

Using the principles outlined in the NIMS, HSPD-5 directed the Secretary of Homeland Security to develop a National Response Plan (NRP). This plan was to integrate all existing Federal plans into one all-discipline, all-hazard plan, which

would enhance the role of all Federal departments and agencies with emergency management responsibilities (Bush, 2003b), by incorporating the principles established in the NIMS. The NRP, as indicated by HSPD-5, would also unify all Federal operational tasks into a national level policy, including Federal support to State and local incident managers.

The National Response Plan (NRP) was released January 6, 2005 in accordance to HSPD-5. The NRP constitutes a national initiative by the Department of Homeland Security to standardize and unify all Federal response actions to any Incident of National Significance. The NRP defines these incidents as “those high-impact events that require a coordinated and effective response by an appropriate combination of Federal, State, local, tribal, private sector, and nongovernmental entities in order to save lives, minimize damage, and provide the basis for long-term community recovery and mitigation activities”. The declaration of an Incident of National Significance is performed by the Secretary of Homeland Security on situations related to the following criteria (DHS, 2004c):

1. A Federal department or agency acting under its own authority has requested the assistance of the Secretary of HS.
2. The resources of State and local authorities are overwhelmed and Federal assistance has been requested by State and local authorities.
3. More than one Federal department or agency has become substantially involved in responding to an incident.
4. The Secretary of HS has been directed to assume responsibility for managing a domestic incident by the President.

The NRP is based on the NIMS framework. It uses the NIMS principles as a way to establish common training and communication procedures for all entities involved, and to establish a clear line of authority among the different parties involved, regardless of the type of incident (DHS, 2004c). By using NIMS, the NRP assures that the operational framework of Federal involvement in any Incident of National Significance is consistent with that used by State and local incident management organizations, hence improving coordination among the parties. As with any Incident Command framework, the NRP is scalable and can be partially or fully implemented depending on the severity and the present conditions.

Although the NRP is effective from the date of issuance, its implementation will undergo a three-phase process. Phase I (0 to 60 days) is intended for Federal departments and agencies to become familiar with the plan, and modify training and staffing necessary for final implementation. Phase II (60 to 120 days) will include any modifications needed to existing Federal interagency plans and conduct necessary training. Finally, Phase III (120 days to one year) is intended for the NRP to be fully implemented and operational by all Federal agencies and departments affected. After this implementation process, the NRP will override all other existing interagency plans such as the Initial National Response Plan, the Federal Response Plan, the U.S. Government Interagency Domestic Terrorism Concept of Operations Plan, and the Federal Radiological Emergency Response Plan (DHS, 2004c).

The NRP consists of several components that follow a similar structure to that of the earlier Federal Response Plan. A Base Plan section describes the overall structure and processes that constitute the NRP. A series of Appendices provide additional relevant information, such as a list of terms, definitions, and a review of other national interagency plans.

The NRP uses the same concept of Emergency Support Functions (ESF) established in the Federal Response Plan, extending the number of these from 12 to 15. The NRP contains an annex for each of these ESFs. Each Emergency Support Function delineates specific missions, policies, structures, and responsibilities of each Federal agency, grouping them into specific duties. Depending on the ESF in question, one or several Federal agencies are assigned as primary agencies according to their level of involvement and importance, with a set of support agencies assigned with support roles. In the case where there are multiple primary agencies, an ESF coordinator is assigned by the primary agencies, and the ESF will be managed under the concept of Unified Command. Figures 2.4a and 2.4b show the 15 ESFs established by the NRP and the corresponding level of involvement of each Federal agency assigned.

The following are the ESFs defined by the NRP (DHS, 2004c):

- ESF #1 – Transportation
- ESF #2 – Communications
- ESF #3 – Public Works and Engineering
- ESF #4 – Firefighting
- ESF #5 – Emergency Management
- ESF #6 – Mass Care, Housing, and Human Services
- ESF #7 – Resource Support
- ESF #8 – Public Health and Medical Services
- ESF #9 – Urban Search and Rescue
- ESF #10 – Oil and Hazardous Materials Response
- ESF #11 – Agriculture and Natural Resources
- ESF #12 – Energy
- ESF #13 – Public Safety and Security

Agency	Emergency Support Functions														
	#1 - Transportation	#2 - Communications	#3 - Public Works and Engineering	#4 - Firefighting	#5 - Emergency Management	#6 - Mass Care, Housing, and Human Services	#7 - Resource Support	#8 - Public Health and Medical Services	#9 - Urban Search and Rescue	#10 - Oil and Hazardous Materials Response	#11 - Agriculture and Natural Resources	#12 - Energy	#13 - Public Safety and Security	#14 - Long-term Community Recovery and Mitigation	#15 - External Affairs
USDA			S		S	S		S		S	C/P	S		P	S
USDA/FS	S	S	S	C/P	S	S	S	S	S	S			S		
DOC	S	S	S	S	S		S		S	S	S	S	S	P/S	S
DOD	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
DOD/USACE			C/P	S	S	S		S	S	S	S	S	S	S	
ED					S										S
DOE	S		S		S		S	S		S	S	C/P	S	S	S
HHS			S		S	S		C/P	S	S	S			P/S	S
DHS	S	S	S		S	S	S	S	S	S	S	S	C/P/S	S	C
DHS/EPR/FEMA		S	P	S	C/P	C/P			C/P	S				C/P	P
DHS/IAIP/NCS		C/P										S			
DHS/USCG	S		S	S				S	S	P			S		
HUD					S	S								P	S
DOI	S	S	S	S	S	S				S	P	S	S	S	S
DOJ	S				S	S		S	S	S	S		C/P/S		S
DOL			S		S	S	S	S	S	S	S	S		S	S

C = ESF coordinator

P = Primary agency

S = Support agency

FIGURE 2.4a – ESFs and agencies assigned (DHS, 2004c)

Agency	Emergency Support Functions														
	#1 - Transportation	#2 - Communications	#3 - Public Works and Engineering	#4 - Firefighting	#5 - Emergency Management	#6 - Mass Care, Housing, and Human Services	#7 - Resource Support	#8 - Public Health and Medical Services	#9 - Urban Search and Rescue	#10 - Oil and Hazardous Materials Response	#11 - Agriculture and Natural Resources	#12 - Energy	#13 - Public Safety and Security	#14 - Long-term Community Recovery and Mitigation	#15 - External Affairs
DOS	S				S			S		S	S	S			S
DOT	C/P		S		S	S	S	S	S	S	S	S		S	S
TREAS					S	S								P	S
VA			S		S	S	S	S					S		S
EPA			S	S	S			S		C/P	S	S	S	S	S
FCC		S			S										S
GSA	S	S	S		S	S	C/P	S		S	S				S
NASA					S		S		S				S		S
NRC			S		S					S		S			S
OPM					S		S								S
SBA					S	S								P	S
SSA						S							S		S
TVA			S		S							S		S	S
USAID								S	S						S
USPS	S				S	S		S			S		S		S
ARC			S		S	P		S			S			S	S

C = ESF coordinator

P = Primary agency

S = Support agency

FIGURE 2.4b – ESFs and agencies assigned (DHS, 2004c)

- ESF #14 – Long-Term and Community Recovery and Mitigation
- ESF #15 – External Affairs

For the purpose of this project, it is important to mention the responsibilities assigned to ESF#1 (Transportation) and ESF#3 (Public Works and Engineering) as they pertain to some of the tasks INDOT is expected to perform within the emergency management framework of Indiana.

The Transportation ESF has the US Department of Transportation as ESF coordinator and primary agency. Some of its primary objectives include reporting damage to transportation infrastructure resulting from an Incident of National Significance, coordinating alternate transportation services, coordinating recovery of the transportation infrastructure affected, and coordinating and supporting prevention/preparedness/mitigation among transportation infrastructure stakeholders at the State and local levels (DHS, 2004c).

On the other hand, ESF#3 – Public Works and Engineering has the Department of Defense/U.S. Army Corps of Engineers as ESF coordinator, in addition to the Department of Homeland Security/Emergency Preparedness and Response/Federal Emergency Management Agency as primary agencies. Its main objectives include providing public works and engineering-related support, including pre- and post-incident assessments of public works and infrastructure, and providing technical assistance for emergency repair of damaged infrastructure and critical facilities affected by an Incident of National Significance (DHS, 2004c), among others.

As mentioned above, it is important for INDOT to understand and be well informed of the responsibilities and tasks Federal agencies may have in the event of an Incident of National Significance, and how they may complement any initiative taken at the local level. The scope of activities included in these two ESFs overlap with some of the responsibilities outlined by Indiana's emergency management framework. The NRP works under the assumption that incidents are typically managed at the lowest possible geographic, organizational, and jurisdictional level (DHS, 2004c). As the incident's magnitude increases and local capabilities are overwhelmed, higher levels are requested to provide assistance. The degree of Federal involvement in local incident operations depends on the Federal authority over the affected area, the requests for assistance by State or local emergency management agencies, and the type, location, magnitude, and severity of the event.

Finally, the NRP contains a series of Incident Annexes with specific provisions and information required for particular types of incidents such as biological, catastrophic, cyber, food and agriculture, nuclear/radiological, oil and hazardous materials, and terrorism events.

2.3.1 NRP National Structure

The NRP establishes a national structure for incident management that integrates the role of the various Federal departments and agencies into the overall organization used at the State and local levels for large scale events. In this way, a clear progression of coordination and communication is established from the local level all the way up to the national level. It is designed in order for the Federal Government to be able to carry out its various roles during a large scale event. These include not only the allocation of Federal resources required for adequate

incident management, but also the direct implementation of eventual Federal-level strategies.

It is important for INDOT to have a general understanding of the duties assigned to each one of the components of the national structure stated in the NRP, considering that in an Incident of National Significance, it will become part of such national structure, specifically at the local and State level.

The NRP's national structure for incident management is shown Figure 2.5. According to its authority and localization, organizational elements are established at the field, regional, or national level. Within the overall national structure, two basic types of elements are defined: Command Structures and Coordination Structures. Command Structures refer to the on-site Incident Command structures established at the local level by the appropriate emergency response and management agencies. Coordination Structures on the other hand refer to those structures that are established for the purpose of organizing activities and the proper allocation of resources for adequate incident management. Two types of Coordination Structures are also classified in the NRP according to their objectives: EOCs/Multiagency Coordination Centers and Multiagency Coordination Entities.

EOCs/Multiagency Coordination Centers are those facilities established to provide central locations for information sharing and coordination of resource allocation to support on-scene operations (DHS, 2004c). From Figure 2.5 it can be seen that these include Local EOCs, State EOCs, the Joint Field Office (JFO), the Regional Response Coordination Center (RRCC), and the Homeland Security Operations Center (HSOC).

FIGURE 2.5 – National Response Plan National Structure (DHS, 2004c)

Multiagency Coordination Entities on the other hand refer to those units whose main duty is to coordinate the overall incident management effort by establishing priorities among the incidents and the allocation of resources, resolving possible agency policy conflicts, and providing general guidance to support the activities (DHS, 2004c). The JFO Coordination Group and the Interagency Incident Management Group (IIMG) are the two bodies comprised in the NRP as Multiagency Coordination Entities.

According to the NRP (2004c), the President leads the Nation in its effort to respond effectively to Incidents of National Significance, and is responsible for ensuring that all the necessary resources are available for this purpose. Nevertheless, the overall coordination of all activities undertaken by the Federal departments and agencies involved in an incident that requires Federal intervention is executed by the Secretary of Homeland Security.

To facilitate information sharing and operational coordination at the national level, the Homeland Security Operations Center (HSOC) is established as part of the national structure through its National Response Coordination Center (NRCC). The HSOC was originally established in July 2004 with the purpose of creating a focal point for collecting and disseminating homeland security information among agencies, as well as to act as a national coordinating point of incident management operations (DHS, 2004a). It is a standing facility that concentrates and delivers real-time information on homeland security and situational awareness nationally. For incident management coordination, as the incident requires, the NRCC activates the necessary ESFs and notifies the appropriate agencies to report in time to the NRCC. According to the NRP, some of the roles and responsibilities assigned to the HSOC (NRCC) for incident management include:

- Establishing and maintaining real-time communications links to other Federal EOCs at the national level, as well as appropriate State, tribal, local, regional, and NGO EOCs.
- Maintaining communications with private sector critical infrastructure and key resources information-sharing entities.
- Providing general domestic situational awareness, common operational picture, and support to and acting upon requests for information from the Interagency Incident Management Group and DHS leadership.

The Interagency Incident Management Group (IIMG) acts as the strategic coordinating and planning entity for interagency incident management at the Federal headquarters' level. According to the characteristics and specific requirements of the event, it is activated and staffed by senior representatives of the DHS, Federal department and agencies, and Nongovernmental Organizations. Its composition is flexible according to the expertise required by the severity and complexity of the incident. The IIMG also serves as a source of information to the White House and provides recommendations to the Secretary of Homeland Security.

Coordination of activities at the regional level is performed by the Regional Response Coordination Center (RRCC) until the JFO is considered necessary and is established in the field. The RRCC facility is operated by the DHS/Emergency Preparedness and Response/FEMA and is activated to coordinate all regional response efforts, establish Federal priorities, and implement local Federal program support (DHS, 2004c). Once a JFO is established, all regional activities by the RRCC are relegated to support responsibilities for the JFO.

The JFO is the multiagency Federal coordination center at the field level. It is organized using an ICS-type structure as established in the NIMS, including the usual

command, operations, planning, logistics, and finance/administration sections. Hence, the JFO structure is flexible enough to accommodate the particular requirements of specific incidents. Even though the organization of the JFO includes an operations section, it does not have on-scene operational duties. Its functions focus primarily on providing proper support to on-scene operations. Following the specific duties assigned in the ESFs of the NRP, it is staffed by personnel from Federal departments and agencies, other entities with jurisdictional authority, and the private sector, as appropriate.

A JFO Coordination Group is established at the field level to direct all activities performed by the JFO, and provide strategic guidance and resolution of any conflicts in priorities for allocation of critical Federal resources (DHS, 2004c). This is especially useful in incidents that require the intervention of multiple States or jurisdictions (e.g., multiple incidents at separate sites) that may require separate activated JFOs, each one competing for Federal resources.

CHAPTER 3 - EMERGENCY MANAGEMENT IN INDIANA

Before going into detail about how emergencies are managed in the State of Indiana, it is important to recognize that Indiana is susceptible to various types of disasters, whether these are natural or manmade. Inclement weather patterns affect the state from time to time, causing floods and snowstorms. Southern parts of the state are considered to have a high-potential for earthquake activity (INDOT, 2000; SEMA, 2005). The recent emphasis on terrorist threats is another of the various types of incidents that must be considered by Indiana's emergency management organizations to protect life and property within the state. Many incidents that occur on a daily basis are effectively managed by local emergency services. Disasters, however, may impose significant damage on the social and economic system beyond the capability of local authorities and may require involvement by the state and even the Federal government, as explained in Chapter 2.

Emergency management in Indiana works under the assumption that, once an incident occurs, response efforts are assigned first to local-level emergency management organizations. Involvement by statewide agencies and departments is required once these local efforts are overwhelmed by the nature or the scale of the incident, and local agencies are no longer capable of handling the emergency appropriately. Depending on the severity and complexity of the incident and the degree of involvement of the different authorities in the response efforts, six levels of response have been defined for Indiana (SEMA, 2003):

- Level I – Local level, no mutual aid or state assistance required.
- Level II – Local level, mutual aid requested, no state assistance required.

- Level III – State assistance requested, State Emergency Operations Center not activated.
- Level IV - State assistance requested, State Emergency Operations Center activated.
- Level V – Governor’s Declaration of Disaster, no federal assistance requested.
- Level VI – Federal assistance requested.

When assistance at the state level is required, state departments and agencies are required to perform certain tasks and responsibilities to adequately support the response efforts for the incident at hand. In this manner, agencies are required, not only to be capable of understanding and assuming certain emergency management roles additional to their normal operation procedures, but also to be capable of integrating their efforts consistently. This represents one of the most problematic issues, considering that agencies that normally do not work together need to suddenly do so during a very limited time frame.

To focus all emergency efforts and enhance the interoperability of the different agencies that might be involved during an incident of statewide proportions, all states in the US are required to have a state emergency management plan (AASHTO, 2002a). These state plans serve as a central guideline and basic framework of operations for all state agencies to adopt and implement once an incident of statewide implications has occurred. Prior to the release of the National Incident Management System, most state plans, including that of Indiana, followed the structure of the Federal Response Plan (AASHTO, 2002a). This structure consisted of a Basic Plan, a set of Emergency Support Functions (ESFs), and a series

of hazard-specific annexes. With the release and implementation of the NIMS, state emergency plans are expected to be updated as required to contain new measures required in this new framework.

After the events of 9/11, a new level of concern was raised regarding the degree of preparedness and the capability of the Nation's state and local entities to deal with large scale terrorist incidents. With this in mind, Indiana has adopted a number of initiatives to update and strengthen its capacity to withstand and respond effectively to these types of incidents. The purpose of this chapter is to describe how emergencies are currently managed in the State of Indiana, and the roles agencies such as the State Emergency Management Agency (SEMA), local Emergency Management Agencies, and the Counter-Terrorism and Security Council (C-TASC) play in this process*. Finally, INDOT's current emergency response capabilities are outlined according to what the research team observed during the development of this study.

3.1 State Emergency Management Agency – SEMA

After the Civil Defense Act of 1950 was amended in 1979 to create the Federal Emergency Management Agency (FEMA), state governments were directed to implement emergency management agencies at the state level (Hamilton County, 2005). Consequently, Indiana Code Title 10 (State of Indiana, 1998) created the Indiana State Emergency Management Agency (SEMA), which is the lead emergency management agency in the State. It consists of four divisions, namely, Mitigation/Recovery, Operations, Preparedness, and Technological Hazards. For the

* At the time this document was written, the Governor of Indiana had announced the creation of the Indiana Department of Homeland Security (IDHS). The IDHS will combine all the state's emergency management and homeland security efforts including the roles of SEMA and C-TASC (IDHS, 2005). No specific modifications in Indiana's emergency management system or procedures was available at this time. Therefore, there is no distinction made between SEMA and IDHS in this document.

purpose of this study, it is important to focus to some extent on how the Operations division works, and how emergency response efforts are handled within the state.

As mentioned above, SEMA is the lead emergency management agency in Indiana. However, as a way to enhance preparedness and response coordination locally, all counties in the state have Emergency Management Agencies (EMAs) as part of their local governments (State of Indiana, 1998). Each EMA has an Emergency Management Plan that includes procedures to follow during the occurrence of an emergency, including a detailed chain of command and an outline of all tasks assigned to local agencies that may be called upon to support response efforts. An Emergency Management Advisory Council (EMAC) consisting of local authorities and agencies involved in emergency management is also part of each EMA. The EMAC serves as a supervising and controlling body for all emergency management programs in the county (State of Indiana, 1998). All emergency management programs and efforts of each EMA are supported and coordinated with SEMA. However, EMAs are not part of SEMA, but part of the local governments. As of 2003, Indiana had an EMA assigned to each of the 92 counties. Of these, 36 had full-time staffs, 49 part-time, and 7 relied on volunteers (C-TASC, 2003).

When the scale or nature of an incident requires local governments to seek State assistance, county officials may declare a local state of emergency. Assistance to local governments is then coordinated through SEMA, and if required, the State Emergency Operations Center (EOC) is activated for this purpose.

The EOC serves as a multiagency coordination center as explained in Chapter 2. It functions as the central point for all information from state agencies, volunteer organizations (such as the Red Cross), and EMAs involved in the response efforts to coordinate their activities. As explained later in Section 3.2, the EOC is the coordination point of all activities and responsibilities outlined in the Indiana

Comprehensive Emergency Management Plan (CEMP). Figure 3.1 shows the chain of coordination of these activities and how these are all concentrated through the EOC. Representatives from the organizations and agencies involved in the emergency response effort may be required to assemble in the EOC as a way to improve coordination between the different parties.

FIGURE 3.1 – EOC Chain of Coordination

An important component of SEMA's operational efforts is the Mobile Command Center (MCC) shown in Figure 3.2. The MCC provides on-site support and assistance to the EOC. It is fully equipped with laptop computers, radio systems, satellite phones, cellular phones, hard-line telephones, FAX, and televisions for monitoring local broadcasts. These features enable the MCC to handle information to and from the EOC, and provide support to local residents during an emergency. Its communication systems are also interoperable with the Indiana State Police, the Department of Natural Resources, the National Guard, and Federal agencies, if required (SEMA, 2004).

FIGURE 3.2 - SEMA's Mobile Command Center (SEMA, 2004)

At the time this report was written, a new MCC was planned to be acquired by SEMA. According to SEMA, this new MCC will have more capacity than the current MCC, and will additionally be able to accommodate authorities and personnel from the local agencies involved in the response efforts, if required, as a way to further coordinate incident activities.

3.2 Indiana Comprehensive Emergency Management Plan – CEMP

For the specific case of the State of Indiana, the Indiana Comprehensive Emergency Management Plan (SEMA, 2003), developed and maintained by SEMA, constitutes the State's emergency plan. The CEMP addresses emergency procedures and actions to be implemented by Indiana agencies in the event of a disaster, once all efforts by local emergency management agencies are overwhelmed by the nature of the incident, and assistance from the State government is required. The plan is activated as the situation warrants by the Executive Director of SEMA, or immediately when a state of emergency is declared by the Governor (SEMA, 2003).

The CEMP follows an all-hazards approach to emergency management. As a result, the elements of the plan are applicable for any type of emergency, whether it is a natural disaster or a man-made incident. The structure of the CEMP is shown in Figure 3.3. As mentioned above, the CEMP was developed following a structure similar to that of the former Federal Response Plan, that is now in NIMS. The CEMP is divided into six sections, as shown in Figure 3.3, with a set of ESFs assigned to each one of these sections. For example, the Infrastructure Support Section is subdivided into four ESFs: Public Works/Engineering, Energy, Damage Assessment, and Transportation. Similar to the concept used in the NIMS, the CEMP gives a primary agency direct responsibilities for each of these ESFs, and a set of support agencies take care of support activities. Figures 3.4a and 3.4b show the primary and support agencies for each one of the ESFs in the CEMP.

Once the CEMP is activated, all activities outlined in the CEMP are coordinated through the EOC. Figure 3.3 illustrates the structure applied to coordinate activities in the EOC once the CEMP is activated.

FIGURE 3.3 - Indiana Comprehensive Emergency Management Organization
(SEMA, 2003)

Each ESF is further divided into the four basic components of emergency management, namely, mitigation, preparedness, response, and recovery. For each of these components, tasks are assigned in checklist form for agencies to perform as required. To illustrate this, Figure 3.6 shows the response tasks defined in the Transportation ESF of the CEMP. The CEMP outlines all tasks so that each State agency or department is aware of its responsibilities in an emergency and the actions it may be asked to perform. The means to accomplish each one of these tasks, however, is the responsibility of each agency. For a detailed description of all the tasks assigned to INDOT for each ESF of the CEMP, refer to Appendix A.

The Hazard Specific Section of the Comprehensive Emergency Management Plan addresses issues not covered in the other sections of the plan for specific types of hazards, specifically for those involving terrorism. It is an attachment with duties each agency has to perform in the event of a terrorist attack, in addition to those already covered in the rest of the plan.

As mentioned above, all State agencies are expected to be capable of performing the tasks outlined in the CEMP when an emergency requires. In this manner, the CEMP directs all State departments and agencies to develop a Standard Operating Procedures (SOP) plan as a way to guarantee adequate preparedness once an incident of significance occurs. The Standard Operating Procedures plan must include some basic elements, such as (SEMA, 2003):

- Designation of lines of succession and delegating authority for the successors
- Provisions for the preservation of records
- Procedures for the relocation of essential departments to ensure continuity of government
- Procedures to deploy essential personnel, equipment and supplies

EMERGENCY SUPPORT FUNCTION	Public Information	Communications	Information & Planning	Resource Support	Fire Fighting	Health & Medical	Search & Rescue	Hazardous Material	Law Enforcement
ORGANIZATION									
American Red Cross	S		S	S					
Board of Animal Health	S		S	S		S	S		
Civil Air Patrol	S	S	S	S			S		
Department of Administration	S		S	S	S				
Department of Budget			S	S					
Department of Commerce	S		S	S					
Department of Corrections			S						S
Department of Education	S		S	S		S			
Department of Fire & Building Services	S		S	S	P		S	S	
Department of Natural Resources	S		S	S	S		S		S
Family & Social Services Administration	S		S	S		S			
Indiana Department of Environmental Management	S		S	S	S	S		P	
Indiana State Department of Health	S		S	S		P		S	
Indiana State Police	S	S	S	S			S	S	P
Indiana Department of Transportation	S		S	S					
Indiana Volunteer Organizations Active in Disasters			S	S			S		
Indiana Utility Regulatory Commission	S		S	S					
Office of the Commissioner of Agriculture	S		S	S		S			
Military Department of Indiana	S	S	S	S		S	S	S	S
State Emergency Management Agency	P	P	P	P	S	S	P	S	S

P- Primary Agency: Manages the Emergency Support Function
S- Support Agency: Supports the Primary Agency

FIGURE 3.4a – Primary and Support Agencies by ESF (SEMA, 2003)

EMERGENCY SUPPORT FUNCTION	Shelter & Mass Care	Food & Water	Animal Health and Care	Donation & Volunteer Management	Transportation	Public Works & Engineering	Energy	Damage Assessment
ORGANIZATION								
American Red Cross	S	S	S	S	S			S
Board of Animal Health	S	S	P	S	S			S
Civil Air Patrol								S
Department of Administration		S			S	P		S
Department of Budget				S				
Department of Commerce					S		S	S
Department of Corrections					S			
Department of Education	S	S			S			
Department of Fire & Building Services								S
Department of Natural Resources	S		S		S	S		S
Family & Social Services Administration	S	S					S	S
Indiana Department of Environmental Management		S	S				S	S
Indiana State Department of Health	S	S	S				S	
Indiana State Police					S			
Indiana Department of Transportation		S			P	S		S
Indiana Volunteer Organizations Active in Disasters	S	S		S			S	
Indiana Utility Regulatory Commission						S	P	S
Office of the Commissioner of Agriculture		S	S					S
Military Department of Indiana	S	S	S		S	S	S	S
State Emergency Management Agency	P	P	S	P				P

P- Primary Agency: Manages the Emergency Support Function
S- Support Agency: Supports the Primary Agency

FIGURE 3.4b – Primary and Support Agencies by ESF (SEMA, 2003)

FIGURE 3.5 –EOC Chain of Coordination (SEMA, 2003)

Transportation

√	Response Task	Resource
5-5	Coordinate with Law Enforcement Emergency Support Function and Public Works Emergency Support Function, to provide assistance in placing barricades, controlling traffic, etc., as needed.	Indiana State Police Indiana Department of Transportation State Emergency Management Agency Department of Natural Resources
5-6	Coordinate the acquisition and allocation of helicopters to assist in overhead incident site inspection.	Indiana State Police State Emergency Management Agency
5-7	Coordinate with local jurisdictions for the acquisition of transportation assets in case of the evacuation of state buildings in Indianapolis (including hospitals and governor's mansion), as needed.	Special Enforcement Section, State Police
5-8	Coordinate with local jurisdictions for the acquisition of transportation materials in case of the evacuation of state properties (excluding state buildings in Indianapolis), as needed.	Indiana State Police
5-9	Coordinate with local jurisdictions for the acquisition of transportation materials in case of the evacuation of state parks, forest, and recreation areas, as needed.	Department of Natural Resources
5-10	Coordinate with local jurisdictions for the acquisition of transportation materials in case of the evacuation of prisons or shelter-in-house, as needed.	Department of Corrections
5-11	Obtain fuel from other states, as needed.	State Emergency Management Agency
5-12	Coordinate with Federal and State agencies, to determine hours of service and issue regulation waiver for commercial vehicles delivery of critical energy products	Indiana State Police Department of Commerce Department of Transportation State Emergency Management Agency
5-13	Provide transportation assistance in the evacuation of special needs population throughout the State, as needed.	State Emergency Management Agency Indiana State Department of Health Family Social Services Administration

**FIGURE 3.6 - Response tasks assigned by the CEMP in the Transportation
Emergency Support Function**

State agencies are also required, as stipulated under Executive Order 02-16 of 2002, to designate a State Agency Emergency Management Coordinator and at least two back-ups to act as the coordination point of the agency in all emergency and disaster matters (O'Bannon, 2002). Documentation of activities to SEMA's Executive Director is also required for agencies included in the CEMP, both during and after a State of Emergency is declared by the Governor. A daily Situation Report is to be submitted during the State of Emergency, and an after-action report including all the costs incurred must be submitted once the event has concluded.

3.3 Indiana Counter-Terrorism and Security Council - C-TASC

As it has been mentioned before, the new terrorist threat transformed the way agencies had been considering emergency management. Shortly after 9/11, many States created homeland security offices and organizations to concentrate specifically on the possibility of terrorist attacks within each jurisdiction. The DHS further directed all State governors to name a State homeland security contact who would be the point of contact between the DHS and the State government in matters of homeland security.

In a similar way, Indiana created the Counter-Terrorism and Security Council (C-TASC) that serves as a liaison between the State and the DHS. The main purpose of C-TASC was to serve as a central guide of all counter-terrorist activities required to protect the State from a terrorist attack, by developing a State strategy for homeland security (C-TASC, 2003). The Council, which meets periodically to revise and update this strategy, consists of a number of different authorities within the State, such as the Lieutenant Governor, a State Senator and a State Representative, and members of the Indiana Department of Environmental Management, the Commissioner of Agriculture, Indiana State Police, Indiana National Guard, the State

Fire Marshall, the Indiana State Department of Health, the State Emergency Management Agency, and the Indiana Department of Transportation.

In January 2003, C-TASC released *Indiana's Strategy for Homeland Security* (C-TASC, 2003). The document is a guide with specific goals that Indiana must concentrate on to enhance its capability to withstand a potential terrorist incident. It is based on information obtained from diverse sources both within Indiana, such as local expert opinions and advisory groups, as well as from national trends and best practices (C-TASC, 2003). The Strategy recognizes four critical mission areas and proposes initiatives to enhance each one of these. These mission areas are:

- Intelligence warning and counter-terrorism
- Protection of critical infrastructure, key assets and events
- Defense against catastrophic events
- Emergency preparedness and response.

The emergency preparedness and response mission area deserves further comment because it is related to the purpose of this project and is intended to affect emergency response in Indiana. According to C-TASC (2003), all emergency response activities should follow an all-hazards approach. Because the Incident Command System (ICS) works under this principle (refer to Section 4.1), the Strategy identifies this system as the protocol to be implemented by all emergency response agencies, and proposes a thorough training regimen to standardize its practice. Another proposed initiative outlined in the Strategy is the need to revise the adequacy of the State EOC, and to consider the possibility to relocate it to a more suitable location. The strategy also highlights the need to normalize EMA operational procedures and preparedness efforts by implementing mechanisms such as the

development of minimum performance standards, comprehensive emergency management plans, and standard operating procedures.

3.4 Indiana Department of Transportation - INDOT

As stated in the CEMP, the Indiana Department of Transportation (INDOT) plays a vital role in emergency management in Indiana. When assistance is required, INDOT will be expected to perform certain tasks that may be different from its normal day-to-day operations. As stated in AASHTO's *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents* (AASHTO, 2002a), INDOT as a State DOT has two sets of responsibilities to focus on during emergency response. There are *internal* responsibilities, which refer to all arrangements within INDOT that need to be performed to accomplish the tasks outlined in the CEMP, and *external* responsibilities, which refer to the specific tasks outlined in the CEMP for the more general Indiana emergency management framework. As mentioned before, the CEMP outlines all tasks to be accomplished by INDOT; these constitute its external responsibilities. However, the means to accomplish each one of these tasks lie within INDOT's capacity and operational capability. Therefore, INDOT's inherent organization should be prepared to perform these external tasks; these constitute its internal responsibilities.

For the development of this study, the research team invested considerable time in understanding INDOT's current emergency response procedures and capabilities. During this time, we were able to attend a number of security-related meetings and discussions within the agency, including those of the INDOT C-TASC.

The INDOT C-TASC is a committee formed within INDOT as a result of the concern about the agency's preparedness and capacity to respond adequately to the new terrorist threat and its implications. It consists of high-level INDOT officials and

representatives from its different divisions and districts. It meets regularly to discuss transportation security issues and programs that need to be considered within the agency. Input from representatives of external agencies such as the Indiana State Police (ISP) and SEMA, and the various Purdue security-related projects is also considered.

As a way to focus on the numerous matters of transportation security, INDOT C-TASC has designated five subcommittees to concentrate on individual topics of interest. These subcommittees are the Awareness/Education Subcommittee, the Prevention Subcommittee, the Communications Subcommittee, the Incident Response Subcommittee, and the Assessment Subcommittee. Each of these subcommittees has developed a list of action items within its purview to address what they identify as their most important issues. Some action items have been addressed; others need further attention.

Current INDOT capabilities were also observed by attending a mock drill designed by Professor Shimon Nof and his team at Purdue University. The mock drill consisted of a computer-based scenario that simulated a series of terrorist events in Indiana's highway system and allowed the different participants of the drill, including representatives from two INDOT districts, INDOT central office, SEMA, and the ISP, to make decisions as the situation evolved. The decisions made by each one of the parts affected the overall situation of the incident and its possible outcome, just as it would in a real emergency. This exercise proved to be an excellent opportunity to observe INDOT's current capabilities and procedures to handle a serious attack on the transportation infrastructure. It also allowed INDOT to see more clearly what its actual strengths and weaknesses are in the case of a significant emergency.

Based on our observations, several comments and conclusions can be stated about INDOT's current emergency management capabilities. The following is a

description of issues observed by the research team during the development of this project.

3.4.1 Emergency Operations Plan - EOP

INDOT's external responsibilities in response to an emergency are basically supportive. INDOT's emergency operations are performed today based on having developed relationships with key individuals in other agencies (e.g., ISP, DNR, SEMA). Based on prior experience, INDOT personnel in both the districts and the central office know what to do and whom to contact (both internally and externally), depending on the type of event. Even though this practice may have proved to be effective for INDOT in dealing with common incidents (USDOT, 2003), the new terrorist framework in emergency management and the potential threat of incidents involving WMD pose a significant challenge and may require revising current procedures and developing new practices. For these types of events, agencies with no previous relationship may have to work closely with INDOT, and this new relationship might have to be formed in the wake of a catastrophe. Clearly, this is neither convenient nor desirable. Furthermore, normal contacts within INDOT, as well as those outside the agency, may not be available during an incident, and this has to be accounted for beforehand.

As this report is being written, there is no INDOT Emergency Operations Plan. There is no set of standards and operating procedures designed to be implemented for response to an incident. In such a way, INDOT relies exclusively on the previous knowledge and prior experience that its employees possess regarding the procedures to follow during an emergency. Although outlines of emergency plans have been drawn up by some INDOT Districts, especially to comply with OSHA emergency standards (e.g., building evacuation procedures and fire escape routes), there are no

specific standards as to the precise requirements and development of highway emergency plans and procedures. Furthermore, these plans are not well known to or coordinated with the Central Office.

3.4.2 Lines of Authority and Communication

When an incident occurs, it is important for INDOT personnel to understand and be clear about what their specific duties are and what they are expected to do. Furthermore, it is important for all personnel involved to understand who is in control and what lines of authority to follow, because these may be different from the usual operational structure. From what we observed during this project, INDOT does not have a specific command structure to adopt during response to an emergency. This was apparent during the INDOT mock drill. The decision-making process varied from district to district and coordination between districts had to be improvised. There was also uncertainty on the part of the districts as to what was the role and authority of INDOT's Central Office during an incident.

During emergency operations, a continuous and significant flow of information may be expected to occur from a number of different sources. Information, which may sometimes be even contradictory, may be originating from the incident site, the EOC, an INDOT district, or INDOT's Central Office. With this in mind, it is crucial that all information is delivered to the correct personnel when it is required, and in the safest and most secure manner. In a similar way, as with the lines of authority, there are no pre-specified lines of communication defined for INDOT to adopt during emergencies. During the INDOT mock drill, there was uncertainty as to whom to call, under what circumstances and how to do so, when the situation was not one that had been faced before. Furthermore, participants were uncertain as to what kind of

information would be available to them if an incident like the one simulated actually occurred.

3.4.3 Standard Operating Procedures

Based on our observations during this project, there currently exists no set of Standard Operating Procedures to be adopted by the INDOT Districts and INDOT Central Office for emergency response operational tasks. The decisions as to what to do and how to do it are basically made independently within each INDOT District based on individual judgment. An example is road closure decisions during the INDOT mock drill. The incidents being simulated caused some significant roadways to be closed and alternate routes to be identified. The decisions to close the roads, and what specific roads to close, were made by each district independently, based on their own judgment about the situation. No standard procedures existed as to guide how these decisions were to be made, and what implications had to be considered in deciding which roads to close. If consideration was given to the capacity of the alternate routes motorists would have to use, or the potential need to modify traffic signals on these routes, it was not obvious to observers of the mock drill. Basically, the decisions of which roads to close were made by observing the location of the affected roadways and estimating what the best alternate routes were by their location on a map. The decisions may have been proper en expedient, but there was uncertainty as to what agencies had to be contacted regarding a road closure decision, or if there was a need to at all.

The closest approximation to a set of Standard Operating Procedures found for INDOT is that for the structural assessment of bridges and roads after an earthquake as stated in *INDOT Post-Earthquake Safety Evaluation of Bridges and Roads CD-ROM* (INDOT, 2000). This CD-ROM contains a set of procedures for the structural

evaluation of bridges and roads by INDOT personnel following an earthquake. It defines two basic levels of inspection that can be performed according to the level of expertise of the personnel performing the assessment. Inspection Level 1 is intended to be a rapid assessment by INDOT personnel with a broad range of backgrounds, while Level 2 consists of a more thorough inspection to be performed by INDOT engineers. Outlined in the CD-ROM are specific procedures to follow for each of the inspection levels, including detailed steps for the evaluation, use of report forms, equipment required for the assessment, and procedures for closing damaged bridges to traffic.

3.4.4 Knowledge of Statewide Emergency Management

As has been mentioned before, INDOT is just a part of a statewide emergency response effort that includes the involvement of a number of different organizations working towards the same goal. With this in mind, it is important for INDOT to understand what its role is and where it stands in this larger state emergency management framework. Furthermore, it is vital to understand what this framework is and how it works.

An important issue observed during the INDOT mock drill was the unfamiliarity of INDOT personnel with SEMA and ISP roles and procedures. Participants of the mock drill were uncertain of the roles other agencies played in the response operations, how these other agencies could be contacted, or if contacting them was appropriate at all. Some participants knew of the existence of a State EOC and SEMA's role as an emergency coordinator of activities. However, there was uncertainty as to what the role of INDOT was and how it related to SEMA. Some participants didn't know if a contact with SEMA had to be established directly, and what were the means to do so. Some were aware of the existence of an INDOT representative in the State EOC.

Nevertheless, they were not certain as to who this contact was, his/her specific role, and how he/she could be contacted. Basically, there was little knowledge as to what the role of SEMA was, and how it related to INDOT.

It is imperative for INDOT personnel to have proper knowledge of emergency management in Indiana, where INDOT stands, and what are the roles of the different agencies involved. This also includes knowledge of the basic terminology used in an emergency and what it means (e.g., State of Emergency, Command Post, and EOC).

CHAPTER 4 – BEST PRACTICES IN EMERGENCY RESPONSE

The terrorist events of 9/11 highlighted the need for transportation agencies to reconsider their level of preparedness to respond adequately to large scale incidents. Up to that point, highway emergency response was considered as a local issue and concentrated mainly on natural disasters (AASHTO, 2002a). Departments of Transportation had different stages of preparedness, depending on the levels and types of risks considered, on a region by region basis.

In an effort to update and enhance emergency response capabilities in the new terrorist threat framework of operations, DOTs across the nation have adopted and implemented a number of different initiatives tailored to their specific needs and budgets. As a result, the level of preparedness of DOTs varies from State to State. In addition, a wealth of information from diverse sources has been developed and is now available for DOTs to consider. Agencies and organizations like FHWA, FTA, AASHTO, TRB, and ITE, as well as private organizations and academia are constantly developing new material regarding transportation security. Emergency response articles and papers are continuously being published on the Internet. Furthermore, the Federal government's concern in security is constantly affecting transportation agencies' security policies.

In this way, identifying what specific measures and requirements to address in order to enhance DOT response capabilities is not an easy task. The purpose of this chapter is to present what the research team has identified as the best practices in highway emergency response currently available and applicable to INDOT. The chapter is the result of an extensive literature search and review of material available from a number of sources, some of which were not exclusively transportation oriented.

In addition to the literature review, the research team concentrated on current practices employed by other State DOTs. Several State DOTs and State Homeland Security Departments were contacted by phone and/or e-mail, and two surveys were performed to obtain information on current practices across the US. Both of these surveys were distributed to the 50 State DOTs.

The first survey was sent to transportation security contacts at each state DOT. Contact was made initially with the Highway Performance Monitoring System (HPMS) specialist at each state DOT, who forwarded the survey to the appropriate state DOT transportation security expert. This survey concentrated specifically on the use of the Incident Command System (ICS) by DOTs, and will be referred to as the “ICS Survey” in this document. A total of 13 responses were obtained. The second survey was performed through AASHTO’s Transportation Security Forum in collaboration with INDOT. This survey addressed a number of questions regarding transportation security, including the use of ICS, the existence of Emergency Operations Plans, and the use of Decision Support Systems (DSS) by State DOTs. A copy of the questionnaire used for this survey is attached as Appendix B.

4.1 Incident Command System – ICS

Emergency response efforts may often involve the participation of a number of different response agencies and organizations that need to work together and share resources in the most effective and efficient way possible. Local level incidents may involve interaction between local law enforcement agencies and fire departments, as well as other local emergency response organizations. When the nature and scale of the incident requires it, State and Federal level agencies may also be required to support local emergency response efforts, as explained in Chapter 2.

Because some of these emergency response organizations do not work together in their routine non-emergency operations, coordination and effective cooperation between them can be a significant challenge in emergency management. Furthermore, the role of each of the parties involved may differ according to the type of incident, whether it is a fire, a chemical spill, or a terrorist incident, to name a few. Different types of incidents may require different response activities and different emergency agencies involved. Regardless of the size of the incident or the number of agencies involved in the response, all incidents require a coordinated effort to ensure an effective response and the efficient, safe use of resources (FEMA, 1998).

As a way to standardize how emergency response activities are integrated and coordinated at the incident site, the Incident Command System (ICS) has emerged as one of the Nation's best practices in emergency response. Its basic objective is to standardize how emergency response efforts are coordinated by applying (a) a basic operational structure that adapts to the complexity and demands of the incident, and (b) a set of standard principles for all responding agencies. In this manner, all agencies will be "speaking the same language" during response to an emergency.

The Incident Command System was first conceived in southern California in the 1970s after response efforts to a series of wildfires highlighted recurrent problems in response operations such as (DHS, 2004b; FEMA, 1998; OSHA, 2004):

- Unclear lines of authority
- Too many people reporting to one supervisor
- Different emergency response organizational structures among responding agencies.
- Lack of coordinated planning efforts among responding agencies.
- Nonstandard terminology among responding agencies.

- Lack of capability to expand and contract as required by the situation.
- Inadequate, nonstandard and nonintegrated communications.
- Lack of consolidated action plans.
- Unclear or unspecified incident objectives.
- Lack of designated facilities.

These set of recurrent problems were found to be common in many other types of emergencies other than wildfires, especially for those that involved the collaboration of different agencies at the incident. Hence, after its creation, the ICS has been adopted by a vast number of emergency agencies as their standard structure for incident response. Although the original ICS has evolved through time, its essential principles and basic organizational structure are still applied today. Its effectiveness has been tested and proven in all types of emergency scenarios in the US, and it is now considered as the standard emergency response system structure. As mentioned in Chapter 3, initial compliance to NIMS requires all emergency response agencies to adopt ICS by FY2005. This includes ICS training of agency personnel who may be asked to be part of an ICS.

The effectiveness of the system is based upon applying a series of basic concepts and principles that allow the model to address some of the most common issues encountered in emergency response operations. These basic concepts and principles, summarized in Table 4.1, include the use of common terminology, a modular organization, integrated communications, application of the concept of unity of command, a unified command structure to organize operations, the use of consolidated Incident Action Plans (IAPs), a manageable span of control, the use of designated incident facilities, and the comprehensive management of resources (FEMA, 1998).

The following sections expand on the organization of the ICS structure, its different components, and how these basic principles are considered and applied in the model.

Table 4.1 ICS basic concepts (FEMA, 1998).

Principle	Description
1. Common terminology	<ul style="list-style-type: none"> - Common names for all resources, as well as for all facilities in and around the incident area. - Radio transmissions in plain English, without codes.
2. Modular organization	- Organizational structure at the incident develops from the top down.
3. Integrated communications	- Common communications plan, standard operating procedures, clear text, common frequencies, and common terminology.
4. Unity of command	- Each person within the organization reports to only one designated person.
5. Unified command structure	- Responding agencies manage incident by establishing a common set of incident objectives and strategies.
6. Consolidated Incident Action Plans - IAPs	-Written or oral plan describing all goals, operational objectives, and support activities for a period of time.
7. Manageable span of control	- Number of individuals one supervisor can handle is limited (usually five).
8. Designated incident facilities	- Incident Command Post and Staging Areas.
9. Comprehensive resource management	

4.1.1 ICS Basic Structure

The basic ICS structure consists of five essential elements as shown in Figure 4.1: *Command, Operations, Planning, Logistics, and Finance/Administration.*

Emergency personnel working in the Command section are normally referred to as the *Command Staff*, while all personnel on the other four sections are part of the *General Staff*.

Responsibilities in emergency response start with the Incident Commander (IC) in the Command element of the structure, and build from the top down. As the complexity of the incident demands, some or all of the other four sections can be activated by the IC to properly organize emergency management efforts. Once this is done, a Section Chief is assigned to each activated element to coordinate and manage activities. For example, if the Planning Section is activated by the IC, a Planning Section Chief is assigned. The ICS organizational structure is modular, extending to incorporate all elements necessary for the type, size, scope, and complexity of a given incident (DHS, 2004b). In this manner, each of the sections can be further broken down into units or branches to adapt to the specific needs of the incident.

Figure 4.1 – ICS Basic Structure (DHS, 2004b)

4.1.2 Incident Facilities

ICS identifies three types of incident facilities that can be implemented by the IC when a given incident so requires (FEMA, 1998): an *Incident Command Post (ICP)*, one or more *Staging Areas*, and a *Base*. The precise need for one or more of these facilities is given by the characteristics and requirements of each incident.

The ICP is the location where the IC is positioned and where all primary command functions take place (FEMA, 1998). For short-term small scale incidents, the ICP is usually a response vehicle such as a fire truck or patrol car (OSHA, 2004). For more complex events, however, the IC may denote a specific facility that will serve as the ICP for the entire response period. In either case, an ICP is always established.

Staging areas are locations designated for the specific purpose of storing and managing resources while they are assigned to response activities. As incidents become larger, a growing number of resources may be allocated to the incident, compromising the effectiveness of the response if these are not handled appropriately. Thus, the utilization of Staging Areas can avoid these problems, because resources are easily identified and promptly located when required.

For emergencies that require response efforts to continue over an extended period of time in which personnel is expected to come in and out of the incident site, the IC may establish a Base. The Base is the facility used to provide primary services and support activities for out-of-service personnel (FEMA, 1998). If established, it is also the place where the Logistics Section is located.

4.1.3 Command Function

The Command Function is conducted by the *Incident Commander* (IC). The IC is the individual in charge at the incident, responsible for all aspects of the response, including the development of incident objectives and managing all incident-related operations. Specific responsibilities assigned to the IC are shown in Table 4.2.

When an incident occurs, the IC position is initially taken by the senior first-responder to arrive at the scene (FEMA, 1998). Regardless of the type of incident, all emergencies have an IC. Once the incident evolves and/or additional units from

other responding agencies arrive at the scene, the IC position may be transferred to other officers with higher authority over the incident. The ICS details specific procedures for transferring command, such as briefing requirements to the new IC and notification procedures.

Table 4.2 – Command Staff Basic Responsibilities (OSHA, 2004)

Position	Responsibilities
Incident Commander - IC	<ul style="list-style-type: none"> • Establish and monitor incident organization. • Brief Command Staff and Section Chiefs • Establish immediate priorities especially the safety of responders, other emergency workers, bystanders, and people involved in the incident. • Determine incident objectives and strategy to achieve the objectives. • Authorize release of information to the news media. • Approve the implementation of the Incident Action Plan (IAP). • Coordinate activities for all staff under the ICS. • Coordinate with key people and officials. • Approve requests for additional resources or for their release. • Order the demobilization of the incident when appropriate.
Information Officer	<ul style="list-style-type: none"> • Obtain IC approval of media releases. • Inform media and conduct media briefings. • Obtain media information that may be useful to incident planning. • Maintain current information summaries on the incident and provide information on the status of the incident to assigned personnel.
Liaison Officer	<ul style="list-style-type: none"> • Assist in establishing and coordinating interagency contacts. • Monitor incident operations to identify current or potential inter-organizational problems.
Safety Officer	<ul style="list-style-type: none"> • Participate in planning meetings. • Review the Incident Action Plan (IAP) for safety implications. • Identify and produce correction of occupational safety and health hazards. • Continuously monitor workers for exposure to safety or health hazards conditions. • Alter, suspend, evacuate or terminate activities that may pose imminent safety or health danger to the workers. • Take appropriate action to mitigate or eliminate unsafe condition, operation or hazard.

For example, consider the case where there is an emergency call of suspicious activity in a residential neighborhood and a police patrol unit is sent to respond to the scene. As the police officer is the first person to arrive at the scene, he/she will perform the duties of the IC. When the police officer arrives at the scene and investigates the area, a shooting between rival gangs begins. The police officer calls for backup and additional police units arrive at the scene. A higher-ranking officer with higher authority is part of these additional units, and so, takes control of the response efforts and assumes the role of IC. The suspects are controlled by the police officers at the scene and are taken into custody. However, a fire has been started in one of the nearby buildings due to the shooting. The IC calls for support from a fire unit to control the situation. Because the incident's major objective at this time is to control the fire, when the fire unit arrives, command is transferred to the senior fire official who arrives at the scene. That fire official acts as IC until the fire is controlled.

When the nature and magnitude of the incident overwhelms the capacity of the IC, a series of positions with support roles for the IC can also be activated accordingly. These positions consist of the *Information Officer*, the *Liaison Officer*, and the *Safety Officer*. The Information Officer's role is to develop and release information about the incident to the news media, to incident personnel, and to other appropriate agencies and organizations (OSHA, 2004). The Liaison Officer on the other hand, serves as the point of contact for assisting and coordinating activities between the IC and other agencies and groups. This position is mainly required for incidents that are multi-jurisdictional, in which coordination between different agencies is expected. The Safety Officer's role is to develop and recommend measures to the IC for assuring personnel health and safety and to assess and/or anticipate any hazardous or unsafe situations (OSHA, 2004).

Although many incidents can be handled properly by an IC, others may require a different approach. Having a single authority from a specific agency has been proven to be inconvenient in some events, as in the case where operations involve the participation of a significant number of responding agencies. In addition, identifying a single authority in large scale incidents may not be an easy task, especially when agencies from multiple jurisdictions attend the emergency. In these types of cases, a *Unified Command* approach may be adopted, where command is taken by multiple incident commanders representing the various agencies involved. Decisions concerning the incident, including the development of objectives, are then made in conjunction with all the members of the Unified Command, thus, improving coordination of activities and avoiding duplication of efforts.

4.1.4 Operations Section

The Operations Section is responsible for all operations directly applicable to the primary mission of the response. Once activated by the IC, an Operations Section Chief is designated as the person responsible of all activities developed within the section. A list of its primary responsibilities is outlined in Table 4.3.

The way in which the different operational elements are organized within the ICS structure depends on the type of incident, the agencies involved, and the specific objectives and strategies to follow (FEMA, 1998). Agencies that could be included in the Operations Section include fire, law enforcement, public health, public works, and emergency services (FEMA, 2004). As the incident evolves, resources from these various sources will be assigned and deployed to accomplish diverse objectives within the overall response objectives. Following the definition stated in the NIMS, resources refer both to all the equipment allocated for incident response as well the personnel assigned (DHS, 2004b). As the number of resources assigned exceeds the

maximum span of control of the Operations Section Chief, the Operations Section can be further broken down into divisions or groups as shown in Figure 4.2.

Table 4.3 – Section Chiefs Basic Responsibilities (OSHA, 2004)

Position	Responsibilities
Operations Section Chief	<ul style="list-style-type: none"> • Develop operations portion of the IAP. • Brief and assign Operations Section personnel in accordance with the IAP. • Supervise Operations Section. • Determine need and request additional resources. • Report information about special activities, events, and occurrences to the IC.
Planning Section Chief	<ul style="list-style-type: none"> • Supervise preparation of the IAP. • Provide input to the IC and the Operations Section Chief in preparing the IAP. • Establish special information collection activities as necessary • Collect and process situation information. • Determine the need for any specialized resources in support of the incident.
Logistics Section Chief	<ul style="list-style-type: none"> • Participate in preparation of IAP. • Prepare service and support elements of the IAP. • Identify service and support requirements for planned and expected operations. • Plan the organization of the Logistics Section • Coordinate and process requests for additional resources. • Advise on current service and support capabilities.
Finance/Administration Section Chief	<ul style="list-style-type: none"> • Manage all financial aspects of the incident. • Provide financial and cost analysis information. • Maintain contact with agency(s) administrative headquarters on Finance/Administration matters.

FIGURE 4.2 – Organizational Elements of Operations (FEMA, 2004)

Divisions always refer to physical or geographical areas of operation, while groups refer to functional areas. Adopting this type of structure not only maintains a proper span of control, but also organizes how these resources are allocated to the incident and clarifies the objectives each one is assigned to perform. The decision regarding whether to use divisions or groups depends on the type of incident. Some cases demand that the Operations Section be broken down geographically for better organization, while in others, resources are better organized by the function they are assigned to perform. Figure 4.3 and Figure 4.4 show examples of the general breakdown when geographical divisions and functional groups are used, respectively. When the number of divisions and/or groups exceeds the proper span of control of the Operations Section Chief, these can be grouped accordingly into branches as shown in Figure 4.5.

FIGURE 4.3 – Example of use of Geographical Divisions (DHS, 2004b)

FIGURE 4.4 – Example of use of Functional Groups (DHS, 2004b)

FIGURE 4.5 – Branches (DHS, 2004b)

4.1.5 Planning Section

In cases where a large scale incident planning effort is required that exceeds the capacity of the IC, a Planning Section can be activated. Its basic responsibilities include the collection, evaluation, and dissemination of all tactical information related to the incident (FEMA, 1998). The Planning Section is also responsible for

maintaining the status of resources assigned to the incident, and for preparing and documenting the IAP. As mentioned before, the IAP is an oral or written plan that contains objectives reflecting the overall incident strategy, specific tactical actions, and supporting information for each operational period, which is usually of 12 or 24 hours (DHS, 2004b).

As with all other sections of ICS, a Planning Section Chief is assigned to oversee all activities within the section. The Chief's basic responsibilities are outlined in Table 4.3. When assigned, the Planning Section Chief is responsible for all tasks designated to the Planning Section. As incidents evolve, its capacity may be exceeded and thus a series of units can be activated as shown in Figure 4.6. Each of these units will perform a series of designated responsibilities as shown in Table 4.4. When a unit is activated, a Leader is designated to oversee all activities and personnel within the unit.

FIGURE 4.6 – Planning Section Breakdown (DHS, 2004B)

Because ICS is intended to adapt to all types of incidents, specialists from diverse fields of expertise may be required to support the overall incident objectives. Although these specialists can be assigned to different sections of the ICS structure, a special division is provided within the Planning Section. Examples of technical specialists include weather observers, environmental specialists, human resources experts, GIS specialists, and legal specialists (OSHA, 2004).

TABLE 4.4 – Planning Section Unit Tasks (DHS, 2004b; OSHA, 2004)

Planning Section Unit	Responsibilities
Resources Unit	<ul style="list-style-type: none"> • Keep track of the current location and status of all assigned resources. • Maintain a list of all resources committed to incident operations.
Situation Unit	<ul style="list-style-type: none"> • Collect, process, and organize ongoing situation information. • Develop projections and forecasts of future events. • Prepare maps. • Gather and disseminate information and intelligence for use in the IAP.
Documentation Unit	<ul style="list-style-type: none"> • Maintain accurate and complete incident files, including a complete record of major steps taken to resolve the incident. • File, maintain, and store incident files for legal, analytical, and historical purposes. • Prepare the IAP.
Demobilization Unit	<ul style="list-style-type: none"> • Develop an Incident Demobilization Plan with specific instructions for all resources that require demobilization.
Technical Specialists	<ul style="list-style-type: none"> • Support incident objectives by providing input from their field of expertise.

4.1.6 Logistics Section

The Logistics Section is activated to coordinate all activities for support to incident personnel. This section is usually necessary for long-term or extended operations (FEMA, 1998) in which significant resources and provisions are required to

support the personnel assigned to the response effort. The major activities can be grouped in six basic units if required, as shown in Figure 4.7. Responsibilities assigned to each of the units are outlined in Table 4.5. When the resources and facilities utilized by the Logistics Section are considerable, units can be grouped under two basic branches, a Service Branch that comprises the Communications Unit, the Medical Unit, and the Food Unit, and a Support Branch that includes the Supply Unit, the Facilities Unit, and the Ground Support Unit. This alternative organization is shown in Figure 4.8.

A Logistics Section Chief is designated once the Logistics Section is activated by the IC. The Chief's major responsibilities are listed in Table 4.3.

FIGURE 4.7 – Logistics Section Breakdown (DHS, 2004b)

TABLE 4.5 – Logistics Section Unit Tasks (DHS, 2004b; OSHA, 2004)

Logistics Section Unit	Responsibilities
Supply Unit	<ul style="list-style-type: none"> • Order, receive, store, distribute, and process all incident-related resources, personnel, and supplies. • Maintain inventory of supplies and equipment.
Ground Support Unit	<ul style="list-style-type: none"> • Maintain and repair primary tactical equipment, vehicles, and mobile ground support equipment. • Record usage time for all ground equipment. • Supply fuel for mobile equipment. • Provide transportation in support of incident operations.
Facilities Unit	<ul style="list-style-type: none"> • Set up, maintain, and demobilize all facilities used in support of incident operations including the ICP, incident base, and camps.
Food Unit	<ul style="list-style-type: none"> • Determine food and water requirements. • Provide food and water services for incident personnel.
Communications Unit	<ul style="list-style-type: none"> • Develop the Communication Plan to make the most effective use of the communication equipment and facilities in the context of a multiagency incident. • Install, maintain, and repair communications equipment.
Medical Unit	<ul style="list-style-type: none"> • Provide all medical services required by incident personnel.

FIGURE 4.8 – Logistics Section Branched Breakdown (DHS, 2004b)

4.1.7 Finance/Administration Section

Many incidents may require careful management of all financial and administrative aspects of the response, especially for reimbursement purposes. When this is the case, the IC may activate the Finance/Administration Section. This section is not always required, as many incidents may need only a technical specialist at the Planning Section that can handle all cost-related activities (DHS, 2004b; OSHA, 2004). When the Finance/Administration Section is in fact activated, a Section Chief is assigned with specific responsibilities as illustrated in Table 4.3. The Finance/Administrations Section can be broken down in units as shown in Figure 4.9. Each of these units is assigned with the tasks outlined in Table 4.6.

FIGURE 4.9 – Finance/Administration Section Breakdown (DHS, 2004b)

**TABLE 4.6 – Finance/Administration Section Unit Tasks (DHS, 2004b;
OSHA, 2004)**

Finance/Administration Section Unit	Responsibilities
Cost Unit	<ul style="list-style-type: none"> • Provide cost analysis for the incident. • Record all cost data. • Analyze and prepare estimates of incident costs.
Compensation/Claims Unit	<ul style="list-style-type: none"> • Handle injury compensation and claims including all necessary forms required by local agencies.
Procurement Unit	<ul style="list-style-type: none"> • Coordinate with local jurisdictions to identify sources for equipment. • Prepare and sign equipment rental agreements. • Process all administrative requirements associated with equipment rental and supply contracts.
Time Unit	<ul style="list-style-type: none"> • Ensure proper daily recording of personnel time in accordance with the policies of the relevant agencies.

4.1.8 Area Command

According to the NIMS (DHS, 2004b), the general purpose of an Area Command (AC) is to oversee the management of multiple incidents that are handled by separate ICS organizations (DHS, 2004b). For example, situations in which incidents occur simultaneously in different geographic locations may require several ICS to be implemented by emergency responders. Furthermore, if the incidents are of the same type, the different ICS response structures may compete for the same resources. In these situations, an AC is activated as a way to coordinate activities and prioritize the allocation of resources to avoid conflicts between the different ICS organizations (see Figure 2.5). Table 4.7 summarizes the responsibilities assigned to an AC once activated according to the NIMS.

TABLE 4.7 – Area Command Responsibilities

Area Command Responsibilities
<ul style="list-style-type: none">• Sets overall incident-related priorities.• Allocates critical resources according to the established priorities.• Ensures that incidents are properly managed.• Ensures effective communications.• Ensures that incident management objectives are met and do not conflict with each other or with agency policies.• Identifies critical resource needs.• Provides for personnel accountability and a safe operating environment.

An AC operates under the same basic principles as the ICS, but does not have operational responsibilities (DHS, 2004b). Figure 4.10 shows a typical Area Command structure as stated by NIMS. It consists of an Area Commander, a Planning section, a Logistics section, and a series of support positions that are activated when required. Each of these positions is responsible for performing certain tasks that ensure overall coordination of the multiple ICS structures activated.

The Area Commander is responsible for the overall management of the multiple ICS systems under the supervision of the AC. The Commander's responsibilities include ensuring that possible conflicts are resolved, that a set of overall incident objectives are established, and that strategies are selected for the use of critical resources (DHS, 2004b). He/she is also the individual responsible for coordinating with external organizations involved in the response (i.e., Federal, State, and local entities).

Figure 4.10 – Area Command Structure (DHS, 2004b)

The AC Planning Section is responsible for collecting information from the multiple ICS organizations to assess and evaluate potential conflicts among them (DHS, 2004b). This includes resolving conflicts that may arise in the allocation of critical resources for the overall response objectives.

The AC Logistics section, on the other hand, is responsible for all services and materials required at the AC level, and more important, for the effective allocation of critical resources and supplies among the multiple ICS structures (DHS, 2004b).

As mentioned before, a series of support positions can be activated when necessary. As shown in Figure 4.10, these may include a Critical Resources Unit Leader, a Situation Unit Leader, a Public Information Officer, and a AC Liaison Officer. According to NIMS (DHS, 2004b), the Critical Resources Unit Leader is activated to track and maintain the status and availability of critical resources assigned to each incident under the AC. The Situation Unit Leader, on the other hand, monitors the status of objectives for each incident or incident management teams (ICS structures) assigned to the AC (DHS, 2004b). The Public Information Officer is activated to coordinate all public information that may be released by the different ICS organizations, and is the point of contact for the media at the AC level

(DHS, 2004b). Finally, the Liaison Officer helps maintain off-incident interagency contacts and coordination.

4.1.9 ICS and DOTs

The previous sections highlighted the basic principles surrounding the ICS concept. As mentioned before, ICS is currently considered as the most appropriate emergency response system and is the standard organizational structure employed by emergency responders. Initiatives like NIMS and the NRP have expanded the use of ICS across emergency management agencies and have highlighted the need for these agencies to adopt the system.

The involvement transportation agencies can have in emergency response efforts has led some agencies to use ICS for their specific purposes. Today, many transit agencies like the Bay Area Rapid Transit in San Francisco, the New York City Transit, and the Long Island Rail Road among others use ICS to manage and coordinate their activities with first responders (Boyd and Sullivan, 2000). In a similar way, many DOTs across the nation have seen in ICS a valuable tool to organize both their internal and external emergency response functions.

For the purpose of this research, it was important to have a better understanding of the applications the Incident Command System currently has in other State DOTs. Particular attention was placed in obtaining information on current applications and how common these were among Departments of Transportation. In this way, in addition to contacting directly many DOTs via telephone or e-mail, specific questions regarding the use of ICS were included in both the ICS Survey and the AASHTO Security Forum survey conducted for this study.

A basic conclusion that was drawn from this exercise is that ICS is a common practice among DOTs. As shown in Figure 4.11, 20 out of the 26 States (77%) who

responded to the surveys said they currently use the ICS (or a modified version of ICS) for responding to large-scale emergencies, while only four (15%) said they do not. However, two of these said that, although they do not currently employ ICS, they expect to adopt it in the future when complying with the NIMS.

FIGURE 4.11 – ICS in State DOTs

The ICS is being used by State DOTs in two ways. First, its organizational structure and basic principles are used as a tool to coordinate and manage response efforts within the DOT. Once an emergency is declared, a pre-defined ICS organizational structure following the principles outlined in this chapter is activated accordingly within the DOT to handle the incident until the event is considered to be under control. All internal activities necessary to handle the emergency are managed within this ICS structure.

Second, because DOT personnel may be asked to perform response activities under the ICS activated by first responders at the incident, many DOTs have required their personnel to have basic training on ICS. In this way, DOT personnel assigned to the incident can integrate more easily with first responders and understand how they operate, thus solving a significant problem that has been observed in emergencies in the past (AASHTO, 2002a).

4.2 Communications

Communications play a key role in emergency response. Once an emergency has occurred, large amounts of information from a number of sources have to be effectively relayed among the responding parties to coordinate overall efforts. However, especially after 9/11, significant issues have been observed in the appropriateness of the communication systems, the technologies employed, and the procedures used by emergency personnel to disseminate emergency related information during an incident. In addition, the new terrorist framework of operations highlighted new considerations such as the redundancy of the systems and the need to prevent sensitive information from being available to the wrong hands. Because transportation agencies may play a crucial role in emergency response, it is important for INDOT to revise and review its current communications systems and procedures to assure they are appropriate to function in the event of a major disaster. This section summarizes some of the current communication issues and technologies found by the research team that are currently being discussed and implemented by emergency response agencies in the US.

4.2.1 Interoperability

Emergency response is a coordinated effort among a number of responding agencies. Although many of these agencies do not work together under normal conditions, they have to be able to communicate appropriately in the case of an emergency. This has become one of the most important challenges in emergency management, because many agencies' communications systems are not interoperable (9/11 Commission, 2004; AASHTO, 2002a; MIPT, 2004). The lack of interoperability may include not only the absence of incompatible technologies, but also discordant communication procedures and plans employed by the different agencies.

In many cases, including the response efforts in New York City after the attacks of 9/11, different agencies from different jurisdictions may use different communications technologies that become an obstacle when trying to disseminate information (9/11 Commission, 2004). Although this problem has been addressed in many jurisdictions, it is most likely that equipment from different jurisdictions is not interoperable (e.g., the county equipment may not communicate with the city equipment) (MIPT, 2004). In addition, the communication technology that is used effectively in normal operations may not be appropriate when trying to integrate activities and operate after large-scale incidents that may require special equipment. For example, it was observed that one of the major problems in the emergency response for 9/11 in New York City was the inability of the radio systems used by first responders to reach the personnel located in the top floors of the World Trade Center (9/11 Commission, 2004).

In other cases, the communication procedures used are not consistent among the different parties involved. For example, different agencies in the same jurisdictions may have the same radio frequencies assigned. Even though this may be considered

an acceptable practice in normal operations, in a large scale emergency this may result in congested channels and unintelligible communications (9/11 Commission, 2004). Another example is the discordant terminology used in radio transmissions. Different agencies may use different radio coding and refer to the same thing in a different way. This may become an obstacle when trying to communicate properly among them.

As mentioned in Chapter 2, the DHS has put significant effort into trying to standardize practices among emergency responders in the US. The NIMS and NRP have highlighted the need to standardize communications systems and procedures among agencies. In this way, the NIMS Integration Center is expected to release in the near future a set of standards to normalize communications among responders. (Refer to Section 2.2.4.) These standards will include specifications of communication systems and technology required to assure interoperability (DHS, 2004b; MIPT, 2004). To ensure proper communications ability, the infrastructure has to be such that it is compatible with equipment of other response agencies.

On the other hand, adopting the ICS as the standard system for emergency response resolves many issues of lack of interoperability. As mentioned in Section 4.1, one of the main principles of ICS is the adoption of common terminology among agencies (e.g., common names for all resources and radio transmissions in plain English without codes) and the integration of all communications (e.g., common communications plan, use of standard operating procedures, and common frequencies) (FEMA, 1998). By adopting the ICS and its principles, it is expected that many of the issues of non-interoperability can be resolved.

4.2.2 Information Assurance

Communications systems are the backbone of emergency response. Without a communication system, information can not be disseminated among the first responders and among the different agencies involved in the overall response initiative. With this in mind, one of the most important concerns for agencies to consider is the ability to have a reliable communications system, that is, one that is not likely to fail when it is most needed. The new terrorist threat has emphasized the importance of this concern, because agencies have to acknowledge the fact that communications systems themselves can be the target of an attack.

In this way, agencies should not only contemplate having communications systems with reasonably low vulnerability, but systems that can also operate and build upon a number of different technologies, like radio, hard-line phone, cell phone, fax, e-mail, and text messaging. For example, if in a large-scale incident the radio system becomes unavailable or inoperable, agencies may still communicate with their personnel via cell phones. The system has to be redundant enough that the possibility of failures during operations are reduced to the maximum extent possible, even if there is an attack on the communications system itself.

In addition to the above, 9/11 emphasized the need for emergency response agencies to reconsider the fact that some of the information handled during (and sometimes prior to) an incident might be classified. Agencies have to be able to communicate effectively in a way that does not compromise the confidentiality and integrity of the information (MIPT, 2004). It is important to ensure that any classified information is available only to the qualified personnel who need this information for their operations. In this way, emergency agencies may need to update their communications procedures to consider this issue appropriately. This may include establishing SOPs for the treatment of sensitive information. If some information is

considered to be classified, SOPs can guide personnel as to how this should be handled.

With this in mind, emergency response agencies may consider implementing some sort of user authentication system embedded in their communications systems and procedures. User authentication technologies have been developed for many applications (e.g., biometrics). Although it is expected to happen in the near future, these technologies are yet to be implemented in the communications systems commonly used in emergency response, like radios (MIPT, 2004). The use of biometric technology for identification is still considered to be relatively expensive. The current state of the practice is to provide authentication in radios with identifiers that allow personnel to know exactly what radios are being operated. However, this authentication system is vulnerable if the radios are lost or stolen (MIPT, 2004).

4.2.3 Lines of Communication and Notification Procedures

When communicating during an emergency, personnel have to be able to identify exactly who needs to be contacted and what procedures to follow to reach those contacts. In order to reduce improvisation, loss of valuable time, and confusion during actual emergency response, lines of communications can be defined prior to the incident as part of a preparedness effort. In this way, depending on the incident at hand, emergency personnel can know beforehand exactly what persons need to be contacted (both within the organization as well as externally), the information that needs to be relayed, and the way in which the contact should be made (radio, cell phone, etc.).

Based on the information gathered from State DOTs across the US, two basic practices are being adopted by transportation agencies to ensure proper communications practices for emergency response: (1) the adoption and application

of the ICS, and (2) the development of Standard Operating Procedures for communications of emergency information.

The ICS is a system that can help deal with some of these issues because it clearly defines an organizational hierarchy to be followed during a specific incident. In addition, the concept of Unity of Command mentioned in section 4.1 ensures that emergency personnel have a clear understanding of who they need to report to and the specific role and responsibilities of each of the components of the ICS structure.

Establishing SOPs for communications is also a good practice in emergency response (FEMA and USFA, 2000). In this case, SOPs may identify the exact procedures to follow given a certain emergency condition, including the personnel that needs to be contacted, the way in which it can be contacted (e.g., phone numbers), and the information that needs to be transmitted. According to the responses obtained from the AASHTO Security Forum survey, many State DOTs have developed or updated their SOPs to include notification procedures to be followed by DOT personnel. These SOPs are developed as a way to guide personnel through the specific steps required to communicate emergency related information, including how to report threats or any suspicious activities.

A common practice among emergency response agencies is the use of Emergency Notification Systems (ENS) to expedite the dissemination of emergency information. The use of ENS has been a common practice of 911 dispatch centers for years (911 Broadcast, 2004). In the simplest form, ENS consist of a central computer station in which a series of predefined call lists are activated by an operator once an emergency has occurred. The individuals included in the call lists are then contacted automatically by the system and given the desired information. Current Emergency Notification Systems on the market are capable of delivering and tracking the information relayed. In this way, a pre-recorded voice message with the

information can be delivered to the person included in the call list only if the individual answers the phone. After several attempts, the ENS will automatically try to make the contact with a secondary phone number if provided, and will keep track of who has received the message and who has not. This information is available to the user to make the necessary adjustments he/she considers appropriate. Many ENS can also be activated by the user over the phone, or access them via the internet (911 Broadcast, 2004; Microsoft, 2005).

Although ENS were originally conceived to support emergency management agencies, they are now applied in a variety of fields. Companies like the US Postal Service and AT&T have implemented ENS-type systems to support their operations (911 Broadcast, 2004). Emergency Notification Systems are also used by some schools to automatically disseminate any emergency-related information to school members and faculty. The research team found a number of ENS software applications available in the market today. Companies like Dialogic Communications, InterAct Public Safety Systems, Positron Public Safety Systems, and Virtual Alert Inc. offer software Windows-based applications to implement ENS for essentially any application (Microsoft, 2005).

4.3 Intelligent Transportation Systems - ITS

With the swift evolution of technologies in fields such as communications and electronics, and these becoming more accessible, their application in the transportation field has become increasingly common in transportation agencies across the US. The application of such technologies, referred to as Intelligent Transportation Systems (ITS), is aimed towards enhancing the operation and improving the efficiency of the transportation system. Examples of common ITS applications include:

- Advanced Traveler Information Systems that provide information directly to travelers, enabling them to make better route choices.
- Advanced Traffic Management Systems that employ a variety of detectors, sensors, and communication systems to monitor traffic in real-time.
- Incident Management Systems that use sensing technologies and detection devices that empower operators to respond quickly to accidents and other emergencies within the system (ITS America, 2005).

The events of 9/11 and the potential terrorist threat to the Nation's transportation system have stressed the appropriateness and importance of ITS as an effective tool to respond to Homeland Security incidents, even for cases in which the target of the attacks is not the transportation system itself. The use of ITS and ITS-related data has been proven to be a valuable resource for emergency response agencies in large scale incidents (e.g., Northridge earthquake in Los Angeles in 1994 and the 9/11 attacks in New York and Washington) (ITS America and USDOT, 2002).

A year after the events of 9/11, ITS America and the US Department of Transportation released *Homeland Security and ITS*, a document that presents new applications and special considerations of ITS to effectively manage terrorist events. This document builds from the fact that ITS can be applied by agencies to enhance capabilities in all stages of emergency management (Franklin, 2004; ITS America and USDOT, 2002) namely, mitigation, preparedness, response, and recovery. It outlines the way in which transportation agencies can consider this new threat in their current and future ITS applications. Although it can be difficult to refer to only one of these elements without making reference to the others, for the purpose of this research we focused specifically on those ITS initiatives intended to enhance highway emergency response.

As has been stated throughout this document, transportation agencies play a supportive role in the overall emergency management effort by performing tasks as required by the characteristics of the event. However, performing these supportive duties appropriately requires significant efforts both within the organization as well as with a number of external agencies. Intelligent Transportation Systems can be a very valuable tool to satisfy both of these requirements.

4.3.1 ITS and Emergency Response

As mentioned in Chapter 1 the unique characteristics of the transportation system make it especially vulnerable to the occurrence of major emergencies, including terrorist incidents. The transportation system will always be affected somehow, even if it is not the actual target of the attacks. While people may need to be evacuated out of the area affected by the incident, emergency responders need to arrive promptly at the incident site to undertake their activities. The transportation system plays a key role, because it is the means by which both of these tasks are performed. Its efficient operation becomes imperative during disasters.

Emergency management agencies and first responders can benefit significantly from the information that ITS technologies can obtain from the field on the status of the system. ITS can also allow these to benefit from the possibility of adapting the system to the ongoing situation and support emergency response as it evolves.

Although there exists a number of technologies that can be developed and implemented to support emergency response, it is important to highlight the fact that many of the existing ITS capabilities and infrastructure used for incident and traffic management may be directly applicable to enhance emergency management both directly within the transportation agency, as well as to support other agencies in their response activities (ITS America and USDOT, 2002). However, it is important

for transportation agencies not only to develop and adopt standard emergency procedures that guide the use of ITS during emergencies, but also to understand clearly how incidents are managed and how other agencies may benefit from ITS (Franklin, 2004; ITS America and USDOT, 2002). It is important to have the technologies available during the emergency, but it is vital to understand how they can be used to obtain the maximum benefit from them.

Many current ITS capabilities can be very useful during emergency response. Cameras and detection devices installed along freeways and major highways to monitor traffic can be used to support response activities within the transportation agency, as well as the activities of other actors involved. They can be used as a way to monitor the status of the transportation system during the response efforts, allowing operators to adjust the system in real-time as the events unfold (Franklin, 2004; ITS America and USDOT, 2002). This information can be relayed to emergency management agencies to support and coordinate all response activities.

When an incident occurs, emergency management agencies need to be able to communicate effectively to the public. Transportation agencies need to communicate to the users of the transportation system to inform them of the status of the current events and that of the transportation system itself. Communication with the public allows users of the system to make more knowledgeable decisions on what routes to take and avoid, and enables the agency to gain control and adapt the system to the evolving situation (e.g., prioritize traffic on evacuation routes).

The use of Dynamic Message Signs (DMS) to display information to the users on the status of the transportation system is currently a common practice for traffic management among transportation agencies. In large scale events, DMS can be also utilized to display emergency information to the users of the system. Nevertheless,

there needs to be a very careful and conscientious use of these systems when displaying security related information.

The FHWA has approved the use of DMS to display security related information by following standards similar to those established for other types of messages. However, it conditions this practice on the existence of policies and procedures that control the messages that are to be displayed (Paniati, 2003). According to the FHWA, these policies and procedures need to address a series of issues prior to implementation, such as (Paniati, 2003):

- The criteria under which DMS will be used for emergency or security messages, including the necessary coordination with public safety or security agencies.
- Protocols or hierarchy for prioritizing messages and determining which messages are to be displayed.
- Geographic area over which the information is to be displayed, to be determined in cooperation with public safety and security agencies.
- Identification of the circumstances under which transportation-related messages, such as lane closures, fog alerts, detours, or other messages that may be needed because of dangerous travel conditions in the immediate vicinity, would preempt emergency or security alert messages.
- The criteria that would cause the discontinuation of use of the DMS if the emergency or security alert message creates an adverse traffic impact, such as queues and markedly slowing traffic.

When applying ITS technologies to support security and emergency response, two basic issues emerge:

1. There is a need for transportation agencies to coordinate their activities with other agencies involved in the response efforts.
2. ITS-related information should be shared with other participating agencies to enhance emergency response.

Because ITS are usually implemented and operated by transportation agencies, the dissemination of ITS-information to/from other emergency response agencies constitutes one of the major obstacles to overcome. This obstacle is further aggravated when there is not a clear prior relationship between the agencies. Transportation agencies operating the transportation system may not be aware of what other emergency agencies are doing and will not know what information from ITS can be useful to support their activities. If no coordination exists, responding agencies may not even be aware of the wealth of information available to transportation agencies from ITS technologies.

The following section presents a way in which some local and state governments are currently attempting to reduce the gap between transportation agencies and emergency management agencies during a disaster.

4.3.2 Integration of Traffic Management Centers (TMC) and Emergency Operations Centers (EOC)

Intelligent Transportation Systems can be a very valuable tool to support emergency response for large scale events. However, due to a number of factors, transportation agencies that operate ITS normally have little interaction with

emergency management agencies in command for incident response (Hedden and Witzke, 2002). This translates into poor coordination between the two parties.

In order to overcome this obstacle, many local and State governments have considered the practice of integrating local and/or State EOCs and TMCs into one common facility where resources are shared between the two entities. This integration is considered to benefit both agencies and can enhance overall emergency response because it may (Hedden and Witzke, 2002, ITE and FHWA, 2004, ITE, 2004):

- Improve access to additional and better information for both EOC and TMC.
- Improve coordination of operations through day-to-day interaction of EOC and TMC personnel. This will translate into better coordination during emergency response.
- Reduce redundancies in infrastructure as both systems operate in the same facility.
- Reduce costs and duplication of efforts. To a large extent, the information and communications systems needed to operate each facility are fairly similar.

However, a major funding issue obstructs the feasibility of integrating both facilities. Not only are the sources of funding different, but the sizes of the budgets can be considerably unequal. Local EOCs may get funding from local governments, while a TMC may obtain resources from local, State, or Federal sources (Hedden and Witzke, 2002). In this way, sharing costs for the implementation and operation of an integrated EOC-TMC facility may be somewhat complicated.

Hedden and Witzke (2002) present two case studies on efforts to integrate EOCs and TMCs. The first case presented is the integration of Chicago's 911 call center (OEC) and the Chicago Traffic Management Center (CTMC). The second case is an

initiative taken by the Emergency Management Agency of Franklin County (EMAFC) in Columbus, Ohio and the Central Ohio Regional Transportation and Emergency Management Center (CORTAN). For the purpose of this research, it is important to expand somewhat on the second case.

As with most local Emergency Management Agencies, the EMAFC is in charge of developing emergency procedures and plans for the Franklin County region, especially those that deal with response to natural disasters. Due to continuing limitations in space, the EMAFC had considered the possibility of incorporating their facility into the City of Columbus EOC. At the same time, transportation planners were considering the development of a regional TMC in the area. In this way, both parties came together and decided to combine efforts by creating a joint facility in which all activities could be integrated. This facility is known as CORTAN and includes the participation of a number of agencies as shown in Table 4.8.

The integration favored both parties. On one hand, the EMAFC is now able to access information that was previously not available to them. For example, they can now access all cameras and DMS installed along the region's highway system to support their operations (Hedden and Witzke, 2002). The TMC on the other hand, improved their ability to coordinate their activities with local and regional emergency management agencies.

**TABLE 4.8 – CORTAN Participating Groups (Hedden and Witzke, 2002;
MORPC, 2005)**

Agency/Group	Participation
Ohio DOT	Columbus Metropolitan Freeway Management System
Franklin Co. Engineer	County and Suburban Traffic Signals and County Snow Plow Operations
Central Ohio Transit Authority	Radio Room and Dispatching Facility
City of Columbus, Public Service Department	City Traffic Signals Traveler/construction information. City Snowplow Operations
City of Columbus, Public Safety Department	Emergency Operations Center
Franklin Co. Emergency Management Agency	

4.4 Decision Support Systems

During an emergency, a large amount of information and data from a number of different sources may be available to responders. Based on this information and the training previously received, responders need to make the most appropriate decisions for the situation at hand in a limited amount of time. Resources have to be deployed in the most efficient way possible. However, how many and what resources should be deployed so to not compromise other operations? From what location should they be deployed? Who needs to be contacted given the present emergency conditions? Where and how can they be contacted? Exactly what information needs to be communicated? What is the standard procedure to follow for this type of emergency?

This decision-making process can be extremely complicated, especially when it has to be performed in real-time and under significant pressure. However, these characteristics are not unique to emergency response. Many other situations in which real-time decisions are required share many of the same limitations. As stated by

Laffey (Laffey, 1991), real-time problem solving tends to exaggerate many human limitations such as:

- Tendencies to overlook relevant information.
- Tendencies to respond inconsistently, to respond too slowly, or to panic when the rate of information is too great.
- Fail to effectively monitor all available information.
- Inability to resolve conflicting constraints.
- Cannot provide a solution quickly enough.

Since the advancement of computers and computing power in the late 1960's, researchers have been trying to imitate human behavior to support their activities in what is known today as the concept of Artificial Intelligence (AI) (Power, 2004). In this way, many emergency agencies have sought AI as a way to cope with the problem of decision-making during incidents, specifically to what is referred to as Decision Support Systems (DSS). DSS are computer-based systems developed to support human decisions by processing data provided as input from the exterior, and presenting the user with a set of proposed decisions based on the information supplied. The operator can then make use of the decisions provided by the system to make his/her own judgment. Figure 4.12 shows a representation of the logic around DSS.

Figure 4.12 – Decision Support System Diagram

One of the most common and yet simple DSS implemented today are Expert Systems (ES). As with DSS, Expert Systems attempt to capture the knowledge and experience of experts in a specific area into a computer system that can be accessed by non-experts in a timely manner. The knowledge of the expert is replicated into the computer by pre-defining a set of simple IF-THEN rules that have to be followed by the system to arrive at a final conclusion. The ES then interacts with the user by asking a series of questions. The answers to these questions are the input of the system. Depending on the answers, the ES will follow the IF-THEN rules and continue inquiring until a final conclusion can be obtained. Hence, non-experts can make decisions by emulating the interaction they will have if an actual expert was physically present.

Developing an ES today is a relatively simple task. In order to establish the set of IF-THEN rules that define the performance of the ES, the user needs what is referred to as an ES shell. Fortunately, there are many of these available on the market today. While some of these applications are offered for free and can be downloaded directly from the internet, other commercial tools can be quite expensive. These shells provide the user with the flexibility of creating an ES in relatively simple way.

In order to have a better understanding of how an ES can be developed, the research team investigated three of these shells: Corvid by Exsys Inc, Flex by Logic Programming Associates Ltd, and CLIPS, a free ES available in the internet. All of these shells were observed as being very flexible and relatively simple to use. However, Flex and Clips required the user to understand programming code in order to create the ES, which made them somewhat more difficult to develop. While Flex works in Prolog, Clips has its own programming language. On the other hand, Corvid comes with a Windows-based layout and a user friendly environment that enables the user to create the rules much more easily, because no coding is required. In any

of the cases, however, the conclusion was that the elaboration of a relatively complicated ES is a moderately simple task.

The use of ES is not new. There are practically thousands of ES today applied in a wide range of fields. Expert systems have been used for applications from medical diagnostics to the military, from monitoring the Hubble Space Telescope to commercial computer costumer support (Laffey, 1991; Slap, Hillman, and Moore, 1988). According to Slap, Hillman, and Moore (1988), expert systems can be considered by any kind of organization in which:

- A solution to a problem has a high payoff.
- Expertise is needed in many locations.
- Expertise is needed in hostile or hazardous environments.
- Cost maintaining expertise within the organization is high.
- Large amount of data must be examined in the decision-making process.
- An error in the decision-making process could lead to disastrous results.

With the above in mind, it is not surprising to find many ES that have been developed for emergency response applications. The characteristics of an emergency and the decisions that have to be made during the response efforts are ideal scenarios for the implementation of ES (Slap, Hillman, and Moore, 1988). Rules can be made that include the operating procedures for a predetermined set of emergency scenarios. Emergency operations plans, which are usually extensive documents, can be included in an ES in such a way that the user of the system is provided only with the relevant material required for a specific type of emergency. Sometimes it may not be appropriate for responders to spend time searching for information as an incident unfolds (De Vlaminck and Mampaey, 2003). Lines of communications and notification procedures, as well as contact information, can be stored to guide the

operator on whom to call and how to reach them. This allows for operators to obtain this information and guide the response efforts appropriately, even if the operator has little experience in these types of events. It is also a good solution in situations in which the personnel normally responsible is not available (e.g., sick or on vacation). ES can also serve as a way to track and log information, because all data used during the response can be stored in the system (Slap, Hillman, and Moore, 1988).

ES has also been found valuable as an emergency training tool. Sharit and Chen (1993) conducted a study that examined how an operator's knowledge of response procedures was affected when an ES was used for training purposes, and found that operators who receive training via ES were better prepared than those who did not. They concluded that when ES was used, it enhanced the ability of operators to capture and process the information, because these will follow the same rule-based structure used in the ES when facing an incident. This was found to be particularly helpful during emergency response.

With the advancement in technology, ES can now be integrated in large databases with real-time data acquired directly from sensing devices; optimization models from the field of operations research (e.g. Hypercube Queuing Model) can be implemented to guide the operator into making more efficient decisions; communication systems can be integrated to acquire and distribute information among responders; weather information can be included; and GIS mapping abilities among other capabilities to provide the operator with a powerful DSS to be used to assist during the decision-making process of emergency response. Furthermore, many DSS today can be web based, allowing multiple operators to access and update information from remote locations.

4.4.1 DSS in Emergency Response

A literature review was performed to find applications of DSS developed especially for emergency response. Although several of such applications were observed, two major DSS applications are worth mentioning for the purpose of this research. These are, namely, DSS for monitoring and responding to emergencies in industrial plants, and DSS for response to hazards and chemical spills. While the first application is especially relevant as it shows how DSS can be used by responders in an emergency response control facility, the second demonstrates how DSS can be applied by personnel to support their field activities.

4.4.1.a DSS for Emergencies in Industrial Plants

Decision Support Systems can be convenient for a number of different applications in multiple fields. As found in the literature, the use of DSS for emergency response in industrial plants has been proven to be a very convenient practice (Delic and Tanaskovic, 1988; Hasbach, 1995; Slap, Hillman, and Moore, 1988). Various papers have been written on this subject, especially during the 1980's, when several applications were developed for monitoring and guiding operators during emergencies in large scale industrial plants.

In this type of environment, operators in a control room may have to deal with a large amount of information coming from automatic sensing devices. Once an emergency occurs, the operator has to be able to identify exactly what the problem is and know exactly what to do in order to cope with the emergency effectively. However, this can sometimes overwhelm the abilities of the operators, because there may be a vast amount of data coming in from the processes. In addition, for emergencies that involve the risk of chemical or hazardous materials, it is important

for the operator to be able to control the incident in a timely manner. In this way, operators cannot spend time searching for information in manuals or other references. This can consume valuable time during the response efforts (De Vlaminck and Mampaey, 2003). For these types of scenarios, many industrial plants have adopted DSS as a way to enhance their response capabilities.

In the 1980's and 1990's, several initiatives were taken to develop DSS to assist operators of chemical plants during the occurrence of an emergency. Such efforts resulted in DSS such as PControl (Delic and Tanaskovic, 1988) and PlantSafe by Geosphere Systems (Hasbach, 1995; Slap, Hillman, and Moore, 1988), developed in the late 1980's and early 1990's, respectively. As an example of how DSS can be used today in emergency response, a brief description of each of these systems is presented below.

PControl is a DSS that monitors industrial processes in normal operating conditions and is capable of suggesting and/or making corrective adjustments to the system to obtain optimal system performance. The system was developed so that when unusual operating conditions are present in the system (e.g., unusual temperatures or pressures), it alerts the operator of the situation and provides precise information on the specific area of unusual activity. With this information, PControl asks the operator if an emergency situation is to be declared, or if further analysis of the information is required (Delic and Tanaskovic, 1988). If an emergency is declared by the operator, the system automatically alerts the proper personnel in the plant of the situation via communication devices such as pagers. The operator is then presented with a series of pre-specified procedures available to cope with the type of emergency detected by the system, and has to choose one of such procedures. Once a set of procedures is chosen, PControl automatically follows these procedures and alerts the operator of any further information available/required.

Once the emergency is under control, PControl will notify the personnel that the emergency is under control and will resume normal operations. In summary, a DSS like PControl is capable of identifying the problem, determining the extent of the problem, and executing corrective measures to handle the incident (Delic and Tanaskovic, 1988).

In the early 1990's, an ES called PlantSafe was developed to assist chemical plant operators in the event of an emergency (Hasbach, 1995). The rule-based expert system, which guided operators through emergency procedures as the situation developed, was complemented by information from gas dispersion models, digital maps, building and tank information, personnel records, notification lists, and other information valuable for emergency response (Slap, Hillman, and Moore, 1988). The system was developed as a way for operators to have better control of emergencies by providing the most complete information and tools for them to make knowledgeable decisions. In this way, information was readily available in a simple to use computer program rather than stashed away in filing cabinets or emergency plans (Hasbach, 1995). According to the PlantSafe website (CSM Inc, 2004), the system is currently implemented in chemical plants of major companies like Dow, Bristol-Myers Squibb, Rohm and Haas, Dupont, and Shell, and has been proven to be successful in their operations.

The PlantSafe system, originally designed for chemical plants, has been further developed into a Windows-NT-based system called 4Command that is now available for application by any organization that requires decision-making support in their operations. Figure 4.13 below shows a screen capture of the user interface of the 4Command system. The system consists of a series of windows for different purposes. The Cue Window at the bottom left is the interaction between the actual expert system and the operator. Data can also be automatically obtained by the

system through sensing devices. The 4Command system includes a knowledge base builder tool that enables the user to build particular sets of rules according to the specific application. Based on the options selected in the Cue Window, the system presents a set of recommendations for the operator to perform in the Recommendations Window. The operator will choose which of these actions to perform. The Status Board Window presents a continuous description of the status of the system (CSM Inc, 2004) by enabling the operator to observe and modify previous recommendations and decisions. It also keeps track of the different actions already performed and the time and date these were taken. Finally, the Mapping Window provides relevant drawings and maps for the operator to use during the emergency. Other information such as emergency procedures and plans can also be accessed through the system with the click of a mouse.

The 4Command system can be coupled with an automated notification system offered by the developers called TeleSafe (CSM Inc, 2004; Slap, Hillman, and Moore, 1988). This system enables the operator to automatically contact and alert the proper personnel included in pre-defined contact lists. The operator records the message and once it is delivered, can monitor the status of the calls (e.g., which of them were successfully received and which of them were not).

As can be seen from these two examples, DSS can be a very powerful tool to assist response activities by emergency control centers. DSS allows operators to manage emergencies in a more timely and effective way. Responders are provided with recommendations that guide them through the specific activities that need to be performed, reducing the possibility of human mistakes during incident response efforts. They can also reduce the time of response, because they can provide the operator with a significant amount of information otherwise difficult to obtain if at all available.

FIGURE 4.13 – PlantSafe - 4Command Screenshot (CSM Inc, 2004)

4.4.1.b. DSS for Response to Hazardous Material Spills

Another common DSS application found in the literature for emergency purposes was that for response to hazardous material spills. In these types of emergencies, the first minutes of the response efforts are especially critical. First responders need to be able to take the appropriate actions as rapidly as possible without compromising their own safety or that of the surrounding community. Due to the vast number of different chemicals and hazardous agents that can travel through the transportation system today, identifying the specific hazardous material in question

can be particularly difficult. However, many of the first responders that attend these incidents are not experts and still have to be able to take the proper measures to control the emergency (Lin and Biswas, 1991). In many cases, response efforts have to be delayed until experts arrive at the scene to assess the situation. This delay may be crucial for the success of the response and may increase the risk of undesirable consequences. A common application of expert systems, which addresses the problem of identifying and treating chemical agents during emergencies, was found in the literature review.

In these type of incidents, an ES can be of significant value to emergency responders, because response efforts will vary according to the agent present. For example, fires where chemical materials are involved are treated in different ways depending on the type of substance. However, identifying the material involved and the procedures that need to be followed to control the situation can be a difficult task. Expert systems have been found to be especially valuable in these cases, because they can assist responders in the identification of these materials and provide them with specific measures to follow to control the emergency. For example, ES can assist emergency responders in answering questions such as (Hushon, 1986):

- Which of the chemicals present represents the greatest human health hazard?
- What is the critical exposure route (e.g., inhalation)?
- If there is fire, what is the best extinguishing material?
- What equipment should be worn by personnel to protect against the chemicals present?
- Should population evacuation be considered?
- Is there a possibility of explosion?

- What are the likely symptoms of chemical poisoning from the substances present?

Many ES applications that assist responders in answering these types of questions were found in the literature (Hasbach, 1995; Hushon, 1986; Lin and Biswas, 1991; Rao, 1990; Wilson, Cantin, and Bisson, 1990). These types of ES are designed to be used by emergency personnel in the field. Most of the ES reviewed worked under the same basic structure. Given a certain hazardous spill, responders can access an ES by means of portable computer devices such as laptops or PDAs. The DSS queries responders on specific characteristics observed in the incident (e.g., is a fire present, or what is the flame color?) and based on the responder's answers, defines the particular type of chemical involved. The DSS then guides the responder on the appropriate procedures and protective measures that need to be considered for the agent in question based on the evidence provided.

For example, an ES found for hazardous spills called EMERG includes the following characteristics (Lin and Biswas, 1991):

- Guidelines for identification of the spilled material
- Provides the material properties
- Predicts the chemical concentration profile in the vicinity of a spill.
- Selects personal protective equipment.
- Recommends actions to handle the emergency
- Reports to the appropriate authorities

As can be seen by the previous example, the use of ES by field response personnel can be very beneficial. Decision Support Systems can provide non-experts in the field with information they could only obtain with the physical presence of a

specialist. Instead of having to wait for such specialist to arrive at the scene, responders equipped with DSS can obtain quick expert information on the field, reducing response time and the possible consequences related.

4.4.2 DSS in State DOTs

Decision Support Systems have been implemented in the field of emergency management for some years now. The two applications presented in Section 4.4.1 were merely examples of current applications of DSS in emergency response that illustrate how these relatively simple systems can enhance the capability of emergency responders. However, DSS can and have been applied in a number of different areas as tools to assist decision makers in the performance of various tasks. With this in mind, and considering the activities and responsibilities that transportation agencies are normally required to perform for emergencies, DSS appears to be an applicable and convenient tool for DOTs to support their incident operations.

For the purpose of this project, the research team investigated on current DSS applications in this area by State DOTs. A question regarding the use of DSS was included in the AASHTO Security Forum survey. The results are shown in Figure 4.14.

From the seventeen State DOTs that responded the questionnaire, ten (59%) responded they did not use any type of computer-based DSS to support their operations. Of these, only New Mexico DOT mentioned they had considered the use of such a system but after an evaluation they had finally decided not to develop one.

Five State DOTs (29%) said they did have some kind of DSS. However, none of these DSS were developed specifically for the DOT to support their internal organization for emergency response. All of the DOTs that answered affirmatively

said the systems they use (or will use) are those provided by their respective State Emergency Management Agencies. These systems, more than a DSS per se, are what are referred to in emergency management as Crisis Information Management Software (CIMS). CIMS are powerful computer-based tools used by many local or State EOC to manage all incident operations, including resource management, communications, information management, and incident follow-up (ICS status) (NIJ, 2002). In an effort to integrate activities in emergency response, many State Emergency Management Agencies provide responding agencies access to these CIMS. Some of these CIMS can be web-based, so information coming to and from these agencies can be shared among them in real-time, without them having to be together in a common facility.

FIGURE 4.14 – DSS State DOT Survey Response

The Department of Justice (NIJ, 2002) recently underwent a study in which ten of the most common CIMS currently implemented by emergency agencies were

compared with each other. The most common CIMS found by this study were Blue292, CRISIS, EM2000, E Team, Incident Master and InfoBook, OpsCenter, RAMSAFE, RESPONSE, SoftRisk, and WebEOC. In the responses obtained in the AASHTO forum, Maryland DOT mentioned they had access to WebEOC through the State EMA, and Oregon DOT said they used OpsCenter in a similar way.

In conclusion, based on the survey responses obtained, it can be said that the use of DSS by DOTs appears not to be a common practice. Most of the DOTs stated they did not use (or plan to use) DSS for emergency response. Furthermore, the systems used by DOTs are those implemented by State EMA for their EOC. There was no DSS found to be developed and implemented to support the DOT's internal activities during emergencies.

CHAPTER 5 - GUIDELINES FOR DEVELOPMENT OF INDOT EMERGENCY OPERATIONS PLAN

Although INDOT is not an emergency response agency per se, its level of involvement in emergency operations can be significant. INDOT may be requested by the State EOC to provide its resources (including personnel) to support emergency response and recovery efforts. In addition, INDOT has to be prepared to perform and accomplish the tasks outlined in the Indiana Comprehensive Emergency Management Plan (CEMP) (see Appendix A). This not only demands that INDOT's internal organization be fully prepared to perform these emergency responsibilities appropriately, but also be able to undertake them in a way that does not jeopardize its normal operations (e.g., traffic control and snow removal). In addition, INDOT has to be capable of integrating its activities within the overall statewide emergency management operations, including the coordination of activities with other State agencies (e.g., as primary agency of the Transportation Emergency Support Function in the CEMP).

Emergency response procedures in INDOT have usually evolved from previous experience in handling emergencies such as snow storms and tornadoes. INDOT personnel know whom to call and what to do based on procedures normally used during these types of emergencies. While this practice may have proven to be effective in the past, the terrorist threat imposed on the nation raises significant questions as to its appropriateness for emergency response to large scale incidents.

To enhance its emergency response capabilities, it is imperative for INDOT to develop and implement an Emergency Operations Plan (EOP), as required by the CEMP (SEMA, 2003). This EOP should initially consist of a written document that includes all the provisions required and the procedures INDOT personnel at all levels need to follow when responding to an emergency. As defined by FEMA (1996), an EOP should describe who will do what, as well as when, with what resources, and by what authority, before, during, and immediately after an emergency. This chapter presents a set of guidelines for the development of an EOP by INDOT, following the current state of the practice at the Federal and State level as presented in Chapters 2 and 3 respectively, and the review of best practices in Chapter 4. These guidelines are intended to be considered and followed by INDOT in the development of an internal EOP.

5.1. Considerations for Development of an INDOT EOP

The main objective of developing an EOP for INDOT is to establish all emergency response procedures and practices prior to an incident, in order to ensure proper operations during the actual response phase. An EOP should standardize the way emergency response is performed at the different levels of INDOT's organization, and still be flexible enough to be applicable to any type of incident. It should also consider the important relationship between INDOT and the statewide emergency management system, and incorporate procedures that will ensure all activities performed can be integrated and are compatible with emergency practices in Indiana. In order to accomplish these objectives, a set of emergency management principles and practices implemented by transportation agencies in the US need to be included. The following is a compilation of what the research team identified as the

basic principles and how these can be applied in the development of an EOP for INDOT.

5.1.1. All-hazards approach

An INDOT EOP should follow an all-hazards approach, one of the most important principles in emergency management (AASHTO, 2002a; DHS, 2004b; DHS, 2004c; FEMA, 2004). The basic idea behind this principle is for emergency management agencies to develop emergency procedures and practices that are applicable for response to any type of incident. Instead of developing different plans and procedures to apply for each different type of emergency, agencies develop a common plan with procedures that are applicable for any case. Specific considerations that may be required for particular incidents are included in annexes to the EOP. For example, any specific requirements for response to a terrorist incident are included in a terrorism specific annex to the EOP. Today, all Federal, state, and local emergency management agencies in the US are required to implement the all-hazards principle in their procedures (DHS, 2004b; DHS, 2004c; FEMA, 1996).

5.1.2 Follow Homeland Security Advisory System

As explained in Section 2.1, the Homeland Security Advisory System (HSAS) was created with the specific objective of establishing a centralized mechanism to communicate homeland security threat levels to the nation. Although the HSAS is directed towards Federal departments and agencies, Homeland Security Presidential Directive 3 encourages state and local entities to adopt the HSAS and develop a set of protective measures that follow the national threat level. Many DOTs have followed this initiative and established their own protective actions (FHWA, 2002).

The research team suggests that INDOT develop a set of preventive and protective actions that considers measures to be taken at all levels of the organization (i.e., Central Office, Districts, Subdistricts, TMC) for each level of the HSAS. These measures are to be included in the INDOT EOP.

The FHWA (2002) developed a survey to obtain information on the specific measures transportation agencies in the US are taken under the different levels of the HSAS, and released a compilation of the information obtained. INDOT can build on the information presented in that report to develop its own set of measures.

5.1.3 Integration and Interoperability

An INDOT EOP must ensure interoperability and proper integration of activities with the statewide response efforts. As has been stressed throughout this document, INDOT is just one of several agencies involved with a common response objective. Emergency response may require INDOT to interact with other state agencies like the Indiana State Police, SEMA, and the Department of Natural Resources. With this in mind, procedures included in the INDOT EOP must be compatible with the activities of other agencies.

In this regard, it is advisable for INDOT to strengthen its relation with SEMA (or IDHS) to ensure that its practices are compatible and interoperable with other Indiana agencies. Moreover, INDOT may ask for SEMA (or IDHS) to have a significant level of involvement when developing the INDOT EOP to further assure its integration within the State's practices.

5.1.4 Redundancy and Continuity of Operations

When developing an INDOT EOP, special consideration must be placed on ensuring a certain level of redundancy in the emergency response capabilities

defined in the EOP. That is, INDOT must ensure, to some reasonable extent, that it will be able to perform its response activities even if there is a disruption in the system. For example, if the radio system is down, a secondary system must be considered in the EOP to be used as a way to ensure proper communications.

This concept of redundancy is known in emergency management as Continuity of Operations (COOP). In this framework, emergency agencies must anticipate the possibility of incidents affecting their essential operations during emergencies, and should plan accordingly.

For INDOT, special provisions in the EOP should be made to include contingency procedures due to (1) inability to use facilities, (2) loss of power, (3) loss of communications, (4) unavailable personnel, or (5) inaccessible information technology systems (TRB, 2005). Furthermore, the CEMP (SEMA, 2003) mandates that all Indiana agencies in the state plan incorporate procedures to ensure continuity of operations. (Refer to Section 5.1.e.)

A joint project between the TCRP and NCHRP (TRB, 2005) that is expected to be released soon will guide transportation agencies in including and developing COOP planning into their emergency plans. INDOT should consider using this report in the future to incorporate COOP into the EOP.

5.1.5 Personnel Safety

Considering that chemical and biological agents may be used in a terrorist incident, protection of INDOT personnel is to be considered as one of the most important elements in any emergency. Although INDOT personnel are not expected to act as first responders, the fact that many of its employees are in continuous contact with the highway system gives them some risk of exposure. Significant effort

must be placed when developing an INDOT EOP to consider the safety of INDOT personnel both prior to and during the response.

When asked what actions were taken to protect DOT personnel from exposure to chemical/biological agents, 13 out of the 17 (76%) DOTs responding to the AASHTO Security Forum Survey mentioned at least one of two activities: (1) awareness training in chemical/biological agents and (2) the implementation of personal protective equipment for DOT personnel.

5.1.6 Compliance with Federal and State Requirements

When developing an EOP, INDOT should pay particular attention to complying with all legal requirements of the Federal and State government, in particular those included in the NIMS and the CEMP.

Initial NIMS compliance requires that all INDOT personnel who may be assigned to the ICS established at the scene have basic knowledge of ICS principles. This initial requirement is fulfilled by taking the IS-700 National Incident Management System course, available on FEMA's website. However, according to SEMA's Preparedness Director, future requirements may involve compliance with other NIMS components, like interoperability of communications and resource typing, as explained in Section 2.2. At the time this document was written, SEMA was preparing a statewide NIMS Implementation Plan that will outline the process the state will use to implement NIMS in Indiana emergency management. This plan will propose a single point of contact between each state agency and SEMA, as a way for SEMA to provide technical assistance and guidance in ensuring compliance with NIMS requirements.

The CEMP has additional requirements. According to the state plan, all state agencies and departments included in the CEMP must have Standard Operating

Procedures in place to be used during emergencies. At a minimum, these SOPs should include procedures for (1) the designation of lines of succession and delegating authority, (2) the preservation of records, (3) the relocation of essential departments, and (4) the deployment of essential personnel, equipment, and supplies (SEMA, 2003).

The CEMP also requires agencies to designate a State Agency Emergency Management Coordinator (and two backups), who will act as the coordination point of the agency during emergencies (i.e., in the State EOC). In the case of INDOT, those contacts have been already designated. However, it is important for INDOT to further strengthen its relation with SEMA and other state agencies involved, so that interaction with external parties does not occur solely during emergency exercises, or worse, only during the actual emergency. In addition, information on emergency management and transportation security is constantly emerging and Federal and state procedures and requirements are constantly evolving. INDOT must be aware of such information to ensure compliance with legal requirements and proper emergency preparedness levels.

The research team suggests that INDOT designate a permanent position within its central organization, with the responsibility of handling all emergency management activities. This position can be responsible for doing a continuous follow-up on all emergency management information, both at the national and state levels. He/she will be in charge of monitoring information on new practices in emergency management and transportation security. Having an emergency management position at INDOT can also ensure and maintain a closer relation between INDOT and SEMA, which will benefit both parties. In this way, INDOT can enhance its emergency response capabilities and be continuously kept up to date on the state of the practice of emergency management in Indiana. This INDOT position

can also be responsible for performing periodic exercises and training sessions, and can be delegated with the task of developing, maintaining, and updating the INDOT EOP as appropriate.

5.2 Application of NIMS-ICS for INDOT in Emergency Response

As mentioned in Chapter 2, the NIMS designated the ICS as the standard operational system to be used by all emergency agencies in the US. Section 4.1 presented an overview of the ICS, its basic principles and operational standards as established by the NIMS. Based on what we have observed during the development of this project, the research team has identified the ICS and its principles as important organizational elements that can be adopted by INDOT to organize and coordinate emergency response activities within the different levels of its organization.

Although intended for emergency response agencies, Section 4.1.9 showed how ICS has been adapted and implemented by many State DOTs across the US (AASHTO, 2002a). In addition, the NIMS now requires all agencies involved in emergency management to adopt the ICS as their basic system for emergency response to be eligible for Federal preparedness grants (DHS, 2004b; FEMA, 2004). According to SEMA, this condition will only affect INDOT initially in that basic training on ICS will be required for all INDOT personnel that may be involved in emergency response. However, based on INDOT's current capabilities, highlighted during the November mock drill, the research team recommends that INDOT coordinate its internal activities by adopting an ICS-type organization for emergency response.

This section proposes a version of such a system that follows the NIMS principles, which can be adopted by INDOT Districts and INDOT Central Office. The proposed structures will not only enhance the management of activities within each of the

organizations, but will also enable the INDOT Districts and Central Office to coordinate their activities during emergencies and integrate effectively with the statewide response. Furthermore, an ICS-type structure can be applied in response to any type of emergency, that is, it will follow the all-hazards approach recommended by emergency management experts. The organizational structure will expand and contract, depending on the type of incident and how it evolves. The required ICS training dictated by the NIMS will further enhance INDOT's capabilities and reaffirm the ICS basic principles applied in the ICS-type systems proposed.

5.2.1 ICS-type structure for INDOT Districts

Section 3.4 presented some of the issues observed in the current emergency response capabilities of INDOT Districts. These issues included the existence of unclear lines of authority and communication within the district organizations. As presented in Section 4.1, the ICS has been proven to be an effective tool to organize emergency response activities. Basic ICS principles presented in Table 4.1, such as the modular organization, the concept of unity of command, and the unified command structure under which ICS builds, can be valuable in addressing these issues. With this in mind, an ICS-type structure like the one shown in Figure 5.1 is proposed for adoption by INDOT districts. The positions shown in parentheses in Figure 5.1 are examples of how each spot within the structure can be filled with positions within the District*.

* At the time this document was written, INDOT was undergoing major organizational restructuring at all levels. The research team was advised by INDOT not to designate specific positions for the District ICS structure because these were expected to change in the near future. Positions shown in Figure 5.1 are examples based on the Seymour District Emergency Plan (INDOT, 2004).

FIGURE 5.1 – Proposed ICS-type structure for INDOT District EOC*

* At the time this document was written, INDOT was undergoing major organizational restructuring at all levels. The research team was advised not to designate specific positions for the District ICS structure because these were expected to change in the near future. Positions shown in Figure 5.1 are examples based on the Seymour District Emergency Plan (INDOT, 2004).

Once an emergency has been declared, each INDOT District will activate a District EOC that will operate following the District ICS structure explained in this section, and will expand or contract to adapt to the specific requirements of the incident. This organizational structure should be activated and maintained throughout the response effort until the emergency is over. The specific procedures that need to be followed for the activation and deactivation of the District ICS should be included in the SOPs, as explained in Section 5.3.

The ICS-type structure for each district will start with the District Incident Commander (DIC). Following ICS principles, the DIC is the person in charge of all aspects of the response within the district. He/she is the person responsible for the overall response activities undertaken by the district. The DIC's responsibilities can include those shown in Table 5.1.

TABLE 5.1 – District Incident Commander Responsibilities

District Incident Commander Responsibilities
<ul style="list-style-type: none">• Establish and monitor district incident organization.• Maintain continuous contact with INDOT EOC representatives and Central Office as appropriate, for coordination of activities.• Establish immediate priorities especially the safety of responders DOT personnel• Determine incident objectives and strategy to achieve the objectives.• Coordinate activities for all staff under the incident organization.• Coordinate with key people and officials.• Approve requests for additional resources or for the release of resources.• Order the deactivation of the incident when appropriate.

The standard ICS includes the possibility for the Incident Commander to activate a series of support positions under the Command Staff (i.e., the Information Officer, the Liaison Officer, and the Safety Officer). This is usually the case for large scale

incidents or incidents that require special considerations in a specific area (e.g., an incident that represents a high risk for personnel may require a Safety Officer) (DHS, 2004b; FEMA, 1998; OSHA, 2004). For the specific case of the INDOT Districts, however, the District ICS organization proposed is relatively simple and will consist of few positions. In this way, the DIC can be expected to perform these tasks appropriately and considering extra positions under the Command Staff may not be required.

An Operations Section is activated by the DIC for incidents that require specific involvement of INDOT resources, including personnel. In the same way as with standard ICS, a District Operations Section Chief is assigned to this section. This Chief's main responsibility is the supervision of all operations undertaken by personnel from the INDOT District. This includes determining the need and request for additional resources to perform all operational activities under the district's responsibility.

Depending on the incident and the type and number of activities that the district is required to perform, the resources assigned to the Operations Section of the district can be further broken down into Divisions or Groups. The decision to use Divisions or Groups depends on the incident at hand. For example, the use of Divisions can be convenient in incidents that require several INDOT Subdistricts involved in the operations. In this case, resources assigned by each Subdistrict can be organized by activating a Division for each of the Subdistricts involved. This is particularly useful when resources want to be tracked by Subdistrict. In addition, it allows for a better understanding of the chain of command, because the current non-emergency structure of each district can be maintained in emergencies. On the other hand, for incidents that require several activities to be performed by a specific INDOT District, it may be more appropriate to organize resources by the function

they perform. For example, all resources assigned for debris removal can be assigned under the Debris Removal Group under the Operations Section. In either case, the procedures required to expand and contract the Operations Section should be included in the SOPs.

A Planning Section is also considered in the District ICS proposed as shown in Figure 5.1. As with any ICS section, a Planning Section Chief is assigned as the overall planning authority. The Planning Section Chief is responsible for all planning necessary for the correct performance of the activities assigned to the District. For the case of a District ICS, not all the tasks assigned to the Planning Section and the respective Planning Units mentioned in section 4.1 are applicable. Only the tasks of the Resources Unit, the Situation Unit, and the Documentation Unit may be required (refer to Table 4.4). However, assigning individual units under the Planning Section as proposed by standard ICS may not be necessary in most cases. It is expected that for most incidents the Planning Section Chief is capable of performing all these tasks. If the characteristics of the incident require extensive planning efforts, one or more of these units can be activated.

Table 5.2 shows the responsibilities assigned to the Planning Section of the District ICS. Among these tasks, one of the most important consists of maintaining the status and tracking of all district resources assigned to the response effort. This way, the District is able to locate and establish the specific tasks its resources are performing. Another important task is the elaboration of the Incident Action Plan (IAP). (Refer to Section 4.1.5.) For the specific case of a District ICS, one may expect the IAP to be commonly established orally rather than written. Having a written plan is more convenient in large scale incidents where a significant number of personnel are assigned to the ICS. In the case of a District ICS, establishing an oral IAP may be sufficient. In any case, the DIC and the Planning Section Chief have to

make sure the incident objectives are clear among all the participants within the District ICS.

TABLE 5.2 – District ICS Planning Section Responsibilities

District ICS Planning Section Responsibilities
<ul style="list-style-type: none">• Collect and process situation information about the incident.• Keep track of the current location and status of all assigned resources from the district.• Collect, process, and organize ongoing situation information.• Develop projections and forecasts of future events.• Prepare maps.• Gather and disseminate information and intelligence for use in the IAP.• Maintain accurate and complete incident files, including a complete record of major steps taken to resolve the incident.• File, maintain, and store incident files for legal, analytical, and historical purposes.• Prepare the IAP.

A Logistics Section can also be activated as a part of the District ICS structure as shown in Figure 5.1. Although the ICS considers six possible units that can be activated within the Logistics Section, for the case of the activities INDOT Districts may be required to perform, only those of the Supply Unit are expected to be necessary. Thus, the Logistics Section of the District ICS structure will be responsible, if necessary, for acquiring and managing all resources required, in addition to those within the District, to support their emergency response activities. For example, if the resources available within a District are not sufficient to perform the response activities appropriately, the District may have to request additional resources from other Districts. The Logistics Section of each District will be responsible of the request and management of these external resources.

A Finance/Administration section is proposed to be implemented within the District ICS structure as shown in Figure 6.1. This section will mainly be responsible

for performing the duties assigned to the Cost Unit as stated in the ICS. These include the estimation, recording, and analysis of all costs incurred by the District during the different stages of the response efforts.

5.2.2 Lines of Communication/Coordination

Figures 5.2, 5.3, 5.4, and 5.5 show the lines of communication/coordination expected for four different response scenarios, each one representing a different level of involvement of the INDOT districts in the response activities. The four cases considered are:

Case 1. Single incident handled by one INDOT District (Figure 5.2)

Case 2. Single incident handled by two INDOT Districts (Figure 5.3)

Case 3. Two separate incidents handled by two INDOT Districts (Figure 5.4)

Case 4. Single incident handled by one INDOT District with support provided by a second INDOT District (Figure 5.5).

These figures show how the coordination of activities of the districts is accomplished directly through the INDOT representatives located at the State EOC, with INDOT Central Office providing any support required. Note that no lines of communication are shown directly linking the different districts. This allows the INDOT representatives at the State EOC to coordinate activities effectively. Direct communication between the districts (as often happens in real emergency operations), may be acceptable if up-to-date information on the actual status of operations is made available to the representatives at the State EOC.

FIGURE 5.2 – Case 1. Lines of communication/coordination for an incident handled by INDOT District A

FIGURE 5.3 – Case 2. Lines of communication/coordination for an incident handled by INDOT District A and INDOT District B

FIGURE 5.4 – Case 3. Lines of communication/coordination for two separate incidents handled by INDOT Districts A and B

FIGURE 5.5 – Case 4. Lines of communication/coordination for an incident handled by INDOT District B with additional resources from INDOT District A

5.2.3 Area Command-type structure for INDOT Central Office

The channels of communication/coordination presented in Section 5.2.2 are appropriate for incidents in which INDOT's level of involvement is not significant enough to overwhelm the capacity of the INDOT representatives at the State EOC. However, large-scale incidents (e.g., terrorist attacks) may demand extensive participation by INDOT, with the possibility of considerable amounts of INDOT resources being deployed. In addition, the possibility of simultaneous incidents occurring in different geographical locations may require the participation of several INDOT districts, for which proper coordination of activities is required. For large-scale emergencies, the capacity of the INDOT representatives at the State EOC to coordinate all aspects of the response directly with the districts may not be adequate.

For large-scale incidents, the research team suggests that INDOT Central Office act as the coordination point of all internal activities, as shown in Figure 5.6. This follows the concept of Coordination Entities used in the NRP as explained in Section 2.3. Once an emergency in which the capacity of the INDOT representatives at the State EOC is expected to be overwhelmed, an INDOT Central Office EOC can be activated to coordinate INDOT's overall activities. This coordination can be organized by adopting and following the concept of Area Command used by emergency management agencies and included in the NIMS, as explained in Section 4.1.8. Adopting such a structure allows INDOT's Central Office EOC to manage overall emergency response in INDOT's districts, by coordinating the response that each District ICS will provide. The specific procedures to activate the Central Office EOC should be included in the SOPs.

A possible Area Command-based structure that can be implemented in INDOT's Central Office EOC is shown in Figure 5.7. The positions shown in parentheses are

examples of how each spot within the structure can be filled by positions within the Central Office*.

FIGURE 5.6 – INDOT Central Office as Internal Coordination Point

Figure 5.7 –INDOT Central Office EOC*

* At the time this document was written, INDOT was undergoing major organizational restructuring at all levels. The research team was advised not to designate specific positions for the Central Office EOC because these were expected to change in the near future. Positions shown in Figure 5.7 are merely examples based on our observations and judgment.

Table 5.3 shows the general responsibilities assigned to each of the elements included in the INDOT Central Office EOC. As mentioned in Section 4.1.8, the Critical Resources Unit Leader, the Situation Unit Leader, and the Public Information Officer positions are only activated when considered necessary. If the incident does not require these positions to be activated, the tasks assigned to the Critical Resources Unit Leader and the Situation Unit Leader can be adopted by the Logistics Section and the Planning Section, respectively.

Table 5.3 - INDOT Central Office EOC Responsibilities

Position	Responsibilities
Central Office Area Commander	<ul style="list-style-type: none"> • Overall management and supervision of District EOCs (ICSs) • Ensure possible conflicts are identified and resolved. • Set overall INDOT objectives. • Select strategies for the allocation and use of INDOT resources.
Planning Section	<ul style="list-style-type: none"> • Collection of information from District EOCs • Assess and evaluate potential conflicts.
Logistics Section	<ul style="list-style-type: none"> • Effective allocation of INDOT resources among District EOCs.
Critical Resources Unit Leader (if necessary)	<ul style="list-style-type: none"> • Track and maintain status and availability of INDOT resources assigned by each District EOC.
Situation Unit Leader (if necessary)	<ul style="list-style-type: none"> • Monitor status of objectives of each District EOC.
Public Information Officer (if necessary)	<ul style="list-style-type: none"> • Point of contact for the media.

5.2.4 Lines of Communication/Coordination with INDOT Central Office EOC Activated

When the INDOT Central Office EOC is activated, the lines of communication presented in Section 5.2.2 are modified to include this coordination point. Figures 5.8, 5.9, 5.10, and 5.11 show how these lines of communication/coordination are modified for each of the four cases presented in Section 5.2.2. The top part of each of these figures shows the lines of communication before the Central Office EOC is activated. The bottom portion shows how these lines are modified once the Central Office EOC is activated.

For Case 1, notice how the activities performed by District A are now coordinated with the State EOC through the INDOT Central Office EOC. The activation of the Central Office EOC may not be generally necessary in emergencies with this type of response, where there is only one district involved. In these cases, coordinating activities directly from the State EOC may be sufficient. However, large-scale emergencies in which the Central Office needs to be involved in the coordination and supervision of activities may require an active Central Office EOC.

Figures 5.9, 5.10, and 5.11 show how all coordination of activities of the districts involved, including the assignment of resources from other districts, is coordinated directly by the Central Office EOC once it is activated. This ensures that the integrated effort of Districts A and B follow the overall objectives defined by INDOT for the emergency, and that these efforts are coordinated with the overall statewide effort in the EOC.

In conclusion, a series of principles underlie the overall coordination of activities, both internally and externally, once the Central Office EOC is activated:

- Information to/from the State EOC goes through the INDOT Central Office EOC.

- Information to/from the INDOT Districts goes through the Central Office EOC and, as necessary, is relayed to the State EOC.
- Coordination (e.g., for allocating resources) required between INDOT Districts is to be coordinated through INDOT Central Office EOC following the principles of AC.
- INDOT Central Office EOC will act as the coordination point for all INDOT emergency response activities. It will define priorities and will ensure that no conflicts arise between the activities of the Districts and the statewide response efforts.

FIGURE 5.8 – Case 1. Modification of lines of communication/coordination for an incident handled by INDOT District A with INDOT Central Office EOC activated

FIGURE 5.9 – Case 2. Modification of lines of communication/coordination for an incident handled by INDOT District A and INDOT District B with activated INDOT Central Office EOC

FIGURE 5.10 – Case 3. Modification of lines of communication/coordination for two separate incidents handled by INDOT Districts A and B with INDOT Central Office EOC activated

FIGURE 5.11 – Case 4. Lines of communication/coordination for an incident handled by INDOT District B with additional resources from INDOT District A with INDOT Central Office EOC activated

5.3. INDOT EOP Structure

The basic principles and organizational elements presented in Sections 5.1 and 5.2 constitute the basis for the development of an INDOT EOP. The EOP is a written document that includes all the procedures INDOT personnel at all levels need to follow when responding to an emergency. Consequently, an INDOT EOP needs to be carefully developed in a way that allows personnel to have all the required information and still be simple enough to quickly absorb its contents.

As a way to guide state and local emergency management agencies in developing EOPs, FEMA released the *Guide for All-Hazard Emergency Planning* (FEMA, 1996). According to this document, there is no definitive format to use when developing an EOP, as long as the final users of the plan can understand it, are comfortable with it, and can use it to extract the information they need. However, most DOT EOPs try to mirror the basic structure used by state emergency management plans in the US (AASHTO, 2002a). These structures usually consist of a general section or Basic Plan that defines all general planning considerations and procedures involved in the DOT emergency response, and a series of sections and annexes that describe responsibilities and operational tasks at a greater level of detail (AASHTO, 2002a; FEMA, 1996). The research team suggests that INDOT use a similar structure to develop their internal EOP. This section presents a general overview of the structural elements that can be considered to develop an INDOT EOP, as an aid to INDOT personnel when developing the actual plan. The elements proposed are based on FEMA's guidelines in *Guide for All-Hazard Emergency Planning* (FEMA, 1996) and AASHTO's recommendations in *A Guide to Updating Highway Emergency Response Plans* (AASHTO, 2002a).

5.3.1 Basic Plan

The Basic Plan is an overview of INDOT's emergency response organization and the policies that govern all response activities. Table 5.4 shows the basic elements and a description of the contents that may be included in an INDOT EOP.

Table 5.4 – Elements included in INDOT EOP Basic Plan

BASIC PLAN	CONTENTS
Purpose	<ul style="list-style-type: none">- State objective of plan
Planning Assumptions	<ul style="list-style-type: none">- Planning considerations- All-hazard approach- Integration with statewide efforts- NIMS, NRP, and CEMP are effective.- INDOT facilities are operational.
Organization	<ul style="list-style-type: none">- Organization based on NIMS-ICS- Organizational elements included (i.e., State EOC, Central Office, Central Office EOC, and District EOCs)- Lines of authority.
Roles and Responsibilities	<ul style="list-style-type: none">- INDOT general responsibilities during response (i.e., support to CEMP)- Roles and responsibilities of each element of response structure (i.e., State EOC, Central Office, Central Office EOC, and District EOCs) and each of the elements within the ICS, with backups.
Concept of Operations	<ul style="list-style-type: none">- Activation procedures of INDOT EOP- Lines of communication/coordination- Notification procedures- Communications Plan

5.3.2 Continuity of Operations Plan

In order to ensure redundancy in INDOT's operations, a Continuity of Operations (COOP) Plan is recommended to be included as a section within the INDOT EOP. As explained in Section 5.1.4, the COOP plan will address all necessary precautions and

internal measures that need to be implemented after a disruption in INDOT's normal operations. The COOP plan should address contingencies to be able to perform all essential emergency tasks in case of (1) inability to use facilities, (2) loss of power, (3) loss of communications, (4) unavailable personnel, or (5) inaccessible information technology systems (TRB, 2005). TCRP project J-10F to be released soon will guide transportation agencies in developing and including COOP plans into their EOPs. The TCRP project can help INDOT incorporate a COOP into the development of its EOP.

5.3.3 Standard Operating Procedures

As a way to standardize response capabilities at the different levels of INDOT's organization, an INDOT EOP should include a set of SOPs that will guide its personnel in performing all emergency response activities. In this way, INDOT personnel will know exactly what specific steps to follow for a given emergency response task. According to FEMA (1996), SOPs should be designed in a way that enables personnel to quickly extract the information required. A common practice is to include them in the EOP as separate sections for quick reference, and present them in a checklist format for personnel to follow. SOPs can be supplemented with maps and other reference material. Table 5.5 presents some of the SOPs that may be included in an INDOT EOP.

Table 5.5 – Standard Operating Procedures for INDOT EOP

Standard Operating Procedures	Description
Notification procedures	Notification procedures (including call lists) for Central Office, Districts, TMC, State EOC, and external agencies like ISP and SEMA.
Resource management	Procedures for allocation and tracking of INDOT resources.
Activation of response elements	Activation and deactivation procedures of State EOC INDOT representatives, Central Office EOC, and Districts EOC.
Road Closure	Considerations and measures for closing roads, including notification procedures to ISP.
Evacuation	Evacuation routes
Traffic Management	Procedures for traffic control during emergencies (e.g., timing plans for evacuation and/or emergency response routes)
Inspection of transportation infrastructure	Structural assessment of bridges, overpasses, and highway intersections.
TMC emergency operations	DMS contents for different types of emergencies. Integration with State EOC (notification procedures).

5.3.4 Hazard-specific Plans

Hazard-specific sections of an EOP address any issues peculiar to certain types of emergencies, but that are not applicable to the rest of the EOP. In order to create hazard-specific plans, INDOT must consider the different types of incidents that may pose threats to Indiana's transportation system, and the countermeasures that need to be put in place for these events. According to AASHTO (AASHTO, 2002a), typical DOT EOPs include hazard-specific annexes for emergencies such as earthquakes, radiological incidents, HAZMAT incidents, hurricanes, snow/ice, mass gathering, and terrorism.

5.3.5 Protective Measures for Different Levels of HSAS

A section that defines internal protective measures following the HSAS should be developed within the INDOT EOP. This section will address specific actions that need to be implemented at the different levels of INDOT according to the threat level on the nation's advisory system.

CHAPTER 6 - CONCLUSIONS AND FUTURE RESEARCH

The events of 9/11 highlighted the need for transportation agencies to review, revise, and update their existing emergency response procedures to include appropriate provisions within the new terrorist threat imposed on the nation. Since then, significant effort has been placed by public and private organizations in developing information that will guide State DOTs in enhancing their emergency response procedures. In addition, Federal measures have been put into place as a way to enhance emergency management at the national level. These efforts' main focus is on standardizing emergency management procedures among the different actors involved, whether these are Federal, state, local, or private organizations.

In the specific case of INDOT, special attention needs to be placed on updating its current emergency response practices to ensure these are integrated and up-to-date with the practices in place by emergency agencies at all levels. This includes the need for INDOT to develop an Emergency Operations Plan that establishes all provisions required and the procedures INDOT personnel at all levels need to follow when responding to an emergency. This INDOT EOP should describe who will do what, as well as when, with what resources, and by what authority, before, during, and immediately after an emergency (FEMA, 1996). The INDOT EOP should follow certain principles and considerations to ensure it is integrated with emergency management practices of other disciplines. The procedures included should consider following an all-hazards approach, ensure proper integration and interoperability, and redundancy and Continuity of Operations. It should also have provisions to ensure INDOT personnel safety both prior and during the response efforts. In addition, all procedures included in an INDOT EOP should comply with Federal and State emergency management requirements like those outlined in the National

Incident Management System and the Indiana Comprehensive Emergency Management Plan, respectively.

INDOT should also consider adopting the Incident Command System as its organizational structure for emergency response operations. After the NIMS was released by the DHS, state and local agencies were required to adopt the ICS to be eligible for Federal preparedness grants. To fulfill this requirement, all agency personnel that may be required to work in the ICS established at the incident needs to be trained in ICS basics. This is accomplished by taking the IS-700 National Incident Management System course, available on FEMA's website. However, adapting the ICS as presented in Section 5.2 would allow INDOT to have a flexible organizational structure that can adapt to the specific requirements of any emergency. INDOT will also be able to build upon a system that has been used since the 1970s by emergency response agencies and is now considered to be the standard system for incident management (DHS, 2004b).

The guidelines presented in this document are intended to be merely recommendations for consideration by INDOT in their future security initiatives. Although interaction between INDOT and the research team was maintained during this project, the adoption of any of the actions described in this document will require further discussion and refinement by INDOT.

As presented in Chapter 4, ITS can be a very valuable resource for emergency response, not only for INDOT itself, but for other emergency agencies. Valuable information can be obtained from ITS technologies deployed in Indiana's highway systems. Further research may be required to identify any specific requirements INDOT's current ITS capabilities may need to fully exploit their potential for support to emergency response. A possible practice may be to strengthen the relationship

between the INDOT TMCs and the State EOC, and even physically integrating their facilities.

Another area of future research is that of Decision Support Systems (DSS) as support for INDOT emergency response. Section 4.4 presented some examples of existing applications and outlined some of the benefits of using such systems. Possible applications of DSS in INDOT may include the design of a DSS that can guide personnel step by step through the specific procedures that need to be followed for different response scenarios. The set of Standard Operating Procedures outlined in Table 5.5 can be included in such DSS. INDOT personnel can then make appropriate decisions based on the output obtained from the DSS.

LIST OF REFERENCES

9/11 Commission (2004), *The 9/11 Commission Report*, National Commission on Terrorist Attacks Upon the United States, July 22, 2004.

911 Broadcast (2005), *Emergency Notification Services*, 911 Broadcast website.

< http://www.911broadcast.com/psemergency_phone.htm >

[Consulted April 2005]

AASHTO (2002a), *A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents*. AASHTO, May 2002.

AASHTO (2002b), *National Needs Assessment for Ensuring Transportation Infrastructure Security*, American Association of State Highway and Transportation Officials, October 2002.

AASHTO and TRB (2002), *AASHTO/TRB Security and Emergency Response Survey of State Transportation Agencies*, AASHTO and TRB, January 2002.

Boyd, Annabelle and John P. Sullivan (2000), *Emergency Preparedness for Transit Terrorism*, TR News 208 May-June 2000.

Bush, George W. (2003a), *Homeland Security Presidential Directive - 3*. The Whitehouse webpage.

< <http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html> >

[Consulted January 2005]

Bush, George W. (2003b), *Homeland Security Presidential Directive - 5*. The Whitehouse webpage.

< <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html> >

[Consulted January 2005]

CSM Inc. (2004), *Critical Situation Management's 4Command Product*, Critical Situation Management Inc. website.

< <http://www.geospheresystems.com/product/plantsafe.html> >

[Consulted May 2004]

C-TASC (2003), *Indiana's Strategy for Homeland Security*, Indiana Counter Terrorism and Security Council, January 2003.

De Vlaminck, Michel and Lucas Mampaey (1989), *Operator Advisor: An Expert System to Help Deal With Emergencies*, Nuclear Engineering International November 1989 p32-33.

Delic, K.A. and N.Z. Tanaskovic (1988), *Designing a Knowledge-Based Emergency Control*. Control Engineering. September 1988 p268.

DHS (2004a), *Homeland Security Operations Center*, press release July 2004.

<<http://www.dhs.gov/dhspublic/display?theme=43&content=3814&print=true>>

[Consulted October 2004]

DHS (2004b), *National Incident Management System*. U.S. Department of Homeland Security, March 1, 2004.

DHS (2004c), *National Response Plan*. U.S. Department of Homeland Security, December, 2004.

DHS (2004d), *Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan*. U.S. Department of Homeland Security.

FEMA (1996), *Guide for All-Hazard Emergency Operations Planning: State and Local Guide*, Federal Emergency Management Agency, September 1996.

FEMA (1998), *Basic Incident Command System*, Federal Emergency Management Agency, January 1998.

FEMA (2004), *National Incident Management System (NIMS): an introduction IS-700 Self Study Guide*, Federal Emergency Management Agency, August, 2004.

FEMA and USFA (2000), *Guide to Developing Effective Standard Operating Procedures for Fire and EMS Departments*, Federal Emergency Management Agency and United States Fire Administration, 2000.

FHWA (2002), *Compilation of Actions Taken by Surveyed Transportation Agencies At Each Level of the Homeland Security Advisory System*, Federal Highway Administration, October 2002.

FHWA (2005), *Guidance on Alternate Route Plans*, Federal Highway Administration
Emergency Transportation Operations website, April 2005.

< http://ops.fhwa.dot.gov/opssecurity/preparedness/alt_route_plans.htm >

[Consulted May 2005]

Franklin, Tip (2004), *The Role of ITS in Homeland Security*, North Carolina DOT
Traveler Information Center website, June 2004.

< http://www.ncsmartlink.org/incident/presentations04/040722_IM01.ppt >

[Consulted March 2005].

FTA (2004). *Federal Transit Administration Transit Threat Level Response
Recommendation*. Federal Transit Administration

<<http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/ThreatLevel>>

[Consulted February 2004]

GAO (2003), *Transportation Security: Post-September 11th Initiatives and Long-
Term Challenges*, United States General Accounting Office, April 1, 2003.

Ham, Douglas (2004), *Post 9/11 State DOT Training Needs*, Parsons Brinckerhoff
presentation to TRB Education and Training Subcommittee of Critical
Transportation Infrastructure Protection Committee, Washington D.C. January
12th, 2004.

Hamilton County (2005), *History of Emergency Management*, Hamilton County website.

< <http://www.co.hamilton.in.us/page.asp?id=2404> >

[Consulted February 2005]

Hamza-Lup, Georgiana L, Kien A. Hua, Minh Le, and Rui Peng (2004), *Enhancing Intelligent Transportation Systems to Improve and Support Homeland Security*

Hasbach, Ann (1995), *Expert System Guides Response to HazMat Incident*.

Pollution Engineering December 1995 p37.

Hedden, Christopher and Erika Witzke (2002), *Emerging Partnerships Between Emergency Management Agencies and Transportation Management Centers*, Columbus, Ohio 2002.

Hushon, Judith M (1986), *Response to Chemical Emergencies*. Environmental Science and Technology. February 1986 Vol. 2 p118-121.

IDHS (2005), *Indiana Department of Homeland Security*, Indiana Department of Homeland Security website.

< <http://www.in.gov/dhs/> >

[Consulted April 2005]

INDOT (2000), *INDOT Post-Earthquake Safety Evaluation of Bridges and Roads CD-ROM*, INDOT Research Division, August 2000.

INDOT (2004), *Seymour District Emergency Management Plan*, Indiana Department of Transportation, 2004.

ITE (2004), *Transportation Emergency Response Checklist*, Institute of Transportation Engineers website.

< http://www.ite.org/security/emerg_response_check.pdf >

[Consulted July 2004]

ITE and FHWA (2004), *Transportation for Emergency Response and Recovery*, Institute of Transportation Engineers website.

<www.ite.org/security/ITE_emerg_response.ppt>

[Consulted November 2004]

ITS America (2005), *What is ITS?*, ITS America Website.

<<http://www.itsa.org/subject.nsf/vLookupAboutITSA/What+is+ITS!OpenDocument>>

[Consulted December 2004]

ITS America and USDOT (2002), *Homeland Security and ITS: using ITS to improve and support Homeland Security*, ITS America and USDOT, September 2002.

Laffey, Thomas J. (1991), *The Real-Time Expert*. Byte January 1991 p259-260.

Lin, Wen-Yinn and Pratim Biswas (1991), *EMERG: An Expert System to Develop Emergency Responses to Hazardous Material Spills*. Hazardous Waste and Hazardous Materials Summer 1991 p263-274.

Microsoft (2005), *Emergency Response Alert and Notification*, Microsoft Government Solutions and Software website.
< <http://www.microsoft.com/resources/government/emergency.aspx> >
[Consulted April 2005]

MIPT (2004), *Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism*, National Memorial Institute for the Prevention of Terrorism, April 2004.

MORPC (2005), *What is CORTAN?*, Mid-Ohio Regional Planning Commission website.
< <http://www.morpc.org/web/transportation/its/cortran.html> >
[Consulted March 2005]

NIJ (2002), *Crisis Information Management Software Feature Comparison Report*, National Institute of Justice/US Department of Justice, October 2002.

O'Bannon, Frank (2002), *Executive Order 02-16*. July 2002.

OSHA (2004), *Incident Command System*, Occupational Safety and Health Administration website.
< <http://www.osha.gov/SLTC/etools/ics/org.html> >
[Consulted March 2004]

Paniati, Jeffrey F. (2003), *Use of Changeable Message Signs (CMS) for Emergency Security Messages (memorandum)*, Federal Highway Administration, March 2003.

Power, D.J. (2004), *A Brief History of Decision Support Systems*, DSSResources website.

< <http://dssresources.com/history/dsshhistory.html> >

[Consulted June 2004]

Rao, Prakash V (1990), *Expert System Interface to Hazard Prediction Models*.
Journal of Hazardous Material October 1990 p93-106.

SEMA (2003), *Indiana Comprehensive Emergency Management Plan*. State
Emergency Management Agency, February 2003.

SEMA (2004), *Emergency Management*. State Emergency Management Agency
website.

< http://www.in.gov/sema/emerg_mgt/ >

[Consulted February 2004]

SEMA (2005), *Earthquake Program*. State Emergency Management Agency website.

< http://www.in.gov/sema/emerg_mgt/mitigation/eqp.html >

[Consulted February 2005]

Sharit, J. and S. Chen (1993). *Expert System Based Training for Emergency Management*. Journal of Computing in Civil Engineering. January 1993 Vol. 7 p6-22.

Slap, Albert J., Daniel Hillman, and David A. Moore (1988), *Expert Systems in Emergency Response*, Paper presented at the 1st Annual Symposium of the Mary Kay O'Connor Process Safety Center, Texas 1988.

State of Indiana (1998), *Indiana Code Title 10*, State of Indiana, Article 4, Chapter 1, 1998 Edition with interpretation.

TRB (2005), *Continuity of Operations Plans for Transportation Agencies*, Transportation Research Board TCRP and NHRP Project J-10F, May 2005.
<<http://www4.trb.org/trb/crp.nsf/0/fe394e87b505353f85256fbf00507ea2?OpenDocument>>
[Consulted May 2005]

USDOT (2003), *Effects of Catastrophic Events on Transportation System Management and Operation*, US Department of Transportation, January 2003.

Wilson, Frank R., Laurie Cantin, and Barry G. Bisson (1990), *Emergency Response System for Dangerous Goods Movements by Highways*. Journal of Transportation Engineering. November-December 1990 Vol.116 No.6 p789-794.

APPENDICES

APPENDIX A – TASKS ASSIGNED TO INDOT BY THE CEMP

The following is a list of INDOT's emergency response responsibilities in statewide emergency management according to the Indiana Comprehensive Emergency Management Plan (CEMP). The list follows the CEMP structure of six sections:

1. Basic Plan
2. Operations Section
3. Emergency Services Section
4. Human Services Section
5. Infrastructure Support Section
6. Hazards Specific Section

1. BASIC PLAN SECTION

The Basic Plan Section is divided into three elements: Financial Management element, General Tasks element, and Public Information Emergency Support Function.

1.1 Financial Management Element

This element provides financial management guidelines to SEMA and other state agencies to ensure funds are provided and financial operations are conducted in accordance with state policies and procedures during the response and recovery phases of an emergency.

According to the CEMP, all state agencies with emergency functions (including INDOT) should:

- a. Provide its own financial services and support to its response operations in the field. Funds to cover eligible costs for response activities will be provided through reimbursement by SEMA.
- b. State agencies may be required to spend more than their allocated budget to effectively respond to an emergency. After state agencies begin their initial response operations, it may be necessary to prepare and submit a report on the estimated funding needs for the duration of the emergency response. The purpose of the estimate is to help establish the need for an additional allocation from the Governor's Contingency Fund or supplemental or special legislative appropriations.
- c. Maintain records, receipts and documents to support claims, purchases, reimbursements and disbursements. Reimbursement requests will be documented with specific details on personnel services, travel and other expenses.

1.2 General Tasks Element

This element consists of those tasks common to all agencies and Emergency Support Functions.

For Response, INDOT's general tasks include:

- a. Identify potential funding resources that are available for mitigation (mitigation).
- b. Identify requirements for hazard specific resources and equipment (mitigation).
- c. Identify Emergency Support Function specific training requirements (mitigation).
- d. Identify Emergency Support Function weaknesses for exercise (mitigation).

- e. Develop and maintain Standard Operating Procedures/Guidelines and other plans and procedures necessary (preparedness).
- f. Develop and maintain resource and equipment lists (preparedness).
- g. Develop and maintain contact lists with essential information (address, telephone, cell, and facsimile numbers, email) included (preparedness).
- h. Develop or participate in two exercises per year (preparedness).
- i. Assess scope, magnitude, and extent of incident. Determine extent of hazard remaining (response).
- j. Activate Emergency Support Function and its personnel, based on incident assessment (response).
- k. Obtain status report on State activities, upon reporting to Emergency Operations Center (EOC) (response).
- l. Assist in the development of the Incident Action Plan (IAP) (response).
- m. Maintain record of actions taken (response).
- n. Request Federal assistance/resources as needed (response).
- o. Prepare appropriate After Action Reports (recovery)

1.3 Public Information Emergency Support Function

No tasks are assigned for INDOT in this section.

2. OPERATIONS SECTION

Consists of three Emergency Support Functions: communications/warning, information and planning, and resource support.

2.1 Communications and Warning Emergency Support Function

Lead agency is SEMA. No tasks assigned for INDOT.

2.2 Information and Planning Emergency Support Function

Lead agency is SEMA, with all agencies serving as support agencies.

INDOT's tasks for Information and Planning include:

- a. Collect/gather, verify, analyze, and disseminate incident information, as needed (response).
- b. Notify appropriate State agencies, keeping them up-to-date on the situation (response).
- c. Provide situation reports of Emergency Support Function activities to EOC supervisor as required (response).
- d. Collect information for periodic situation updates (response).

2.3 Resource Support Emergency Support Function

Lead agency is SEMA, with all agencies serving as support agencies as needed.

Resource Support provides support requirements not specifically identified in the other Emergency Support Functions.

INDOT's role in Resource Support is merely recovery oriented and includes:

- a. Account for all equipment used during incident (recovery).
- b. Provide resource status and accountability updates as required (recovery).
- c. Compile accurate accounting for all resources acquired (recovery).

3. EMERGENCY SERVICES SECTION

The Emergency services section consists of five Emergency Support Functions:

Firefighting, Health and Medical, Search and Rescue, Hazardous Materials, and Law Enforcement.

There are no INDOT-specific tasks assigned in this section.

4. HUMAN SUPPORT SECTION

The purpose of this section is to directly support those agencies giving aid to victims of disasters and emergencies. It consists of four Emergency Support Functions: Shelter/Mass care, Food/Water, Animal Health and Care, and Donations/Volunteer Management.

4.1 Shelter/Mass Care Emergency Support Function

No tasks assigned for INDOT.

4.2 Food/Water Emergency Support Function

Two tasks are assigned for INDOT in this Emergency Support Function:

- a. Coordinate with Transportation Emergency Support Function the identification and location of transportation assets necessary for the transport of food/water/ice (mitigation).
- b. Coordinate with Transportation Emergency Support Function to implement procedures for the transportation of food/water/ice and other supplies to shelters and feeding sites/facilities (response)

4.3 Animal Health and Care Emergency Support Function

No tasks assigned for INDOT.

4.4 Donations/Volunteer Management

No tasks assigned for INDOT.

5. INFRASTRUCTURE SUPPORT SECTION

Consists of four Emergency Support Functions: Transportation, Public Works and Engineering, Energy, and Damage Assessment.

5.1 Transportation Emergency Support Function

INDOT serves as the primary coordinating agency. The main objective of the Transportation Emergency Support Function is to assist local governments and voluntary organizations requiring transportation capacity to perform response missions following a major disaster or emergency. It serves as a coordination point between response operations and restoration of the transportation infrastructure.

INDOT's tasks in the Transportation Emergency Support Function include:

- a. Maintain and update personnel and equipment certifications (preparedness).
- b. Coordinate with Law Enforcement Emergency Support Function and Public Works Emergency Support Function, to provide assistance in placing barricades, controlling traffic, etc., as needed (response).
- c. Coordinate with Federal and State agencies, to determine hours of service and issue regulation waiver for commercial vehicles delivery of critical energy products (response).

5.2 Public Works and Engineering

Lead agency is the Department of Administration, with INDOT acting as one of the support agencies.

INDOT's tasks include:

- a. Inspect bridges throughout the State on an annual basis (mitigation).
- b. Maintain small portable generators (preparedness).
- c. Provide traffic control resources to Law Enforcement, as needed (response).

- d. Coordinate with Law Enforcement Emergency Support Function, on the decision to close roads (response).
- e. Provide engineering expertise, equipment, contractors and contract equipment, traffic control, and barricades, as needed (response).
- f. Secure dump trucks for use in an emergency, as needed (response).
- g. Assist in clearing roads and bridges in an emergency and as requested (response).
- h. Provide chainsaw crews and loader/dump truck crews for debris removal and road clearing (response).
- i. Inspect public bridges, overpasses, and railroad/highway intersections for structural integrity after a disaster (recovery).

5.3 Energy Emergency Support Function

No tasks assigned for INDOT.

5.4 Damage Assessment Emergency Support Function

Lead agency is SEMA Recovery Division, with INDOT acting as one of the support agencies.

INDOT's tasks in this Emergency Support Function are the same as for all agencies included in the CEMP, and include:

- a. Send assessment reports to SEMA (response).
- b. Assist local authorities in performing damage assessments, as requested (response).
- c. Assist in the preparation of economic injury information of affected areas from major disasters (recovery).

6. HAZARDS SPECIFIC SECTION

The purpose of the section is to contain specific information on emergency or disaster situations not found in the other sections of the CEMP.

6.1 Terrorism Consequence Management Element.

This element addresses the specialized emergency response operations and supporting efforts needed by Indiana in the event of a known, suspected, or threatened terrorist incident occurring within its borders. It supplements the CEMP by addressing those specialized considerations necessary in case of a terrorist attack.

The Terrorism Consequence Management Element is organized in the same manner as the CEMP's structure. For INDOT, there are no additional tasks assigned in the case of terrorism additional to those already covered in the rest of the CEMP.

APPENDIX B

Questions for AASHTO Forum on Transportation Security

For Indiana DOT

1. Which person (by job position), if any, has been designated to lead your state DOT's planning activities for transportation security?
2. To what extent has your DOT carried out a vulnerability assessment?
 - A. Complete, having considered all transportation-related assets in the state.
 - B. Preliminary, having focused on those assets deemed to be most important.
 - C. Nothing formal yet.
 - D. Other (specify):
3. If a vulnerability assessment has been conducted, who did it?
 - A. DOT staff (please list job positions involved)
 - B. A multidisciplinary team (describe briefly)
 - C. A consultant (give company name)
 - D. Other (specify)
4. If a vulnerability assessment has been conducted, please describe briefly the method that was used, and/or provide a person to contact for more information.

5. Does your DOT have an internal Emergency Operations Plan, independent of the usual all-hazards State Emergency Management Plans, with specific provisions for emergency response to terrorist incidents?
6. Does your DOT have a special organizational structure (e.g., the Incident Command System) for emergency response? If so, please describe or provide a person to contact for more information.
7. What actions, if any, have been taken to protect DOT personnel responding to an incident from exposure to chemical/biological agents?
8. Has your state DOT adopted any type of surveillance (such as sensors or cameras) to monitor its assets? If so, what technology and what types of assets?
9. How are the DOT's emergency response actions coordinated with other agencies within the state?
10. Were there any modifications in your DOT's internal (within the DOT) and external (with other agencies) communications procedures to respond to terrorist incidents? If so, what actions were taken?
11. Does your DOT (plan to) use any type of computer-based decision support system as a tool for emergency response decision making?

STATE DOT SURVEY AASHTO FORUM

Emergency Response

STATE DOT		EOP	ICS	ACTIONS TO PROTECT DOT PERSONNEL	MODIFICATIONS IN COMMUNICATIONS PROCEDURES	DECISION SUPPORT SYSTEM
1	Arkansas	Yes	Yes	- Awareness training in HAZMAT.	- Critical structure emergency action plans.	No
2	Colorado	No	No	- Personal Protective Equipment. - Awareness training in HAZMAT.	- None	No
3	Connecticut	Yes	N/A	- Awareness training in HAZMAT.	- Notification procedures for reporting threats. - Notification lists activated according to threat level.	N/A
4	Georgia	Yes	Yes	- None	- None	No
5	Kansas	No	No	- None	- None	- Yes, in development by State EMA.
6	Maryland	Yes	Yes	- Personal Protective Equipment. - Awareness training	- Integration of DOT with ER agencies. - Ability to conduct statewide communications through State communication system.	- Yes. - WebEOC operated by State EMA. - Web-based GPS mapping application (EMMA) to coordinate and assist decision making, communications, and resource allocation.
7	Missouri	Yes	Yes	- None	- No modifications in procedures. - Update radio system	No
8	Montana	Yes	Yes	- Basic protective measures guide.	- Emphasis in interagency communications and interoperability. - Lines of communications modified to adopt ICS.	No
9	Nebraska	Yes	N/A	- None	- Calling system that manages calling groups and monitors internal communications through a central point (operator).	- Yes. In development by various State agencies.
10	Nevada	Yes	Yes	- Awareness training in HAZMAT.	Yes	No
11	New Mexico	Yes	Yes	- Awareness training in HAZMAT.	- Developed system for transmission of secure information	No. Considered but not recommended.
12	New York	Yes	Yes	- Several initiatives. Did not specify.	- Several initiatives to update notification and communication procedures.	No
13	Oregon	Yes	Yes	- Personal Protective Equipment. - Awareness training	- Notification procedures for reporting threats.	Yes. Web-based system (Ops Center) through State EMA to track resources.
14	Pennsylvania	Yes	Yes	- Personal Protective Equipment.	Yes	N/A
15	Texas	Yes	No	- Awareness training	- Notification procedures for reporting threats. - Equipped by the Texas DHS with a Nextel phone to be attended 24/7/365.	No
16	Vermont	No	Yes	- N/A	- None	No
17	Wyoming	No	No	- None	- None	- Yes, communication system used by State EMA.

STATE DOT SURVEY - HPMS

QUESTION

Does your DOT use a version of the Incident Command System as your operational structure for responding to large-scale terrorist events or natural disasters? If not, have you devised another special command and control structure for such situations?

STATE DOT		ANSWER	ICS
1	New Mexico	A State Highway Incident Management plan has just been developed. Training on it is expected to begin within the next quarter.	YES
2	Minnesota	Uses ICS, currently MIMS (Minnesota Incident Management System) Will be transitioning to NIMS (National Incident Management System) as soon as it is available.	YES
3	Colorado	Yes. The State Division of Emergency Management is revising this system based on the National Response Plan (NRP) and the NIMS. CDOT is participating in this process.	YES
4	Utah	N/A	
5	Puerto Rico	N/A	YES
6	Rhode Island	Do have an IC protocol that is followed within the Transportation Management Center. Have distributed to multiple responders and are presently revising that protocol through Incident Management Task Force.	YES
7	Mississippi	Yes, ICS is being used by all MS State Agencies as directed by the governor.	YES
8	South Dakota	Not sure what ICS is, but they are part of the State Emergency Response Plan which delineate overall operational structure. Feel that thorough their experience with winter storms and floods, they have developed a structure to be able to respond to most disasters	NO
9	New Hampshire	Uses ICS, in conjunction with other emergency reponse agencies. Have not developed or trained DOT personnel on this. Currently act as support agency at scene. This will come into more use as part of a four (4) Department MOU on Traffic Incident Management.	YES
10	Delaware	Yes. They will be incorporating the NIMS in the future.	YES
11	Pennsylvania	Uses a version of ICS for responding to natural hazards.	YES
12	Connecticut	Currently use the ICS and are migrating towards the NIMS within the mandated framework.	YES
13	Iowa	ICS used by all departmental first responders in their fields operations. Also used by the departmental motor vehicle enforcement officers in their field operations. Its use is required by the Code of Iowa.	YES

STATE DOT SURVEY AASHTO FORUM

Vulnerability Assessment

State	TP Security lead	Extent of VA	Who conducted VA	Methodology Used
Arkansas	Highway police chief	Preliminary-bridges and tunnels	DOT Staff, brige, maintenance and district engineer	assessing the vulnerabilityby evaluating the engineering integrity of
Colorado	Operations and Maintenatce Manager	Preliminary	Field, bridge and maintenance staff	AASHTO
Connecticut	Manager of Highway operations	Preliminary	Multidiciplinary team	Bridges and interchanges based on cost , replacement time and usage
Georgia	Director of operations	Complete	DOT staff, GEMA,Georgia HS, Bureau of investigation and Secret Service	N/A
Kansas	Staff engineer	VA as a part of study by Adjutant General's Office	Adjutant General's office	N/A
Maryland	HS Coordinator	Preliminary-just headquarters	Systech Group In	AASHTO
Montana	Disaster and Financial Management Bureau	Informal		Informal process used for bridges
Nebraska	Operations and maintenance manager	Preliminary	Dot Staff, Field, operations and maintenance personnel	Bridges based on cost, redundancy and exposure
Nevada	Chief Maintenance Engineer	Preliminary	Chief Maintenance Engineer	Individual target VA worksheets
New Mexico	Deputy Secretary	Preliminary	SAIC/Parsons Brinkerhoff and NMDOT	Developed by SIAC
New York	Chief of Staff	Complete	Chief engineer and his staff	Principles of risk management
Oregon	Statewide Emergency Operations Manager	Preliminary	Operations manager with a multidicplinary team	AASHTO
Pennsylvania	Deputy Secretary of Highway Administration	Complete	Consultant- Volpe center	Best practices assessment
Texas	Deputy executive director	Preliminary-bridges	Senior staff members and bridge personnel	TxDot methodologyfor bridges and AASHTO
Vermont	Maintenance Program Engineer	Nothing formal yet	N/A	N/A
Wyoming	Assistant Chief Engineer -Operations	Preliminary	Executive Management Program Managers	Focus on noteworthy and impact on nation

STATE DOT SURVEY - HPMS

Question	<i>To what extent has your Dot conducted VA?</i>
State	
Iowa	The highway and Modal divisions have determined the iowa critical transportation assets. the assets include highway and railroad bridges, commercial points and major river facilities
New Mexico	VA based on AASHTO-- modified to include non transportation assets
Colorado	Complete, used AASHTO Methodology
Puerto Rico	contact Mr. Samuel Forestier, SForestier@act.dtop.gov.pr
Rhode Island	unable to find anyone familiar with VA
Mississippi	VA has been completed and given to AASHTO, FEMA and USDOT
South Dakota	Nothing Formal, discussed critical bridges and infrastructure with emergency management staff
New Hampshire	Preliminary, Bridges
Pennsylvania	With the help of a consultant, developed the "Commonwealth of Pennsylvania Enhanced All-Hazard Mitigation Plan."
Delaware	Used a consultant to train staff on AASHTO methodology
Utah	N/A
Minnesota	Preliminary, used a consultant

HPMS CONTACTS

Colorado	Christopher.Robbins@dot.state.co.us elbert.hunt@dot.state.co.us	Chris Robbins Elbert Hunt
Delaware	Sbhai@mail.dot.state.de.us	Subash Bhai
Iowa	Michael.Clement@dot.iowa.gov Raymond.Callahan@dot.iowa.gov	Michael Clement Raymond Callahan
Minnesota	Sonia.Pitt@dot.state.mn.us elizabeth.hartmann@dot.state.mn.us	Sonia Pitt Elizabeth Hartmann
Mississippi	jely@mdot.state.ms.us	Jeff Ely
New Hampshire	BFarrington@dot.state.nh.us	Bruce Farrington
New Mexico	Antonio.Abeyta@nmshtd.state.nm.us	Antonio Abeya
Pennsylvania	lheltebrid@state.pa.us	Laine A. Heltebridle
Puerto Rico	SForestier@act.dtop.gov.pr	Samuel Forestier
Rhode Island	jbucci@dot.state.ri.us	Joseph Bucci
South Dakota	Mike.Durick@state.sd.us	Mike Durick
Utah	gkuhl@utah.gov	Gary Khul

AASHTO CONTACTS

Arkansas	Ruth.Foggo@arkansashighways.com	Ruth Foggo
Connecticut	David.Kilpatrick@po.state.ct.us	David Kilpatrick
Georgia	Stephen.Henry@dot.state.ga.us	Stephen Henry
Kansas	Ikirmse@agtop.state.ks.us Jaci@ksdot.org	Kirmse, Ida Jaci Vogel
Maryland	jgeckle@sha.state.md.us	Joseph M. Geckle
Missouri	Don.Hillis@modot.mo.gov	Don Hillis
Montana	jhyatt@mt.gov	Jim Hyatt
Nebraska	jschmail@dor.state.ne.us	Jim Schmailzl
Nevada	jsouba@dot.state.nv.us	James R. Souba
New Mexico	David.Albright@nmshtd.state.nm.us	David Albright
New York	pgavin@dot.state.ny.us	Paul Gavin
North Dakota	mfery@state.nd.us	Michael Frey
Oregon	Rosemary.M.GENTRY@odot.state.or.us	Rosemary M. Gentry
Pennsylvania	rgarret@state.pa.us	Robert Garret
Texas	JALLEY@dot.state.tx.us	Scott Alley
Vermont	Alec.Portalupi@state.vt.us	Alec Portalupi
Wisconsin	jeffrey.western@dot.state.wi.us	Jeffrey L. Western
Wyoming	ken.shultz@dot.state.wy.us	Ken Shultz

APPENDIX C – TRANSPORTATION EMERGENCY RESPONSE CHECKLIST (ITE, 2004)

Emergency Transportation Plans

- ☐ My jurisdiction has an emergency transportation plan.
- ☐ The emergency transportation plan has been coordinated with the state and local organizations in the region.
- ☐ Redundancy of routes and systems is specifically addressed and provided for in the emergency transportation plan.

The emergency transportation plan includes:

- ☐ Provisions for transportation response to an incident.
- ☐ Plans for alternate and evacuation routes depending on the incident type and location.
- ☐ Consideration of “all hazards” – chemical, biological, nuclear, etc.
- ☐ Specific actions for each level of the Homeland Security Advisory System.
- ☐ Plans for distributing transportation information to the public.
- ☐ Standard Operating Procedures for basic transportation response activities.

Inter-jurisdictional Cooperation

- ☐ Transportation professionals responsible for emergency preparedness know and routinely work with emergency response and first responder decision-makers.
- ☐ Transportation professionals responsible for emergency preparedness know and routinely work with transportation professionals in adjacent jurisdictions.
- ☐ Transportation responders are part of discussions on interoperable communication issues.

- ☐ Tabletop exercises are conducted regularly and transportation issues are part of the discussion.
- ☐ Transportation professionals are included in tabletop exercises conducted by other responders.
- ☐ Transportation departments have provisions in place for the rapid addition of operations personnel.

Training and Preparedness

- ☐ Transportation responders are trained in incident command system (ICS) and unified command system (UCS).
- ☐ Transportation responders are able to communicate with other responders at the scene via radio, phone or other means.
- ☐ Transportation officials are part of the distribution for intelligence and threat information.
- ☐ Transportation responders are adequately equipped with protective equipment and other tools for emergency response.
- ☐ Transportation responders are trained in basic skills for first responders and hazardous materials response.

Transportation System

- ☐ Information (data, voice, images) from traffic management centers is integrated and shared with emergency management centers and/or other first responder centers.
- ☐ GIS and CAD systems used by transportation and other emergency response professionals are capable of working together and sharing/overlaying data.

- ☐ Contracts and/or contracting provisions are in place that provide for construction work under emergency conditions.
- ☐ Construction contracts on key alternate or evacuation routes include provisions for rapid clearance of work zones in an emergency.
- ☐ Traffic signal systems are coordinated across jurisdictions on key evacuation and response/recovery routes.
- ☐ Traffic signal timing plans are prepared for evacuation and response scenarios.
- ☐ Traveler information systems are available and prepared for use to communicate emergency transportation information.
- ☐ Predetermined routes are appropriately signed and support traffic signal timing plans and information signing.
- ☐ Procedures and policies are in place for sharing of camera control, signal control, use of officers at intersections, websites, variable message sign control, etc.
- ☐ Traffic management centers include emergency security provisions and procedures to ensure protection of the center and center personnel.
- ☐ ITS systems are designed for redundancy and to reduce single points of failure.