

The Inherent Challenges of Securing Transportation Infrastructure – An Examination of the National Capital Region

Theodore A. Smith

George Mason University School of Law, Critical Infrastructure Protection Project

Address: 3301 Fairfax Drive – MS 1G7, Arlington,
Virginia 22201-4426, United States of America
phone: +1 703 993 4840, +1 202 427 7760 (cell)
fax: +1 703 993 4847
e-mail: theodore.smith@mitretek.org, tsmithj@gmu.edu

Abstract

Surface transportation systems are a critical element of virtually every aspect of life in the United States (U.S.). They move people and goods, employ millions of people, generate revenue and consume resources and services generated by other sectors of the economy. The terrorist's attacks of September 11th, 2001 have forced transportation service providers at every level of government in the U.S. into devoting significant time and resources to securing infrastructure. Past experiences and the analysis of the events of the September 11th, 2001 terrorist attacks confirm that many inherent challenges, including those that are institutional, technical and operational in nature, have the potential to significantly hamper efforts to secure transportation infrastructure. The inherent challenges of securing transportation infrastructure presented to Federal, state and local agencies are unlike any that the U.S. has ever faced. The threats have no boundaries – jurisdictionally, nor in terms of disciplines they affect. To adequately secure transportation infrastructure it is imperative that new approaches and processes be developed and implemented. The purpose of this research is to examine the inherent challenges that transportation service providers face in securing transportation infrastructure in the National Capital Region (NCR). In addition, this research examines various planning, development and operational activities that are being executed to ensure transportation systems security in the NCR, including the George Mason University (GMU) led Critical Infrastructure Protection Project.

Introduction

Surface transportation systems are a critical element of virtually every aspect of life in the U.S. They move people and goods, employ millions of people, generate revenue and consume resources and services generated by other sectors of the economy. In 2001, the transportation sector of the U.S. economy contributed \$1.047 trillion to a \$10.08 trillion Gross Domestic Product (GDP).¹ This is not surprising considering that the U.S. is one of the most mobile nations in the world, accommodating over 4 trillion miles of passenger travel annually.² In 2001, there were also an estimated 191 million licensed drivers and 226 million registered vehicles in the U.S.³ Further, public transit users made more than 9 million unlinked trips using the more than 6,000 transit properties in 2001.⁴

Surface transportation systems in the U.S. have evolved into complex networks over a series of defining periods of time that have been marked by their focus on planning, development, management and

operations, and now security of the systems. The activities focal to these periods of time have often been motivated by federal legislation that aimed to provide safe, efficient and reliable transportation services. The terrorist's attacks of September 11th, 2001, however, were largely responsible for forcing transportation service providers at every level of government in the U.S. into devoting significant time and resources to securing infrastructure.

The purpose of this research is to examine the inherent challenges that transportation service providers face in securing transportation infrastructure in the National Capital Region (NCR). In addition, this research examines various planning, development and operational activities that are being executed to ensure transportation systems security in the NCR, including the George Mason University (GMU) led Critical Infrastructure Protection Project. The research and analysis presented in this paper concentrates on highway networks and mass transit systems including railways and buses.

National Capital Region Transportation Systems

The NCR is defined in the United States Code [40 USC 71 (b)] as the District of Columbia; Montgomery and Prince Georges Counties in Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties in Virginia; and all cities existing in Maryland or Virginia within the geographic area designated by the outer boundaries of the combined counties listed. The geographic area of the NCR covers more than 3,000 square miles and is currently home to some 4.2 million people and 2.7 million jobs.

The vast transportation network in the NCR includes 14,100 lane miles of highways, more than 200 miles of carpool lanes, 103 miles of Metrorail and 162 additional miles of commuter rail. The system also includes an extensive bus network or local and commuter services, as well as three major airports – Reagan National, Dulles and Baltimore/Washington International.⁵ Figure 1 illustrates the comprehensive highway network that serves the NCR.

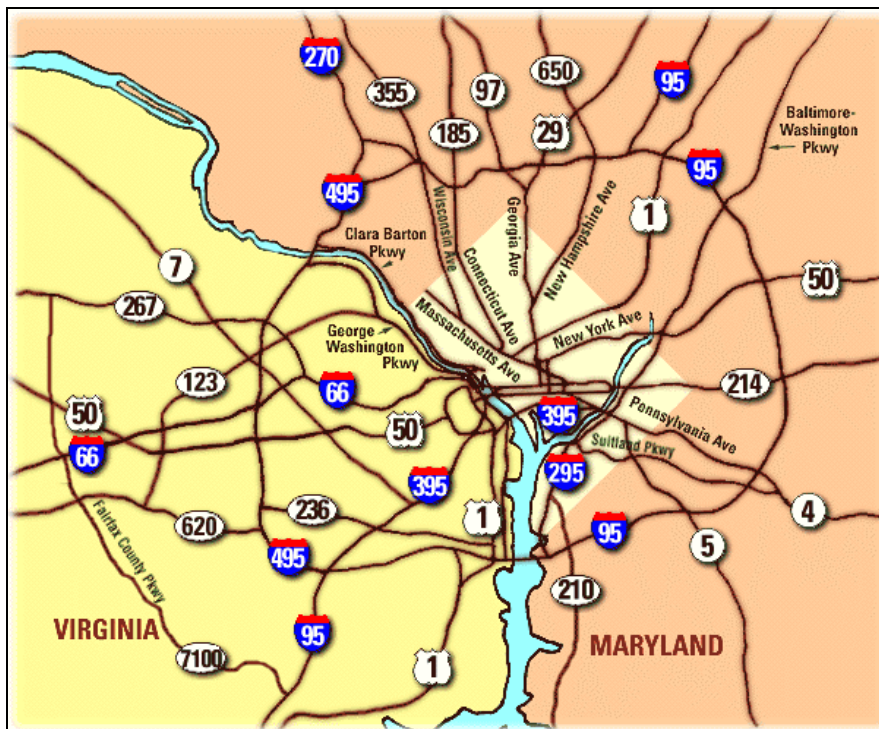


Figure 1: National Capital Region Highway Network (source: smarttraveler).

Disaster Lifecycle

The discussions and analysis presented in this paper are structured around what is commonly referred to as the Federal Emergency Management Administration (FEMA) disaster life-cycle. The FEMA disaster lifecycle defines a series of activities that regional partners, like those in the NCR, engages in to prepare for emergencies and disasters, respond to them when they occur, assist people and public and private institutions recover from the emergencies and disasters, mitigate the affects of the emergency or disaster, reduce the risk of loss, and help prevent disasters and emergencies from occurring. Collectively these functions represent the processes and activities necessary to secure transportation infrastructure. Although there are varying definitions of the FEMA disaster lifecycle, for the purposes of this research it includes:

- Response - The mobilization and positioning of emergency equipment and personnel to get the public out of danger, bringing the impacts of the disaster under control, providing medical services to those impacted by the disaster, and repairing damaged systems and re-establishing services as soon as possible.
- Recovery – Repairing and/or rebuilding transportation infrastructure and vehicles in order to return them to their pre-disaster level of service.
- Risk Reduction and prevention - Reducing the probability of an attack on transportation infrastructure, and mitigating the potential impacts should an attack occur.
- Planning and preparedness – Ensuring that when a disaster occurs, transportation and public safety agencies are ready to respond in the safest and most efficient manner while providing for the safety of the general public.

Figure 2 provides a sequential illustration of the disaster lifecycle as it relates to general tasks that are critical in securing transportation infrastructure.

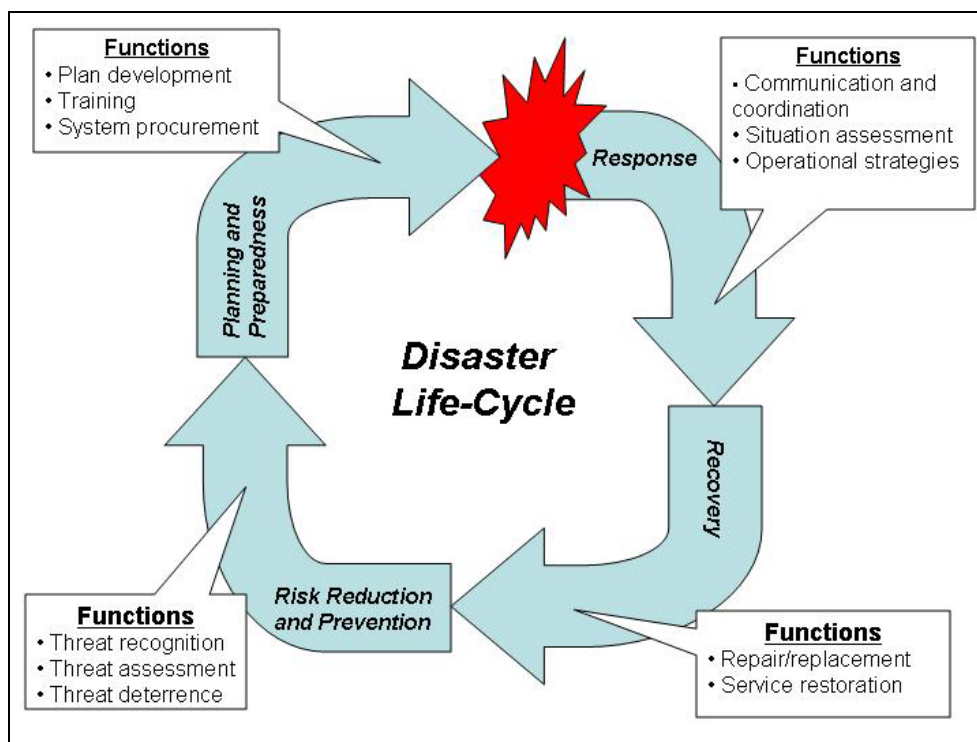


Figure 2: FEMA Disaster Lifecycle as it relates to securing transportation infrastructure.

Securing Surface Transportation Infrastructure – The Inherent Challenges

Past experiences and the analysis of the events of the September 11th, 2001 terrorist attacks confirm that many inherent challenges, including those that are institutional, technical and operational in nature, have the potential to significantly hamper efforts to secure transportation infrastructure. Challenges described in this section focus on those specifically relevant to the NCR.

Response

The emergent nature of disasters, including terrorist attacks, creates an environment that quickly expands, with many agencies and service providers from various disciplines and jurisdictions descending on the same scene at virtually the same time. Consequently, a span of control, or command structure, among a multitude of responders can be quite difficult. Consider the potential number of agencies that could respond to a terrorist attack. What may start out as fire and rescue response to a “major incident” will quickly grow to involve literally dozens of responders. Fire and rescue are likely to be the first, to respond to a “major incident.” EMS and law enforcement then will likely follow closely behind. As soon as there is even the slightest notion that the event is a terrorist attack Federal investigators will become involved and the scene then becomes a “crime scene.”

An additional level of complexity is added if it is suspected that a weapon of mass destruction (WMD) is involved in the attack. Multiple players from Federal, state and local agencies who are specifically concerned with containing the attack and reducing further exposure of the agent to humans and the environment then become involved.

Generally speaking from an operational perspective, at the local level there is also a chronic lack of voice and data communications systems interoperability among responding agencies, from various disciplines and jurisdictions. A study sponsored by the National Institute of Justice – National Task Force on Interoperability concluded that a variety of factors are impediments to interoperability of voice and data communications systems, including:

- Communications equipment is aging and incompatible – Adjacent jurisdictions many time use different types of radio systems and different frequencies.
- Limited and fragmented funding – Resources for replacement of voice and data communications systems are limited – at every level of government.
- Limited and fragmented planning – Planning activities are typically under funded and are rarely conducted in the context of the region as a whole.
- Lack of coordination and cooperation – Many times agencies are reluctant, if not unwilling, to give up management and control of their own voice and data communications systems – at any level of planning, development, implementation or operation.

Additionally, attacks on transportation infrastructure involving WMD pose even more complicated response challenges. Responding to such attacks requires a combination of trained personnel, specialized equipment, well defined procedures and supplies. The challenge lies not only in having access to these resources, but having access to a sufficient number of these resources. As an example, an attack on a transit facility, like Washington Metropolitan Transit Authority’s (WMATA’s) Metrorail, that could affect literally thousands of people at one time would likely be overwhelming for all of the involved response agencies.

Many problems can also arise when trying to evacuate the urban core of a metropolitan area following an attack. Peak hour congestion is problematic in every metropolitan area to begin with. Evacuating panicked citizens from a metropolitan area in an even more condensed timeframe can increase delay exponentially. Consequently, evacuation plans that are coordinated and encompass multiple modes and jurisdictions are critical. The problems with the September 11th evacuation of Washington, DC made it clear that regional partners needed to do a better job of communicating and coordinating activities when trying to evacuate the urban core where thousands commute to work daily.

Recovery

Terrorist attacks on transportation systems involving weapons of mass destruction (WMD – chemical, biological or radiological agents) are frightening for a number of reasons from the perspective of returning systems to their pre-disaster level-of-service. First, transit facilities are particularly susceptible to such attacks – as demonstrated in other parts of the world. Second, release of biological agents is different than chemical and nuclear attacks. An explosion or release of a chemical agent results in a visibly dramatic event, usually with casualties and injuries, which would set into motion efforts to contain the agent. In contrast, a biological attack could go undetected for an extended period of time – resulting in the unknown spreading of the agent.⁶

With respect to WMATA's Metrorail system, agents could be spread to a number, if not all, of the systems 86 stations before being detected. Consequently, large portions of the system would be rendered unusable for long periods of time while clean-up activities were being conducted, dramatically extending recovery times. This could be catastrophic from a regional mobility perspective considering that more than 40 percent of the work trips to the urban core of the NCR are made via public transit.

Recovery of the transportation system to the pre-disaster level-of-service can also be hampered by interdependencies of other critical infrastructures such as power and telecommunications. Interdependencies of critical infrastructures can take on two dimensions. First, and most logical, the safe and efficient operation of some transportation systems is not possible without the services of other critical infrastructures. As an example, if traffic signals are not equipped with un-interruptible powers supplies (UPS) when power to the signals is lost, they are rendered inoperable. Loss of power can also render some, or all, rail operations inoperable. This situation was experienced in many areas of the NCR following hurricane Isabel in October 2003.

Second, as was experienced during hurricane Isabel, the recovery efforts of one critical infrastructure can delay the efforts of another. Crews from the Maryland State Highway Administration (MDSHA) wanted quicker access to roadways so that they could be cleared of storm debris. Access to the roads, however, was impeded by downed power lines. Power companies did not send crews out to move downed lines in the timely manner that MDSHA anticipated. Consequently MDSHA's recovery efforts were not as expedient as they had hoped for.

A primary operational challenge related to returning the transportation system to its pre-attack level of service is that the capacity of the parallel facility or mode not affected by the attack will undoubtedly be impacted – perhaps dramatically - by the demand created by loss of the attacked facility. If a transportation facility is rendered inoperable for long periods of time, whether it be a transit station or bridge over a river, regional mobility will be greatly affected. This ultimately affects the economic well being of a region. As an example, if the American Legion Bridge on I-95 that connects Fairfax County,

Virginia and Montgomery County Maryland were to be destroyed, traffic volumes would significantly increase on other bridges that provide a regional connectivity, including the Woodrow Wilson Memorial Bridge American Legion Bridge (I-495), George Mason Memorial Bridge (I 395), Arland D. Williams Jr. Memorial Bridge (I-395) and John Philip Sousa Bridges. These alternate facilities would likely become much more congested than they already are.

And quite possibly the biggest challenge in providing regional transportation services following a disaster will be the dissemination of timely, useful and accurate information to the public. In the NCR on September 11th there were many conflicting reports on the status of various transportation facilities which presented a great deal of confusion to those trying to evacuate the urban core.

Risk Reduction and Prevention

According to a U.S. General Accounting Office (GAO) report, ineffective collaboration among homeland security stakeholders remains one of the principal impediments to integrated sharing of information in order to prevent and minimize terrorist attacks.⁷ At the core of this problem is the chronic lack of intelligence information that makes it way to those responsible for securing transportation infrastructure – state and local transportation and public safety agencies. According to a report sponsored by an Independent Task Force Sponsored by the Council on Foreign Relations an estimated 650,000 state and local law enforcement agencies continue to operate in a virtual intelligence vacuum, without access to terrorist watch lists provided by the intelligence community.⁸ More often than not, the bureaucratic nature and long standing cultures of the involved agencies and turf battles impede this ever critical exchange of information.

One only has to look at the attacks of September 11th, 2001 to understand the magnitude of events that can result from a lack of information between those responsible for securing transportation infrastructure and the intelligence community. Investigations into the attacks concluded that a wealth of existing information (including among other things, arrest warrants, invalid visas, and suspicious wire transfers of large sums of money from overseas) about the 19 hijackers, if pieced together properly, and conveyed to the appropriate parties could have prevented the attacks, or at the very least lessened the impacts the horrific acts.⁹

Further, in the intelligence community there are still substantial challenges in using existing databases, voice and data communications systems to ensure that timely, useful information is appropriately disseminated to those who secure surface transportation infrastructure to prevent or minimize terrorist attacks. Among these challenges are:

- Lack of agreed upon formats and standards for collecting and aggregating data from disparate agencies.
- Undefined guidelines and procedures for establishing effective data collection processes, and mechanisms to ensure that adequate, and accurate, information is collected from agencies. This is an extremely challenging task given the large number of federal, state and local government agencies, and other public and private organizations that are involved in data collection.
- Databases and technologies important to securing infrastructure lack compatibility. Databases belonging to federal law enforcements agencies, for example, are frequently not connected, nor are the databases of the federal, state, and local governments.¹⁰

The daunting, and never-ending task of securing transportation infrastructure through human or technological means, is made even more difficult by the expansive and diverse nature of transportation system in the US. The breadth and comprehensiveness of surface transportation systems in the NCR still present challenges, despite being contained in a much smaller geographic envelope. It would be literally impossible to continuously secure transportation facilities spread over 3,000 square miles through surveillance and patrols by law enforcement agencies.

Planning and Preparedness

A primary challenge underlying planning and preparedness efforts are the sheer numbers of disparate players from multiple jurisdictions and disciplines being brought together to address an issue that is extremely critical to society. Just as with response efforts, the dimension of coordination must be accounted for in the regional planning activities as well.

Making the planning process all the more challenging from the perspective of the transportation service provider is a relative unfamiliarity with security planning activities. Although the most recent transportation authorization bill, Transportation Equity Act for the 21st Century (TEA-21) required metropolitan surface transportation planning activities to address safety and security, a majority of these efforts addressed safety issues alone such as identifying and prioritizing remediation strategies for high-accident locations. Circumstances now dictate that issues such as long terms closures, destruction of facilities and WMD attacks must now be addressed in planning activities.

Conducting threat assessment is also a new task that creates additional challenges for transportation service providers. According to a Heritage Foundation study, it will be critical for DHS to establish a methodology for conducting Federal, State, and Local threat assessments to ensure general uniformity of findings. Additionally, a methodology will need to be developed for government entities to follow in assessing risks to people and infrastructure in their jurisdictions to ensure the compatibility of the information derived from other assessments.¹¹ However, prioritizing needs can present significant challenges - within an individual critical infrastructure sector - and to a greater extent across multiple sectors. The NCR is a classic example of this with the multitude of state and local jurisdictions that are within the region.

The root of this challenge is two-fold. First, comparing vulnerability risks across sectors is somewhat like “comparing apples to oranges.” The inherent nature of the individual sectors makes meaningful comparisons and analysis quite challenging. Second, agencies conducting vulnerability assessments and prioritizing needs will undoubtedly be territorial and act in their own self interest. Stated more simply, it is the attitude that “my needs are more critical than yours” that will be the challenge. Absent an unbiased methodology for prioritizing vulnerabilities (and subsequent funding), conflicts are more than likely to arise.

Consequential to security measures being put into place to reduce terrorist threats, aggregate estimates from subject matter experts estimate \$151 billion in additional costs annually for the American economy.¹² This is especially troubling to transportation service providers as to date the Federal Transit Administration (FTA) and Federal Highway Administration (FHWA) have conducted security activities with limited funding. FHWA and FTA have also had limited funds to provide to state and local agencies for security activities. Much of the funds allocated for transportation security have been used for costs associated with setting up the Transportation Security Administration (TSA), and of course for supporting

airline security initiatives. Further, although Congress has authorized general-purpose grants to state and local agencies for homeland security, they did not include funding specifically for infrastructure, let alone transportation infrastructure.

Questions also persist on how allocated funds are being spent – or not spent as the case may be. Federal data for fiscal years 1999 through 2002 show that the Office of Domestic Preparedness (ODP) allocated \$500 million to states to support planning, training and equipment procurement. Shockingly, \$330 million remains unspent by state and local agencies.¹³ All the more troubling is the fact that politicians continue to call for increased funding for security initiatives, despite the fact that much of the funding that has been allocated to date has been left unspent. This issue is not foreign to the NCR. According to a Washington Post investigation two years after Congress approved \$324 million in grants to help fight terrorism, much of it remains unspent by local jurisdictions. This investigation found that in part these funds have been spent on projects with or no connection to regional security initiatives.

With respect to improving operational communications many times it is difficult for public safety and transportation agencies to jointly procure voice and data communication systems that would foster information sharing. The United States Department of Justice (USDOJ) and United States Department of Transportation (USDOT), as an example, each have their own standards and requirements for procurement that are required for federal funds or grants. More often than not, these requirements are not consistent with one another.

Further, joint training for transportation and public safety agencies is seen as critical to the task of securing transportation infrastructure. There are, however, a multitude of reasons why these training efforts are difficult to execute, including:

- Daily demands on each of the agencies make it difficult to initiate such activities,
- Coordinating each with and every agency that should be included in the training activities are difficult.
- Public safety and transportation agencies do not necessarily operate with a limitless supply of equipment.

Overcoming Challenges in the National Capital Region

The inherent challenges of securing transportation infrastructure presented to Federal, state and local agencies are unlike any that the US has ever faced. The threats have no boundaries – jurisdictionally, nor in terms of disciplines they affect. To adequately secure transportation infrastructure it is imperative that new approaches and processes be developed and implemented. Described below are descriptions of such initiatives that have been executed in the NCR.

Defining a New Set of Tools

The Critical Infrastructure Protection Project, led by GMU, has been engaged by the U.S. Department of Homeland Security (DHS) to develop new and innovative strategies and processes for conducting vulnerability assessments across multiple critical infrastructures. These efforts ultimately seek to ensure that critical infrastructure sectors address the most important security concerns while enhancing the overall security of the NCR through the development and implementation of an open standard for conducting vulnerability assessments.

GMU is currently collecting and reviewing existing vulnerability assessment procedures, processes, and tools employed in eight distinct infrastructure sectors, including transportation. After evaluating

components of these methodologies, GMU will develop a best practice process for conducting vulnerability assessments. This will help ensure processes are coordinated and appropriately integrated so that preparedness activities and planning mechanisms are consistent, non-duplicative, efficient, and cost-effective. While the best practice recommendations will support individual sector needs, they will also provide standard elements that allow for cross-sector comparison for use in local, state and regional critical infrastructure protection efforts. As part of this research effort, policy and business practice strategies for implementing the tools will be developed.

Other Regionally Significant Initiatives

Recognizing that the federal government was not organized, staffed, nor adequately prepared to meet the changing demands of the 21st century (including preventing terrorist attacks and securing transportation infrastructure), President George W. Bush proposed draft legislation to Congress to create DHS on June 18, 2002. With the passage of the legislation and the subsequent creation of DHS represented the largest reorganization of the federal government since the outbreak of the Cold War when the National Security Act of 1947 unified the Armed Forces under a single department and created the National Security Council (NSC) and the Central Intelligence Agency (CIA).

With respect to influence on the NCR, the Office of National Capitol Region Coordination (ONCRC), located within the DHS, has been charged with overseeing and coordinating Federal programs and domestic preparedness initiatives for state, local and regional authorities in the region. ONCRC has been an instrumental player in the many initiatives that have been carried out in the NCR by the Metropolitan Washington Council of Governments (WashCOG) and its member agencies, including the development of the Regional Emergency Coordination Plan and its' ancillary components that are described below.

Regional Emergency Coordination Plan

Initial evaluations of the WashCOG's security planning following the attacks of September 11th indicated that the components of the regional transportation system preformed fairly well – individually.¹⁴ However, collectively, at the regional level coordinating among the various transportation service providers fell short. Consequently the Transportation Planning Board (TPB) was charged with developing a coordinated emergency response plan.

In response to this challenge the TPB developed the Regional Emergency Coordination Plan (RECP) to provide a vehicle for collaboration in planning, communication, information sharing, and coordination activities before, during, or after a regional emergency for the seventeen WashCOG member governments, the State of Maryland, the Commonwealth of Virginia, the Federal government, the public agencies, the private sector and volunteer organizations, and local schools and universities.

Regional Integrated Communication and Coordination System

The Regional Integrated Communication and Coordination Systems (RICCS) provides a system for COG members, the State of Maryland, the Commonwealth of Virginia, the federal government, public agencies, the private sector and volunteer organizations, and schools and universities to collaborate in planning, communication, information sharing, and coordination activities before, during, and after a regional incident or regional emergency. RICCS utilizes a variety of new and existing communication devices to foster collaboration that will be critical in the event of an emergency that has regional impacts.

Regional Emergency Evacuation Transportation Coordination

The Regional Emergency Evacuation Transportation Coordination (REETC) is intended to address the transportation aspects of moving people around or out of the regional area and moving required resources into the area in anticipation of, and following a regional incident or emergency that requires evacuation. Therefore REETC addresses coordination of demand management, identifying situations and strategies where the majority of people do not evacuate the area, but shelter in place, to ensure that transportation system capacity is available for those who truly need it.

Capital Wireless Integrated Network

The Capital Wireless Integrated Network (CapWIN) project is a partnership between transportation and public safety agencies in the States of Maryland, Virginia and the District of Columbia. The focus of this initiative is to develop an integrated transportation and criminal justice information wireless network. CapWIN will integrate transportation and public safety data and voice communication systems in the two states and the District of Columbia and will be the first regional transportation and public safety integrated wireless network in the United States. CapWIN will enable critical and time sensitive data to reach responders in other jurisdictions throughout the region.

Preliminary Findings

To secure transportation infrastructure in the NCR it will be necessary for the regional partners to overcome the inherent challenges associated with phase of the process. Further, it is becoming increasingly important to continue the shift of planning, operations and management and systems procurement activities from that which has a localized focus to one that considers such activities in the context of the entire region. The NCR has made significant progress with respect to this challenge as demonstrated in the development of the Regional Emergency Coordination Plan and the Regional Information Communication and Coordination Systems. The efforts of GMU in developing new and innovative strategies and processes for conducting vulnerability assessments across multiple critical infrastructures have the potential be significantly beneficial in securing transportation infrastructure in the NCR. It is also recognized that it will be necessary over time to define equitable processes for allocating resources in order to maximize transportation security expenditures at the Federal, state and local level.

Notes and References

- ¹ Pocket Guide to Transportation Statistics. United States Department of Transportation - Bureau of Transportation Statistics. January 2004.
- ² Conditions and Performance Report: Chapter 1 – Personal Mobility. Federal Highway Administration. Washington, District of Columbia. http://www.fhwa.dot.gov/policy/1999cpr/ch_01/cpm01_1.htm.
- ³ Highway Statistics 2002. Federal Highway Administration. <http://www.fhwa.dot.gov/ohim/hs01/dlchrt.htm>
- ⁴ <http://www.apta.com/research/stats/>
- ⁵ A Citizens Guide To Transportation Decision-Making in the Washington Metropolitan Region. National Capital Region Transportation Planning Board.

- ⁶ Fiedelholz, G. Responding to Biological Terrorist Incidents: Upgrading the FEMA Approach. May 2003. <http://www.homelandsecurity.org/journal/Articles/fiedelholz.html>.
- ⁷ Walker, D.M. Homeland Security: Information sharing Activities Face Continued Management Challenges. General Accounting Office. GAO-02-1122T. October 1, 2002.
- ⁸ America Still Unprepared – America Still in Danger. Report of an Independent Task Force Sponsored by the Council on Foreign Relations. Gary Hart and Warren B. Rudman. 2002.
- ⁹ Atkinson, R.D. & Ham, S. Using Technology to Detect and Prevent Terrorism. Progressive Policy Institute, Policy Brief. January 2002.
- ¹⁰ Walker, D.M. Homeland Security: Information sharing Activities Face Continued Management Challenges. General Accounting Office. GAO-02-1122T. October 1, 2002.
- ¹¹ Fisk, D.W. Top Priorities for Improving Intelligence and Law Enforcement Capabilities. Defending the American Homeland – A report of the Heritage Foundation Homeland Security Task Force.
- ¹² Five tenets of security-aware logistics and supply chain operation. Transportation Journal. July 1, 2003.
- ¹³ Dealey, S. Anti-Terror Funds Left Unspent. The Hill. March 26, 2003. Volume 10. Number 13.
- ¹⁴ Wegmann, F.J., PhD. The Role of Security in the Surface Transportation Planning Process.

