SOUTHEASTERN

TRANSPORTATION CENTER

(STC)

SECURITY PAPERS

2002

TABLE OF CONTENTS

SECURITY ISSUES INVOLVING INTERMODAL FREIGHT TRANSPORTATION AND TERMINALS

Arun Chatterjee, Ph.D
The University of Tennessee

INTRODUCTION AND BACKGROUND

Passenger transportation usually receives more attention for safety and security than freight transportation, and since the tragic events that occurred on September 11th, 2001, passenger air transportation has been receiving a great deal of attention for the risks of further terrorist attacks. However, safety and security-related risks involving freight transportation should not be ignored, and it also is receiving considerable attention of both public and private sectors. This paper examines these risks with a special focus on security issues involving terrorism. There are several different types of safety and security-related occurrences involving freight movements and these are discussed briefly in the following sections.

Accidents/Crashes

In most cases, these involve collisions among two or more freight vehicles or freight and passenger vehicles. Single vehicle crashes/accidents involving freight vehicles are also included in this category. These accidents represent unintentional failures on the part of drivers and/or vehicles, and may also be caused by deficiencies of transportation guideways such as roads and rail tracks and related controls such as air traffic control and signals. Traditionally this category receives a great deal of attention of public sector engineers and law enforcement officials.

When a collision or a single-vehicle accident involves a vehicle transporting hazardous cargo, the consequences can be very serious and widespread. Public agencies involved with freight transportation modes have developed detailed guidelines for regulating the transportation of hazardous materials. The enforcement of these guidelines reduce the risks associated with hazardous cargo movements considerably.

Cargo Theft

Theft has been a common problem with freight transportation throughout its history, and it includes a wide range of occurrences such as the piracy of ships, hijacking of rail cars and trucks, and theft of small items, which is referred to as "leakage". Theft occurs in or near terminals as well as along the route. The majority of thefts occur in large metropolitan areas. Although cargo theft has major financial impact on the freight transportation industry and insurance companies, it does not pose a threat to the general public. However, an understanding of the acts of theft, how and where they occur, is useful for identifying how and where terrorist acts may occur.

Terrorist Acts

A terrorist act is intentional and planned, and its underlying reason usually has a political purpose. Another important characteristic of a terrorist act is that it tries to cause a major loss of human lives and property to create fear, panic and chaos in a country. Attacks on

human lives usually are more likely than those on physical assets only. For example, a cruise ship full of passengers on board may be more vulnerable than a cargo ship. An expensive container crane in a port may be a less likely target of terrorism than a shopping center full of shoppers. However, the freight transportation system can be used to smuggle and deploy weapons to harm a large number of people. These weapons of mass destruction or harm (WMD) include nuclear devices and harmful "germs", which can be placed inside a "container" and exploded or activated when the container is transported through a large metropolitan area, or any other location enroute. Further, damaging a major physical facility or asset such as a port or a ship can cause panic and disrupt domestic and international trade.

Objectives of this paper

The general scope of this paper covers security-related issues of freight transportation in the United States of America (USA). The focus, however, is on terrorism that utilizes the intermodal freight transportation system. Of particular interest is how terrorists from other countries can use international marine containers to cause destruction in the USA. These containers are processed through seaports and rail-truck intermodal yards and so their passage through these terminals will be examined in detail. In the following sections, the vulnerability of the intermodal freight system to terrorist acts will be examined. This will be followed by sections that will examine different phases of the movement of an international marine container and identify where and how foul play by a terrorist group can occur. Specific actions that can be and are being taken to minimize the vulnerability to terrorist acts will be identified. It should be pointed out that this paper does not present a thorough risk assessment, which requires much more analysis.

SECURITY OF INTERMODAL FREIGHT TRANSPORTATION

Intermodal transportation involves the movement of cargo by two or more modes that are interconnected logistically. Due to its very nature, intermodal transportation is more complex than transportation by a single mode because of the use of multiple modes, which are usually managed by different parties. It should be pointed out that intermodal transportation includes both containerized and non-containerized cargo as well as bulk commodities. However, this paper will deal primarily with containerized cargo. Of special interest will be containers coming from other countries by ships since the threat of terrorism at this time seems to be higher from outside sources than domestic sources. This focus of this paper on marine containers is not meant to imply that other modes of international cargo movements and domestic sources of terrorism can be overlooked.

The involvement of several different modes and related parties in international intermodal freight movements makes it vulnerable to terrorism attacks for the following reasons:

Different countries have widely varying levels of control with regard to surveillance and inspection of cargo that are placed inside containers. It is relatively easier in some countries to get a container with dangerous materials loaded on a ship without being detected/intercepted during its passage on land and through a port. Once a container passes through its port of origin and moves in a group of thousands of other containers, say aboard a mega-size container ship arriving at a port in the USA, the job of detecting its dangerous contents becomes more difficult. There are many ways to bypass the scrutiny of port and customs officials.

1. This possibility was described by Stephen Flynn vividly at a recent conference as follows:
   "Hypothetically, based on current practices in the U.S. Customs Service, Osama Bin Laden could have a front company in Karachi load a biological agent into a container, ultimately destined to New York – New Jersey, with virtually no risk that the container would be intercepted. Under this scenario, he could use a Pakistani exporter with an established record of trade with the United States. The container could be sent via Singapore or Hong Kong, and it could arrive in the United States at the Port of Long Beach or the Port of Los Angeles and be loaded directly onto bonded rail and truck for the transcontinental trip. Because the entry port is Newark, the U.S. government does not require the cargo manifest to be on file until it actually reaches the East Coast. The carrier has up to 60 days after the goods arrived to make changes to the manifest, including what and how it was actually shipped. The container could be diverted or the weapons activated anywhere en route long before it was visually identified to be in the country." (1)

2. A container is transferred several times at different locations. The above-described example given by Flynn describes the chain of different "links" and "nodes" of a typical movement of international marine containers imported to the USA. This chain is illustrated in Figure 1. The figure shows the minimum number of "links" and "nodes". The chain actually can have more "links" and "nodes" if the container is diverted via another country's port and another steamship line. Further, an additional transfer can occur within the USA if the domestic rail movement involves interlining, that is the use of two different rail companies, which is commonly done for movements between east and west coasts. In Chicago, for example, numerous rubber-tired interchanges between two rail terminals take place every day, and these drayage trucks travel through crowded roads and densely populated areas. **The more "links" and " nodes" are involved in the chain of a container's movement, the greater is the risk of tampering and the more are the opportunities for terrorist activities**.

3. The success and attractiveness of intermodal transportation depend on efficient and seamless transfer of containers, which calls for faster transfer and less paper work. In this situation, the delay caused by inspection/screening of cargo and documents is not welcome, and thus it is likely that there may be a tendency to resort to tactics for bypassing inspection and/or screenings. It is unfortunate that some of the measures for enhancing security will be counter-productive for the efficiency of intermodal freight transportation.

VULNERABILITY AT LINKS AND NODES OF INTERNATIONAL MARINE CONTAINER MOVEMENTS

In this section a hypothetical scenario of the passage of a marine container shipped from overseas to a receiver in the USA will be examined. Further, it will be assumed that this container contains very dangerous materials, which can be explosives or germs. Another assumption is that a terrorist group is sending this container to the USA and plans to explode it somewhere enroute. In the context of this hypothetical scenario, each node and link comprising the passage will be examined to identify the risks of foul play at each location and also what steps can be taken to prevent such an event.

Origin, Drayage And Storage In Another Country

The passage of a container in the country where it originates is very vulnerable to be accessed and corrupted by terrorists. Many ports in other countries where a container can be loaded on a ship bound for the USA have poor control on security. There are certain checks that the United States and/or a cooperating foreign port can use at the port of origin. The first check can be the screening of all originating containers based on the individual shipper's recognition and status. Another check that can be introduced involves the consignee's status. Every imported container has a consignee in the United States, and it is possible to verify if the consignee listed on the bill of lading indeed is expecting the container, which is being checked for authenticity.

Relying on the shipper's identity may not be foolproof. A shipper's identity may be obscure since the container may go through an intermediary (freight forwarder). A port's employees can be bribed to accept a false bill of lading with a false name of the shipper and a false description of the content of the container. The risk of such an occurrence varies from country to country because of varying levels of unethical practices that are commonly found in other countries.

The second check of the identity of the consignee and the actual verification whether the consignee indeed is expecting the container being checked may be important. Since the consignees of imported containers are located in the USA, it would be easier and more reliable to check with them about the containers they are expecting. However, the implementation of these checks in a foreign country is difficult and it may take a long time before such procedures will be established on a regular basis.

The containers that fail to pass the checks of the status of shippers and consignees should be subjected to a physical scanning of their content, which requires sophisticated equipment. The availability of such equipment and its proper use would vary from port to port. The number of containers to be scanned also presents a problem since it is a time-consuming process. Ideally, all containers should be screened. If that is not possible, the containers with questionable shippers and/or consignees must be scanned thoroughly. Some of the leading ports in other countries such as the Port of Rotterdam and the Port of Singapore are capable of scanning a large number of containers. However, for the majority of ports, it is doubtful whether a plan for thorough scanning of suspected containers can be implemented soon.

Another possibility of foul play is that the content of a legitimate container shipped by a recognized company for a recognized consignee/receiver may be taken out and replaced with dangerous material. Such an act is possible during drayage to a port or inside a port when the container may be stored for a few days before it is loaded on a ship. This type of foul play can be detected with Electronic Seal devices. Actually, devices of this type are being developed and tested by the U.S Department of Transportation as a part of ITS intermodal freight projects.(2, 3) An electronic seal (e-seal) can be installed at the shipper's location or an inspection station. This is a radio frequency device that emits signals, which can be read by special devices at strategic locations. Any tampering of this seal can be detected by a reader, as the e-seal will generate messages to that effect.

Voyage on a Ship

Once a container is loaded on a ship, little if anything is done during the sea voyage with regard to screening or detecting any dangerous material it may contain. Large container ships carry several thousands of containers on board and it may not be easy to access them during the ocean voyage. Further, a steamship line's crew is neither trained nor expected to inspect containers' contents. It is not known whether the need for U.S. inspectors to be onboard during the entire sea voyage of container ships coming to an U.S. port has been examined and whether it is practical to do so.

If a container on board a large container ship does contain explosive materials, there is a risk of the explosive being detonated during the voyage. The detonation may be accidental or preplanned using a timing device. The intended purpose of a preplanned detonation on board a ship, of course, will be to seriously damage the ship and even sink it. Although such an event may not result in the loss of a large number of human lives, it would cause panic in the international trade community. Such an event would also disrupt international trade because many steamship lines and ports may stop their operation for a while as a precautionary measure. The economic loss of several days of disruption of international trade can be huge.

Passage Through A U.S Port

The passage of a container through a port usually includes several phases, which involve the following physical locations and facilities:

1. Approach channel
2. Harbor
3. Dock
4. Apron
5. Gate

The vulnerability at each of these locations and precautionary measures that can and are being taken are discussed in the following sections:

Searching A Ship Approaching A Port In The USA[1]

The approach channel begins on the sea and depending on a port's location, it may also include a length of a river. For example, the ports of Long Beach and Los Angeles are located on the ocean, whereas the ports of Savannah (Georgia) and Wilmington (North Carolina) are located on riverbanks 20-30 miles inland from the coastline.

[1] Some of the information in this section was obtained from an article by Fred Bayles in *USA Today*, December 31, 2001(4)

Since September 11th, the Coast Guard has intensified its effort of inspecting ships prior to their arrival in the harbor areas. Coast Guard officers actually go out offshore in small boats and board the ships for inspection (4). This has become a major effort for the Coast Guard as compared to the level of this activity, prior to September 11th. Even now the Coast Guard can inspect only a portion of a ships containers – 20 to 25 percent – due to the lack of resources. The Coast Guard actually had to develop and implement a set of new strategies, which required reassignment of its cutters, helicopters and inspectors. The priority for preventing terrorist acts has surpassed that of the fight against drug smuggling. The physical distribution of the Coast Guard's assets and manpower now is very different from how it used to be before September 11th.

It should be pointed out that finding nuclear and other explosive devices or biological weapons concealed in any one or two containers among the thousands of containers aboard a mega-size container ship is not an easy task**.** Boarding teams of coast guard officers rarely carry radiation detection devices, and it is also difficult to detect other types of explosives. So only a small sample of containers on a ship can be checked for explosives and biological weapons. Coast Guard requires advance notification of a ship's arrival. The minimum notice time has been increased from 24 hours to 96 hours in advance of a ship's arrival.

Harbor Area

The approach channels lead to harbor areas, and the incoming ships are guided by local pilots and tugboats to the docking space, where a port's labor help it anchor. The harbor area adjacent to a pier or wharf is usually quite busy with a variety of watercrafts. The Coast Guard boats patrol this area to prevent a variety of criminal activities that can occur which can include theft and smuggling. This area is vulnerable to terrorist acts, since a boat with suicide bombers can attack a ship in order to damage it severely. It is also possible that an unoccupied boat with explosives can be let loose to hit a ship or an unoccupied dock for the purpose of causing serious damage. This type of terrorist act was used against the USS Cole in Yeman in 2000. Container cranes, which are usually located very close to the edge of a pier or wharf, can be destroyed by such a runway boat hitting the pier or wharf. Although this may not cause the death of a huge number of people, the property damage can be very costly, and such an event would cause panic and disrupt the normal trade activities. Thus, the surveillance of the harbor area by the Coast Guard is an important element of the overall security process and more consideration should be given to providing Coast Guard harbor patrol teams advanced devices for detecting nuclear and other types of explosives on watercrafts operating in the harbor area.

Port Facility (Dock, Apron and Gate)

Once a container is unloaded from a ship, it has to pass through a few screenings before it can leave the port facility. U.S Customs plays an important role at this stage. In recent years, a great deal of progress has been made toward the preclearance of containers by U.S Customs even before a ship arrives at a port. The preclearance is possible because of the availability of information on the cargo content of a container, which is received electronically before a ship's arrival. For example, the Port of Charleston (South Carolina) clears more than 90 percent of arriving containers before the arrival of ships. As discussed earlier the preclearence should be based on two levels of checks, one involving the shipper and the other involving the consignee.

U.S. Customs can and does inspect any suspicious container after its arrival. Customs officials are using sophisticated equipment to scan containers. Geiger counters for detecting nuclear radiation have been used by U.S Customs for a long time. Now more sophisticated detecting devices may be made available to customs inspectors. Scanners that can provide images of the contents inside a container are also being used by U.S Customs. However, these special scanners are expensive and the current number of available scanners may not be sufficient. Further, the use of the scanners requires trained personnel.

Another agency involved with the inspection of containers inside ports is the U.S Department of Agriculture (USDA). Although USDA officers do not look for explosives or biological weapons, their effort to find contraband agriculture products can lead to the finding of terrorism-related materials.

The agency that is responsible for the overall security of a port terminal and all assets stored inside as well as those passing through is the port's police department. Although they are not involved with the screening and scanning of containers for determining what is inside them, port police officers are responsible for preventing theft and/or the infiltration of dangerous persons inside the port terminals. The areas immediately adjacent to a port terminal usually have a variety of port-related industrial and commercial activities, and these areas also are under the surveillance of port police. Despite the use of a fence along most of the length of a port's boundary, it is a challenging task for the port police to prevent infiltration of dangerous persons and stolen items in and out of a port.

The last step of an imported container's passage through a port involves its processing at the gate. At the gate, a variety of checks should be made. In addition to the identification of the container and the verification of the clearance received from customs and USDA, a careful check must be made of the driver's identification.

Landside Movement

A container on a chassis leaving a port is either going to a rail intermodal terminal for a long haul or directly to the consignee/receiver. The drayage trip to an intermodal yard can vary. It can be very short, say 15 miles, or moderately long, say 200 miles and any distance in between. If the container is placed on an intermodal train – containers on flat cars (COFC) train – at the other end of the rail movement the container is again drayed by a truck to its destination, and that drayage distance also may vary from a short to a moderate distance. The direct delivery of a container to a consignee from the port where it arrives usually is no longer than 400 to 500 miles and can be much less. In any case the movement of an imported container along highways involves several risks if it indeed contains dangerous materials. Truck hijacking and driver switching are possibilities. Hijacking of trucks occur for theft purposes even without any link with terrorism, and so it is quite possible for a terrorist group operating inside the USA to hijack a truck with a container that has been imported for the purpose of being blown up in the USA. The terrorists can be tracking and following the movement of this container with the help of various technological devices or persons working in a port who have been bribed or may belong to their group.

Therefore, the screening and inspection of truck drivers have become an important issue that is receiving more attention from both public and private sectors. The risk of hijacking is not limited to international containers coming from other countries, as similar risks exist

with domestic trailers containing hazardous materials. Therefore, the screening and inspection of truck drivers should include all truck drivers.

Each state in the USA has an agency that is responsible for the inspection of trucks and truck drivers. Under normal circumstances the inspectors of these agencies inspect a sample of trucks for mechanical defects and also the condition of the driver. The usual concerns regarding the driver usually involves drug use or driving for too many hours without adequate sleep and rest. The cargo being carried may also be inspected. The inspectors of these agencies may need special training to detect terrorism-related clues during their regular inspections and other monitoring efforts. Truck drivers themselves now are more aware than before of the risks of hijacking trucks by terrorists and are more watchful. (5)

The tracking of container movements along US highways can be helpful for identifying and locating a problem such as hijacking and/or intentional diversion from a legitimate route of travel for destructive purposes. The Office of Freight Management and Operations of the Federal Highway Administration (FHWA) currently has a project referred to as Asset Cargo Tracking, which involves installing especially designed transponders on every chassis used to move a container. (2) The signals from the transponder can be processed to identify its location, to know when a container is on it and when it is connected to a truck tractor. If the container has an electronic device with information about its cargo, it is possible that the transponder on the chassis can read and transmit that information. Several transportation companies are working with FHWA on this project for chassis tracking. The cost of fully implementing this project will require a large amount of funds.

The risks associated with the movement of a container on land is not limited to long distance movements on highways. A container moving on a TOFC train can also be hijacked or exploded on the train. A movement from the east coast to the west coast and vice versa also involves a transfer between terminals of different rail companies by a truck, which is commonly referred to as a rubber-tired interchange. These short distance movements usually happens in large urban centers such as Chicago, and any foul play at these locations can cause severe damage to human lives and property. Rail intermodal terminals also are not fully protected. The fences along the tracks do not always give full protection, as trains occasionally have to stop and wait for clearance before reaching the terminal. Theft of goods from rail cars that have to stop before reaching the protected area inside a terminal is not uncommon, and it is quite possible for a terrorist group to take advantage of such a situation to hijack a container or deploy a destructive device inside a container. Therefore, the area that should be under surveillance for terrorist acts extends beyond the usual boundary or limit of a rail terminal. Even inside a rail terminal, a rail car or a container can be broken into if it is parked for a long time.

CONCLUSIONS AND RECOMMENDATIONS

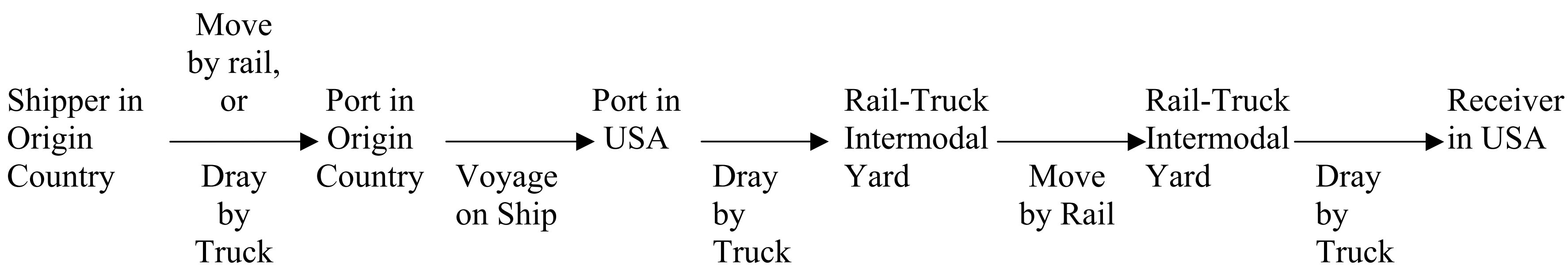
In the recently published report of the Interagency Commission on Crime and Security in U.S. Seaports (6) the risk of a breach of security involving marine transportation was examined and according to this report the risk depends on three factors – vulnerability, threat and consequence. The analysis presented in this paper primarily addresses the vulnerability of the international marine container transportation system, and it is quite clear that its vulnerability to a terrorist act is high. One of the main reasons of the high vulnerability is the complexity of this transportation system, which involves many different parties or actors located in different countries and many links and nodes through which a container must pass. The reduction of the vulnerability will require a coordinated effort of several different groups in the USA and other countries. Also required will be advanced technologies and other resources including manpower. The U.S. Department of Transportation, which includes the U.S. Coast Guard, has begun work on many fronts. U.S Customs and the individual ports also have intensified their work. These efforts can reduce the vulnerability substantially, and probably already has done so to some extent. Obviously, more has to be done in many areas as discussed in this paper.

With regard to the magnitude of threat, an objective analysis is difficult to perform. Subjectively it is quite possible that the terrorists may try to use a means other than the 'aviation' on which a great deal of attention is being given. The international marine container transportation is one of these other means that many be exploited by them. The 'surprise' factor may be attractive to the terrorists. The threat of terrorists using marine transportation may be considered high.

The consequences of the use of a marine container by terrorists for destructive purposes will depend on the type of device that will be used and the location where the device will be deployed. The possibilities are many. The worst possibilities include the use of nuclear devices and biological weapons in large urban area. Location-wise the densely populated urban areas such a Chicago, Los Angeles and New York are likely to be the high target locations, and if a device contained inside a container is deployed in such large urban areas, it will have severe consequences. Besides the urban areas, the ports can be targets too. Damages to a major seaport's infrastructure can have a serious impact on the national economy.

This study does not represent a thorough risk assessment of the international marine transportation system. It merely makes a case for continuing and further intensifying the efforts to minimize the risks of a foul play by a terrorist group at each link and node that comprise the chain of international container movement. It also points to the need for a thorough risk assessment as well as risk management. Risk assessment studies focusing on safety (i.e. accidents) of the marine transportation system in the USA have been done and the state-of-art is fairly advanced. (7) Similar studies are needed for security issues.

FIGURE 1. CHAIN OF LINKS AND NODES FOR IMPORTED MARINE CONTAINERS



REFERENCES

1. North, R., Spear A., Flynn, S., McGowan, J., and Black, J. "Cargo Clearance, Security, and Safety," *Global Intermodal Freight: State of Readiness for the 21st Century, report of a conference, Transportation Research Board, National Academy Press, Washington, DC 2001*

2. Onder, Mike. "Transportation Security Intermodal Freight," Unpublished Paper, The Office of Freight Management and Operations, Federal Highway Administration, U.S. Department of Transportation, Undated

3. Biter, Richard, and Maring, Gary. "Intermodal Freight Efficiency and Security," A Presentation, U.S. Department of Transportation, Undated

4. Bayles, Fred. "Coast Guard Sheds 'Stepchild' Status," A Report Published in USA Today, December 31,2001

5. Bowles, Scott. "Government, Truckers Keep Their Eyes on Rigs," A Report Published in USA Today, January 2, 2002

6. Report of the Interagency Commission on Crime and Security in U.S. Seaports, August 2000

7. Risk Management in the Marine Transportation System, Proceedings of a Conference, Transportation Research Board, National Academy Press, Washington, D.C., 2000

SECURITY CONSIDERATIONS IN TRANSPORTATION PLANNING

Steven Polzin, P.E. Ph.D.
University of South Florida

INTRODUCTION

This paper explores the implications of enhanced security concerns on transportation planning activities. It is becoming increasingly clear that security concerns will significantly influence how transportation facilities and services are provided. Hence, via this white paper possible implications on transportation planning are explored. Over the next several years, security considerations will most probably result in a multitude of changes in how transportation is planned, designed, implemented and operated. Transportation goals, planning processes, databases, analytical tools, and organizational structures will change due to security concerns. This paper is intended to seed that discussion and facilitate that process of change. Just as the transportation planning professional and the planning process have evolved to accommodate issues such as enhanced environmental concern, social equity, evolving technologies and multimodal considerations, the inclusion of demand management strategies, and various other new goals and considerations, so too, it will have to adapt to the need to address security considerations in the planning of transportation infrastructure and services.

TRANSPORTATION AND SECURITY

A secure transportation system is critical to overall national security from terrorism. Groups or individuals motivated to terrorize or injure people or the economy may well have transportation facilities as a target or a tool. Most assuredly, they would have a transportation element in an overall plan of terrorism. Thus, securing the transportation system is a critical consideration in overall security planning.

Terrorists may be motivated to disrupt the economy. Transportation infrastructure is critical to the functioning of the economy. Transportation activities comprise 12 percent of the gross domestic economy, and virtually all of the economy is contingent on a functioning transportation system. Disruption to critical links in the transportation system provides an opportunity to cause serious economic harm. Thus, transportation facilities may be targets of terrorists intending to harm the economy.

Terrorists may be motivated to cause personal injury to concentrations of people. Transportation facilities often provide anonymous gathering places for large numbers of individuals. Planes, trains, buses, terminal facilities, and pedestrian plazas have been terrorist targets. Thus, transportation facilities as gathering places for large groups of people may be targets of terrorists seeking to kill or injure significant numbers of individuals.

Terrorists may be motivated to strike at symbolic targets in an effort to harm a group or organization of people. Thus, high profile transportation facilities may be emotionally appealing targets for terrorism. The Golden Gate Bridge, the LA Airport, and other high profile transportation facilities have been mentioned as possible targets due to the fact that damaging

these facilities would have impacts beyond the personal and economic consequences. Thus, high profile transportation facilities may be targets of terrorism.
Terrorists need to deliver the people, munitions, explosives, biological agents, or other destructive elements in their initiatives to terrorize. Thus, transportation is explicitly an element of delivering terror. Be it airplanes, as in the case of September 11, 2001; trucks, as in the case of the Oklahoma federal building bombing and the 1993 World Trade Center bombing, or personal and freight vehicles that move the people and materials of terrorism around, transportation vehicles and facilities are critical elements in delivering terror.

Finally, as transportation is critical to the mobility of all people, including individuals who inflict terror and jeopardize security, transportation operating and regulatory agencies have opportunities and responsibilities to oversee various aspects of person movement and licensure. This includes involvement in securing borders, licensing vehicle operators, licensing vehicles, and enforcing various other laws regulating the safe use of vehicles and the transportation system.

Thus, collectively, the transportation sector is intimately involved in the security of our society and, in many respects, will be a front-line area of focus in enhancing security. The future of transportation will be very much influenced by security considerations.

Transportation requires security because it:
- *Is a critical element of the economy*
- *Is a gathering place for groups of people*
- *Has symbolic and emotional importance*
- *Provides a delivery means for people and products of terrorism*
- *Includes institutions with licensing and enforcement responsibilities*

SECURITY RISK
In its simplest terms, security risk might be expressed as a mathematical function. The security risk is a product of the probability of an incident attempt times the vulnerability of the target times the damage costs of a successful breach of security:

$$\text{Security Risk} = \text{Probability of Incident Attempt} \times \text{Vulnerability} \times \text{Damage}$$

Each of these terms suggests something about the nature of security risks to the transportation sector and the potential consequences of ongoing security concerns. Historically domestic security concerns have been modest as a result of the fact that the probability of an incident was believed to be so dramatically small that the extent of vulnerability and the size of the potential damage had been relatively unimportant. However, in the post September 11th era, the probability of an incident attempt is believed to be far greater than previously appreciated by the vast majority of the public, thus resulting in the security risk being far greater than heretofore acknowledged. Additionally, the magnitude of the potential damage from an incident is now recognized as far higher than previously perceived. The extraordinary human and monetary consequence of the September 11th incident increased by orders of magnitude the perceived size of the possible damages from an incident of terrorism. Subsequent expert and media scenarios of increasingly sophisticated and dangerous tools of terrorism, including biological and chemical

agents as well as the use of ever more powerful explosives strategically placed, has resulted in the commonly held perception of security risk being far higher to virtually all public and private sector entities in the United States.

While the above calculation could be applied to individual services and facilities, it can also be applied at the systems level where it would suggest that the security risk is now far greater, and, accordingly, should receive more attention and resources to aid in more fully diagnosing and taking other steps to reduce one or more of the factors -- probability of incident attempt, vulnerability or damage. Both the freshness of the memories of September 11th and the empirical reality of this event on the cumulative calculation of security risk will result in heightened attention for a period of time, certainly several years, even in the absence of subsequent events. If significant subsequent terrorist events occur that involve transportation services or infrastructure, then the corresponding values in the above equation will continue to increase the measure of security risk and, most assuredly, the investment in enhancing the security of transportation.

WHAT DOES INCREASED SECURITY RISK MEAN?

Within days of the tragedy of the September 11th terrorist incidents, speculation began in the media among security and transportation experts and among the general public regarding the consequences of these incidents on America's mobility. The speculation has run the gamut, from predicting the end of skyscraper construction and the subsequent decline in urban densities, to anticipating or advocating new infrastructure investments such as high-speed rail as alternatives to air travel. In the months since the incident, there has been a flurry of responses including military personnel policing airports, organizations and businesses pulling sensitive information off web sites that could have aided terrorists in planning attacks, and the U.S. Department of Transportation establishing a process whereby all transportation employees will go through a screening and verification process. A multitude of other activities is in various phases of planning and implementation, and a significant amount of effort is appropriately being invested in careful analysis and planning for subsequent steps in the overall plan to improve security. Old reports are being dusted off, new reports are being written, task forces are being formed, and training initiatives are being provided. Early action steps are already being identified and implemented while other actions will require considerable more evaluation before prudent actions can be determined.

The remainder of this paper explores how heightened security concerns will impact the planning, design, implementation and operation of transportation infrastructure and services and how these changes then might influence how transportation planning is carried out – specifically, how the impacts of heightened security sensitivity may result in changes in how transportation planning is conducted. Evaluation criteria for project programming are likely to change and costs for various transportation investments may change as a result of different design standards that enable enhanced security. Intelligent Transportation System (ITS) investments may have security roles and incident response rolls that may change how we design and specify these systems. Mode choice behaviors may change influencing the overall demand for various travel options. The era of placing parking lots under elevated freeway sections may end, and the processes of issuing driver licenses and vehicle titles may change as security considerations influence the data collection and screening steps. The goal of this paper is not to identify or

prescribe all the actions that will need to be taken, but rather to focus on how the changes that do occur will impact how one might go about conducting transportation planning efforts.

The response to terrorism is not restricted to any single level of government. Transportation planning is carried out by localities, regional authorities, Metropolitan Planning Organizations, state departments of transportation, the US Department of Transportation and various other authorities and transportation providers. Security issues permeate all levels of government and all aspects of planning and delivery of services and infrastructure. The private sector also is significantly impacted be they service providers, contractors, consumers, vehicle manufacturers and operators, or consultants and others in support roles. Security will impact day-to-day operations, mid-term planning and programming and long-range planning activities.

The following section outlines some possibilities on how security concerns might influence transportation. The intention is to speculate on the full range of possible impacts and to subsequently sort and classify them in a manner that enables a systematic exploration of what this might mean in terms of transportation planning. Subsequent sections explore the implication on the transportation planning process.

The Impacts of Security Concerns on Transportation

The September 11th incident created a financial crisis for the airline industry; government involvement will inevitably change our perception of a mode that heretofore was generally regarded as user supported. Regardless of who pays, the long-term cost of air travel is likely to go up, due to greater security costs, higher risk costs, and perhaps fewer economies of scale. Time costs of air travel may also go up as security clearances slow boarding. And, somewhat unique to air travel, there may be an increase in those who have a mode-choice-altering fear of flying. How do these changes filter into our transportation planning activities? Should mode choice coefficients or the time and money cost estimates of various modes be altered for future planning studies? Has the steeply sloped curve of growing air travel demand been permanently altered? Can technology and procedures ultimately provide needed security without significant time penalties? Does the willingness of the federal government to make a significant financial contribution to the airline industry render subsequent subsidies to Amtrak or high-speed rail more palatable?

After a decade of preaching multimodalism and modal integration, do we need to rethink those plans for remote airline check-in counters at downtown rail transit stations? Is the convenience of intermodal transfer offset by the security risk of larger concentrations of passengers and the complications of security screening to the highest prevailing standard of the associated modes? Are all modes of public travel inherently more attractive to terrorist attention and hence subject to higher security costs? Some have argued that investment in alternatives such as rail provides a necessary contingency – do we now justify investments in these alternatives by highly valuing this contingency potential in our resource programming decisions?

Many have noted that transportation's importance to the economy was underscored by the terrorists' actions, and hence, the public may be more willing to increase the investment in our transportation system. Yet, security concerns and subsequent initiatives are competition for funds in the near term and may significantly impact the cost of transportation infrastructure and services over time.

Will there be more subtle impacts in personal activity schedules and behaviors that will impact transportation? Some suggest that there is a renewed focus on the family and a tendency to stay closer to home. Others have speculated on a fear of traveling to high profile locations. Within an hour of the first terrorists' actions on September 11th, traveler behavior in response to security threats changed remarkably from passive to active roles in responding to security incidents.

Intelligent transportation system investments are now seen as an important tool in responding to terrorist incidents and their design is taking into consideration the possible role in disaster evacuation. Physical locations of transportation infrastructure are receiving more attention, with parking locations being scrutinized from the perspective of the opportunity parking provides for staging an attack on adjacent facilities. A host of responses to various security threats can be hypothesized. Table 1 outlines the types of security threats that have been contemplated as possibly impacting transportation facilities and services.

Table 1: Scenarios Considered in the U.S. DOT Vulnerability Assessment

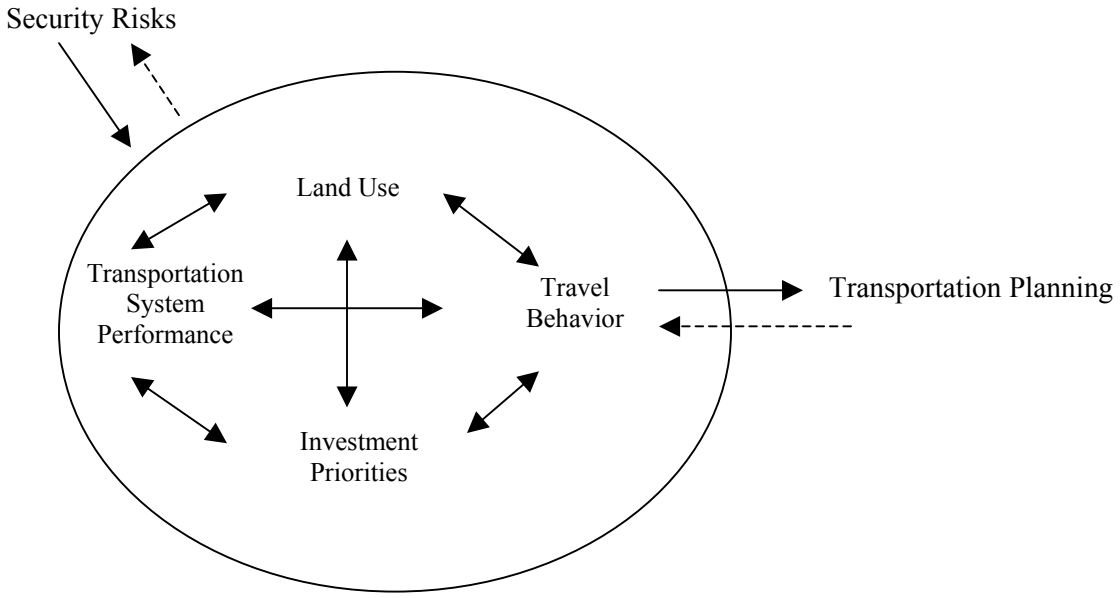
PHYSICAL ATTACKS	
• CAR BOMB AT BRIDGE APPROACH • SERIES OF SMALL EXPLOSIVES ON HIGHWAY BRIDGE • SINGLE SMALL EXPLOSIVE ON HIGHWAY BRIDGE • SINGLE SMALL EXPLOSIVE IN HIGHWAY TUNNEL • CAR BOMB IN HIGHWAY TUNNEL • SERIES OF CAR BOMBS ON ADJACENT BRIDGES OR TUNNELS • BOMB(S) DETONATED AT PIPELINE COMPRESSOR STATIONS • BOMB DETONATED AT PIPELINE STORAGE FACILITY • BOMB DETONATED ON PIPELINE SEGMENT • SIMULTANEOUS ATTACKS ON PORTS • TERRORIST BOMBING OF WATERFRONT PAVILION • CONTAINER VESSEL FIRE AT MARINE TERMINAL • RAMMING OF RAILROAD BRIDGE BY MARITIME VESSEL	• ATTACK ON PASSENGER VESSEL IN PORT • SHOOTING IN RAIL STATION • VEHICLE BOMB ADJACENT TO RAIL STATION • BOMBING OF AIRPORT TRANSIT STATION • BOMBING OF UNDERWATER TRANSIT TUNNEL • BUS BOMBING • DELIBERATE BLOCKING OF HIGHWAY-RAIL GRADE CROSSING • TERRORIST BOMBING OF RAIL TUNNEL • BOMB DETONATED ON TRAIN IN RAIL STATION • VANDALISM OF TRACK STRUCTURE AND SIGNAL SYSTEM • TERRORIST BOMBING OF RAIL BRIDGE • EXPLOSIVES ATTACK ON MULTIPLE RAIL BRIDGES • EXPLOSIVE IN CARGO OF PASSENGER AIRCRAFT
BIOLOGICAL ATTACKS	
• BIOLOGICAL RELEASE IN MULTIPLE SUBWAY STATIONS • ANTHRAX RELEASE FROM FREIGHT SHIP	• ANTHRAX RELEASE IN TRANSIT STATION • ANTHRAX RELEASE ON PASSENGER TRAIN
CHEMICAL ATTACKS	
• SARIN RELEASE IN MULTIPLE SUBWAY STATIONS	• PHYSICAL ATTACK ON RAILCAR CARRYING TOXICS
CYBER AND C3 ATTACKS	
• CYBER ATTACK ON HIGHWAY TRAFFIC CONTROL SYSTEM • CYBER ATTACK ON PIPELINE CONTROL SYSTEM • ATTACK ON PORT POWER/TELECOMMUNICATIONS	• SABOTAGE OF TRAIN CONTROL SYSTEM • TAMPERING WITH RAIL SIGNALS • CYBER ATTACK ON TRAIN CONTROL CENTER

Source: National Research Council, Improving Surface Transportation Security, A Research and Development Strategy, Washington D.C: National Academy Press, 1999.

It may be useful to explore the implications of security threats on transportation planning by reflecting on a simplistic model. Figure 1 outlines such a model, where security concerns influence land use, travel behavior, public investment priorities, and transportation system performance. In each category, impacts can be long or short range. These changes may create a need to change transportation planning activities. Changes in our planning subsequently feed

back to influence these four factors and thus, the level of security risk may experience an impact as changes influence the probability of an incident attempt, the vulnerability, or the damage.

Figure 1- Conceptual Model of Impacts of Security Risks on Transportation Planning



Each of the four factors is discussed below with examples of how they may change as a result of security risks.

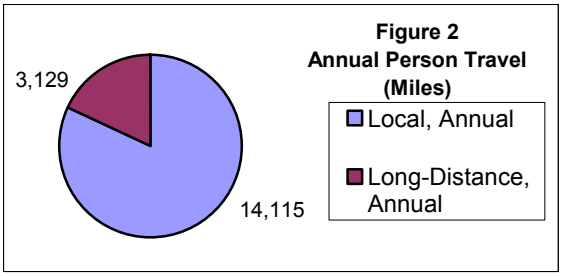
LAND USE – Individuals have speculated on a variety of land use implications, ranging from an increase in employment dispersion and sprawl to a renewed focus on the importance of the city. While signature high rises may not be a growth market, there is little reason to anticipate meaningful land use changes in the short term. The fixed nature of land use and capital intensive supporting infrastructure dampens any rapid land use changes even if there were strong pressures to make changes. According to participants in the recent Urban Land Institute's Global Mayors Forum, the September 11th terrorist attacks have sharpened the focus of municipal officials, both nationally and abroad, on the need to sustain urban revitalization efforts and enhance community livability. The participants concurred that while the possibility exists that the attacks could drive some people out of urban areas, the reaction of urban residents so far has resulted in an "overwhelming celebration" of cities. Other planners have postulated that the economic impacts will slow retirement-driven migration patterns as well as growth in tourism intensive economies. Subsequent reports from New York real estate analysts suggest that there will be some dispersion from Lower Manhattan to other locations in the near term. This appears to reflect a variety of factors including security concerns but other factors as well. There does seem to be some reinforcement of the concept of a given firm having multiple locations to enable it to have redundancy in case of disasters.

The complex set of factors that govern location choice will make it difficult to determine the significance of security risks in location decisions and subsequent land use patterns. Discerning security considerations from factors such as the ongoing shift to service and information industries and the influence of improved communications on location choice may favor dispersion of activities regardless of security concerns. If there were to be multiple future terrorist incidents concentrated in highly urban areas or other specific locations, this could result in land use responses becoming more significant over time.

One would not currently anticipate security concerns to induce changes in land use patterns that would influence transportation planning initiatives. While one might speculate that heightened security concerns may reinforce demographic shifts to lower density smaller areas, there is currently no empirical basis for this expectation. There is no reason to expect that security concerns will impact migration to or from various regions of the country.

TRAVEL BEHAVIOR – One can speculate on how security risks may impact each of the traditional four elements of travel behavior that transportation planners typically consider: trip generation, trip distribution, mode choice, and route assignment. As in the case of land use location choices, travel behavior is complex behavior influenced by a host of factors. The cumulative experiences and perceptions of travelers will influence travel behavior; thus, the perception of security risk as influenced by security incidents and perceptions of security levels for various travel options will influence individuals' travel decisions.

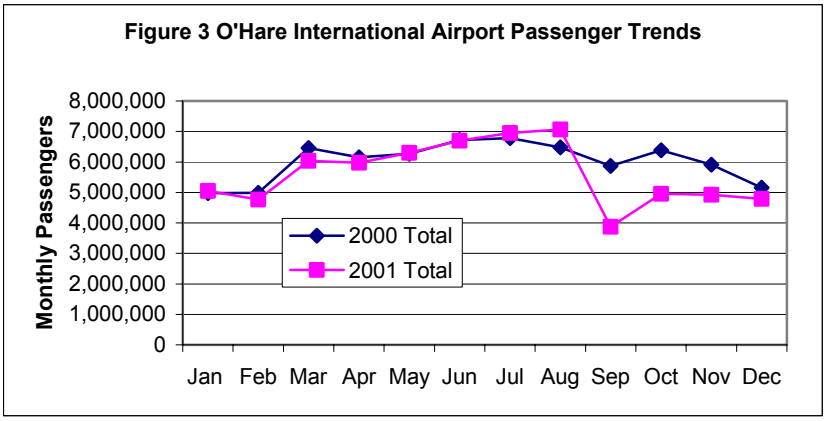
Travel Behavior:
- *Trip Generation*
- *Trip distribution*
- *Mode Choice*
- *Route Assignment*



TRIP GENERATION – After September 11th, trip making declined as people chose to forgo certain trips. This behavior was particularly apparent for long distance business and personal trips. There is speculation that a proportion of the general public will remain unwilling to fly. Some may substitute auto or rail travel, but some others will simply forgo the activity. On the business side, there is likely to be some mode shift but also some occasion for other forms of communication to substitute for travel. The September 11th tragedy is likely to enhance the use of evolving telecommunications capabilities and result in some activities being carried out by phone and other electronic communications means. The information we have on changing trip generation is based on the single extraordinary September 11th event and is complicated by the economic consequences of that event and the underlying slowing of the economy. Certain travel demand may be postponed in time while other travel may be a net loss. The empirical data that is currently being gathered suggests that the travel industry is recovering from the consequence of September 11th. It is premature to predict how security risks will impact long-term long-distance trip generation directly. Indirectly, changes in travel costs and other factors as a result of security considerations could also impact trip generation levels. As shown in Figure 2, the share of total person travel that is classified as urban (less than 100 miles from home) is the vast majority of all travel nationwide, approximately 82 percent. Arguably, the fear of security risks has had very modest, if any, direct impacts on overall local trip making beyond the immediate

physical area of an incident and the immediate aftermath of an incident. Only with sustained security incidents is it likely that local trip making rates would be measurably impacted.

Figure 3 indicates travel activity at O'Hare International Airport. As this graphic indicates, air travel levels have recovered from the immediate post September 11th levels5. The remaining discrepancy in travel levels from pre-September levels is most probably attributable to a number of factors from security related fears to economic conditions to declining air service frequency to longer travel times through airports as a result of security precautions.



Trip Distribution – Another possible significant change resulting from September 11th may be altered trip destinations. Individual travel location choices might be modestly altered. As people refocus their priorities, some may value time with family more highly and choose to minimize lengthy commutes to distant job sites. Conversely, others have argued that the push toward decentralized urban areas may result in greater sprawl, meaning longer commute trips for many. Independent of the effects of the slowing economy, work commitments and local urban travel activities are likely to remain unaffected. There may be situations where a high profile location and presumed attractive terrorist target may be avoided by some travelers. For example, following September 11th, there were warnings that the Golden Gate Bridge may be a target of terrorists. This type of attention may result in altered trip destinations with people substituting alternative destinations to avoid certain routes, or trip paths. Other travelers may be more reluctant to use various facilities that are perceived to be at risk or susceptible to significant damage if attacked. For example, some travelers may avoid tunnels and bridges. An example of changes in trip distribution includes dramatic falloff in retail sales at downtown Chicago buildings, such as the Sears Tower, when security measures made it more difficult to access interior businesses, such as restaurants and service outlets.

The largest prospect for change in trip distribution again involves those longer distance trips - specifically, trips that might involve air travel. In this regard, both personal and business trips are likely to be affected. Some individuals will choose vacation locations that do not require air travel, and other locations that are perceived as unsafe or prone to security bottlenecks, may be avoided. Travelers have long avoided international hot spots, and, if sustained terrorist activities result in concentrations of incidents in certain locations, then those locations are likely to be avoided. In a more general sense, travelers may seek to avoid crowded or high profile locations or events in fear that these could be targets for terrorists. Only with a sustained significantly higher frequency of incidents are travelers likely to meaningfully alter trip destinations as a result

[5] http://ohare.com/doa/about/statistics.shtm

of the fear of terrorist incidents. One may see more significant impacts for discretionary travel purposes. Various airports were impacted differently by September 11th, partially as a result of the nature of the travel market served and partially as a result of the target market and financial health of the particular airlines that have high activity levels at that airport.

MODE CHOICE – Mode choice changes as a result of security concerns are possible due to fears that arise from terrorist incidents or the prospects of them and as an indirect result of changes in the performance of modes due to security induced changes. The most obvious example is the impact on airline travel. Initially fears of flying altered long-distance trip-making mode choices for some people and, over time, change in the time or money cost of air travel may continue to impact air travel choice. To the extent that there is a fear that vehicles such as planes or buses could be hijacked and used in a terrorist incident or that mass mode vehicles or station locations are perceived as attractive targets with crowds of people, these modes may be avoided by some travelers. It would appear that public modes offer the opportunity for terrorists to both remain anonymous and to impact groups of people; thus, one might expect individual vehicles are less likely to be targets of terrorism. Currently there is no empirical or anecdotal evidence to indicate the extent to which mode choice behavior will be altered. There is no evidence to indicate the extent to which travelers removed in time and space would react to a terrorist incident. Would travelers in a west coast city be less likely to use the bus if there had been a bus bombing in New York three days ago, or three months ago, or three years ago? What if the incident were in an adjacent city or in your city? At this point in time, planners do not know what types of incidents or frequency of incidents would be necessary to change the travel behaviors that are reflected in transportation modeling.

As shown in Figure 3, air travel has experienced a disproportionate impact from the September 11th attack – however, one can only speculate with limited data regarding how much of this decline in air travel was accommodated by travel on other modes. Amtrak, as shown in Figure 4, was less seriously impacted, but there is little evidence that much air travel shifted to intercity rail. Some speculate that there was a shift to auto travel. Again, mode choice changes appear to be more apparent for long distance trips. Local travel is predominantly auto travel, and the terrorist incident did nothing to discourage the individual auto mode choice.

Figure 4 Amtrak Ridership Trends

Indirect impacts to mode choice are also likely as a result of security risks. Significant and highly visible changes to air travel security and perhaps less visible changes in security precautions for other modes of collective travel could result in mode choice differences. The most obvious impact will be the time and dollar cost of providing the security for travel by public carriers. Currently airport arrival time increases are variously perceived to be in the vicinity of an hour (more than previously required). Intercity bus and rail security has also increased, but service times are not perceived to have had an impact. Air travel security changes are continuing

and are expected to evolve over the next several years as strategies and technologies are put in place. A $2.50 per flight-segment passenger security surcharge had been proposed in federal legislation for heightened airport security. Other estimates and strategies could result in a significantly higher per trip increase in the cost of delivering air travel. The magnitude of that cost and how it is passed on to travelers and non-travelers will impact the extent to which security costs influence mode choice for air travel. Time penalties for security enforcement also can influence mode choice as they may impact the comparative attractiveness of air travel versus alternatives. In many locations, an additional hour per air trip for check–in could be enough to encourage the traveler to choose an alternative such as driving or perhaps rail travel in corridors where it is available.

Security incidents such as evacuations of terminals and cancellations of flights as a result of suspicious circumstances can, over time, result in poorer reliability of air travel and hence a greater reluctance of travelers to use it. However, air travel nationally carries approximately 100 times as many passenger miles as Amtrak; thus, the absence of competitive alternatives will dampen the impact of security concerns on air travel mode share.6

Beyond long-distance travel, security considerations may impact local travel as well. Factors that may affect more localized urban travel include changes in security procedures that affect public transit and parking facilities. In several areas of the country, parking facilities have been closed or security enhanced in order to restrict access. The fear that vehicles loaded with explosives could damage adjacent facilities or gatherings have resulted in changes in parking policy and locations in numerous areas. The 1993 World Trade Center bombing and the 1995 Oklahoma Federal Building bombing both involved trucks parked in locations that enabled their explosive contents to cause tremendous damage to the respective facilities.7 To the extent that security concerns impede access by car or truck to various locations or result in search delays for entering vehicles, travel behavior could be impacted. Greater walk access from parking to the ultimate destination, higher-priced parking as accessible supplies dwindle, or other changes imposed as a result of security concerns could dampen the relative appeal of personal auto travel.

Finally, to the extent that subsequent terrorist activities create a fear of group travel, there is the prospect that public modes of group travel could be impacted. In Israel, repeated terrorist incidents on public buses have reportedly altered the willingness of some individuals to use public transportation. While the prospects of such perceptions developing in the U.S. are not imminent at this time, they could impact mode choice.

---

[6] Bureau of Transportation Statistics, *Pocket Guide to Transportation*, Table 9, Page 13.

[7] 1993, Feb. 26, New York City: bomb exploded in basement garage of World Trade Center; killing six and injuring at least 1,040 others. Six Middle Eastern men were later convicted. They claimed to be retaliating against U.S. support for the Israeli government.

1995, April 19, Oklahoma City: car bomb exploded outside federal office building, collapsing walls and floors. 168 persons were killed. Over 220 buildings sustained damage. Timothy McVeigh and Terry Nichols later convicted in the antigovernment plot to avenge the Branch Davidian standoff in Waco, TX.

TRIP ASSIGNMENT – Trip assignment refers to the actual decisions on the trip route once the location and mode have been determined. Security concerns may result in some changes in trip assignment behavior. Individuals may choose to avoid routes/facilities that they feel are higher security risks. Certain stations may be perceived as less secure due to crowds or other factors. Similarly some routes may be perceived as less safe if they traverse areas that may be perceived as more likely to have security risks. For years international travel has been influenced by security concerns where persons would avoid certain airports or locations in their travel due to security concerns. For example, large hub airports may be avoided in favor of secondary hubs or direct flights. Certain bridges or tunnels may be avoided as in the case of individuals choosing to avoid using the Golden Gate Bridge.

TRANSPORTATION SYSTEM PERFORMANCE – Perhaps the most obvious area of impact to transportation emanating from security concerns is the prospect that the performance of the transportation system will be altered as a result of the responses to security risks. These changes in transportation system performance will then impact travel behavior. The nature of the changes in performance covers the range of performance attributes.

How Can Security Impact Transportation System Performance?

- *Cost to User*
- *Speed*
- *Accessibility*
- *Reliability*
- *Safety/Security*
- *Convenience*
- *Connectivity*

For example, near-term impacts of September 11th include the suspension of many airline services, long delays for airport security, security enhancements for rail travel, and minor changes in auto parking. Other changes, all intended to enhance security, may impact the transportation of various products. Of most interest to transportation planning efforts are the longer-term impacts.

Security provisions will most probably result in higher user costs for some modes. Air travel costs are likely to increase as a result of airport security costs. The prospects that various modes will have to devote resources to security precautions may divert resources or in essence increase the cost of delivering services. Parking cost may increase if security initiatives and location constraints impact the available space for parking. Additional manpower will be required to provide the enhanced security, and the implementation of various technologies to inspect baggage and screen passengers will increase costs. To the extent that these costs are passed on to travelers, the comparative cost of air travel will increase and travel behavior may change. Other modes may also have higher costs as a result of security. This could include public modes and freight transport modes.

Travel speeds for various modes could also be impacted by security concerns. Specifically, security screening for public modes may impact the total trip time for those modes. In the case of air travel, there has been a significant increase in airport passenger servicing time in the near-term, and there is some prospect that some share of that extra time will be required even when the system fully adapts to new security standards. The high value of travel time for many air travelers will inevitably result in technology and staffing level adjustments to minimize the extra total trip time, however, that may be years in coming. Other travel time delays could be incurred

for travel that involves structure parking with security, border crossings, and traveling to sensitive locations that have security restrictions.

Various modes could have changes in accessibility. For example, some parking facilities have closed sections in close proximity to buildings. Truck traffic has been restricted from certain locations and bridge, tunnel, and dam crossing travel may be eliminated or restricted. Access to and by sensitive facilities such as nuclear power plants may be more restricted, and no-fly zones for such events as the Olympics and the Super Bowl are temporally impacting accessibility for some air travel. Modal reliability could also be influenced in situations where security incidents impact the on-time reliability of travel on various modes. Numerous incidents at airports have resulted in multi-hour shutdowns that have stopped air travel. Inspection delays for other modes may similarly impact travel time reliability. Over time, repeated occurrences will influence public perceptions about reliability and hence the attractiveness of the respective modes.

Safety and security is of concern to travelers, and, to the extent that the public perceives a change in relative security, they may change their travel behavior. This may include such actions as avoiding air travel, avoiding particular stations and terminals that are feared to be targets, avoiding routes with critical links that might be targets (bridges, tunnels etc.), and avoiding group travel. Convenience may be impacted in a number of ways. Enhanced security is certainly an inconvenience, as are luggage limitations and ticketing changes that, for example, require e-ticket receipts to access airport gate areas. Additional inconveniences may be caused by requirements for enhanced personal information sharing as a condition of receiving tickets for some modes. Parking location changes, restrictions on certain vehicles such as vans, and other changes may also inconvenience some travelers. Lack of vehicle access to certain locations or parking will inconvenience some travelers and licensure and vehicle registration requirements may become more burdensome. Security and convenience perceptions may alter some travel behaviors, particularly if they fall differentially across modes.

Finally, system connectivity could be impeded by security risk concerns. Over the past decade, a significant effort within the transportation planning community has focused on intermodalism for both personal and freight travel. The intention of intermodal connections is to enable easy transfer between modes and vehicles to facilitate the most convenient and cost effective use of various technologies for transport of people or freight to various locations. The focus of such planning has been to enable convenient unencumbered transfers. To the extent that security concerns require additional scrutiny of people or freight for various modes, then intermodal initiatives may be impeded by security concerns. For example, several states are considering high-speed rail networks that are being designed to have direct convenient access to airports. To the extent that direct connections require that all rail passenger undergo the same level of security review as airline passengers, then the concept of an integrated system requires the air travel security precautions to be applied to all rail travelers that would have access to the rail-air transfer station. Similarly, precautions for baggage handling would be required to meet the perhaps higher standards of airline baggage scrutiny. Airport security requirements could also impede the convenience envisioned with off-site airport baggage and passenger check-in planned for some intermodal terminals. Similar issues could arise on the freight side where convenient intermodal transferring might require the security precautions of the most restrictive mode or product to be more broadly applied to insure security for intermodal connections.

INVESTMENT PRIORITIES – Speculation has centered on whether security risks will have an influence on public attitudes toward transportation investments. Some have suggested that the economic value of transportation is being recognized, and this will aid efforts to increase investment in transportation. Others anticipate a renewed interest in having transportation choices; specifically enhanced funding for rail modes. Still others worry that diversions of dollars to enhance security will detract from capacity improvements. The Bush administration proposal for the 2003 budget suggest at the aggregate level, overall national priorities for enhanced security may put pressure on available transportation resources in the short term. Transportation investment priority changes could result from a number of considerations.

Transportation Resource Pressures Resulting from Security Concerns

- *Diversion of resources to security needs outside of transportation programs*
- *Diversion of funds to operating security enforcement/policing/planning/training*
- *Diversion of funds to capital investments in security (barriers, fencing, inspection, etc.)*
- *Use of funds to support network redundancy/connectivity*
- *Use of funds to support modal choice/redundancy*

Post September 11th, actions suggest a variety of possible investment needs as a result of increased sensitivity to security risks. These needs range from near-term initiatives such as conducting strategic planning and assessments to supporting enhanced enforcement levels such as those found at airports, to longer-term needs to alter the physical characteristics of individual transportation investments and the system or network of investments. Changes could range from rerouting roadway alignments from sensitive sites to removing trash containers from rail station platforms. Enhancements to ITS technology as a tool to utilize in incident prevention and incident response have been contemplated, and simple design changes to enable additional vehicle inspection queues at border crossings or luggage and passenger scanning capacity at airports may be necessary. Revisiting the capability of our transportation network to handle special vehicles or military equipment in response to incidents or the exploration of modifications in our roadway network to more easily enable mass exodus from an urban area in response to a crisis are among the more complex and expensive strategies that might be pursued. Other major financial obligations could occur if decisions to change the connectivity or range of modal options in our transportation system were to move forward. Several interests, for example, have proposed major investments in high-speed rail in order to provide an alternative to dependency on air travel for longer distance trips. Additionally, certain travel behavior changes could result in different demands for transportation by various modes than are currently anticipated. This could result in changes in modal priorities, shifting geographic priorities, changes in project costs due to design or other security related changes, or other shifts in long-range transportation facility and service plans.

Having speculated on the possible repercussions of security risks to transportation and having attempted to organize these thoughts in something of a logical structure, the remainder of this paper focuses on more explicit consideration of how transportation planning might change to accommodate explicit consideration of security risks.

The Role of Security Risks in Transportation Planning

Prior to September 11th, state DOTs thought of security issues as being operational, not planning issues. Principal responsibility usually rested with law enforcement agencies. State DOT involvement was mostly in a support role in development of emergency response plans. Security issues were not an issue in most state and MPO surface transportation planning processes. Transportation Improvement Programs (TIPs) at the state and MPO levels did not contain allocations for security related issues. Agencies are now faced with determining how security concerns should be integrated into how we plan, design, implement and operate transportation facilities and services. Is security simply another goal for our transportation system that can be integrated into our planning similarly to how we accommodate safety concerns today, or does addressing security require more radical changes including such actions as redefining organizational structures, modifying basic planning processes and developing or refining planning methods, models and tools?

The goal of transportation planning is generally to lay out a vision of the transportation system and its role in the overall economy and quality of life, specifically identifying priorities and goals that will drive subsequent decisions on investments. The plan also often lays out the processes by which these visions are turned into specific implementable projects. Exactly how the transportation planning process might be altered in light of security risks is explored in the context of the security risk definition noted previously.

Table 2 outlines examples of how security risks might be interpreted in terms of the role of a transportation agency and the implications on transportation planning. As noted in the table, the role of transportation agencies in reducing the probability of an incident attempt is relatively modest. Prudent, sensitive actions of the agency can reduce the prospects of internal and customer incidents motivated by actions of the agency. There is very limited history of these types of incidents and no basis for assuming significant changes in the future. Prudent administration and appropriate training of employees to deal with potential problems is the best action and this is an operational issue whose impact on planning will be non-existent or at most represent a modest shift in resources to administration from capital or operating categories.

The second area where transportation agencies may influence the presence of individuals who may be motivated to carry out terrorist actions is in their role as a regulator. Prudent controls on the licensing of individuals and in selected other regulatory areas may also limit the prospect that individuals who may cause terrorist attacks are around or able to do so. This regulatory responsibility could preclude individuals from entering the country or from having the mobility afforded by vehicle licenses. Again, prudent administration and appropriate training of employees to deal with potential problems is the best action. The impact on planning will be non-existent or at most a modest shift in resources to administration from capital or operating categories.

Transportation agencies can play a larger role in influencing the vulnerability of transportation facilities to attack. Strategies can include limiting the information that can help in planning a successful and damaging attack, reducing the prospect for an internal attack, limiting the geographic access to sensitive locations/facilities, or providing security to reduce the prospect that someone could do something harmful in sensitive locations. Only certain aspects of these

strategies would have implications on planning efforts. There could be implications to facility location, facility design, and operations of facilities and services.

The final category of potential involvement of transportation agencies is in the area of reducing the damage associated with an incident. There are two major areas of damage reduction that merit consideration. The first is limiting the personal and physical damage of the incident by limiting the severity of the impact. This might, for instance, include structural design changes to limit the prospect of an explosion causing serious damage. Other responses could include physical and locational design considerations that minimize the amount and nature of incidents. The second general area of damage mitigation refers to minimizing the subsequent personal and economic impact by having evacuation and service restoration strategies in place that can limit losses and restore functioning. Among the most expensive strategies that are being considered as actions to respond to terrorism are actions to increase the redundancy of the transportation system. Thus, alternative modes or network connectivity strategies are primarily a tactic for post-incident restoration of system functioning. These strategies may reduce the impacts from an incident, particularly the economic impacts, however they do not impact the probability of such incidents.

Table 2 Responsibilities of Transportation Agencies in Influencing Security Risks

Security Risk Component	Possible Role of Transportation Agency	Implications for Transportation Planning
Probability of Incident Attempt Presence of individuals who have the motivation to plan and carryout acts of terrorism.	• Utilize regulatory and oversight capabilities to help identify/capture or exclude entry of possible terrorists (via licensing, border crossing enforcement, routine traffic enforcement, etc.). • Carry out responsibilities in a manner that will minimize the prospect that employees, or affected parties (land owners, contractors, system users etc.) will be motivated to seek revenge through terrorism.	• Enhance transportation agency capabilities in the areas of regulation and enforcement. • Enhance customer interface capabilities of transportation workforce.
VULNERABILITY Prospect that a transportation target could be successfully terrorized	• Limit the information availability that might influence the choice of transportation as a terrorist target. • Ensure the transportation workforce is screened and monitored to reduce likelihood of internal terrorism. • Limit the access to sensitive targets. • Secure critical elements in transportation system.	• Evaluate Knowledge sharing/dissemination strategies. • Upgrade employee and contractor screening and control capabilities. • Explore physical and operational controls on access to sensitive locations. • Reconsider alignment and service location criteria to include security concerns.
DAMAGE The direct and indirect magnitude of the consequences in personal and economic terms	• Design systems and facilities so as to be resistant to attack. • Have incident response capability to minimize loss of life and restore functioning of transportation system. • Provide redundancies to enable system robustness after an incident.	• Evaluate/modify system and facility design standards. • Consider network robustness in project design and selection. • Support investments to enable rapid incident response.

Integrating Security Concerns into Long-Range Planning

The discussions above address relationships among security risks and transportation agencies and transportation planning. They suggest how security concerns might be interjected into how transportation planning could be adapted to respond to security concerns but do not take the next step of specifically exploring how transportation planning professionals might go about changing what they do and how they do it in order to be more sensitive to security concerns. Are existing planning tools and models altered? Is the process amended to incorporate security? Is security another goal to add to the list along with subsequent objectives and performance measures? Can one simply screen all the jargon in plans and replace the term "safety" with "safety/security", or is there a distinct difference? Do security concerns merit changes in organizational charts, and how do the security responsibilities get spread across the federal, state, regional and local agencies involved in delivering transportation planning? Is security something that gets addressed in the public participation part of planning? How do the financial commitments to security initiatives get evaluated and how are tradeoffs made to reflect security concerns? And, is it premature to draw conclusions about how security impacts transportation planning?

One can speculate on how security issues might be reflected in the planning process. For purposes of discussion, the planning process is generalized into five specific steps that are common to most planning processes. Each of these steps is discussed in terms of how security issues might be accommodated.

Simplified Planning Process Steps

1. Goal Development
2. Conditions Assessment
3. Needs Assessment
4. Project Identification
5. Project Programming

1. Goal Development – Clearly the reemphasized interest in security merits its incorporation as a goal of the transportation system. Security will be a prominent goal for all types of transportation planning and operations just as safety is the single most noted goal for transportation today. Thus, with the incorporation of the security goal will come the need to develop specific objectives, criteria and performance measures that reflect security concerns. It may be logical to structure these goals along the lines of the security risk calculation by focusing on minimizing each factor: incident attempts, vulnerability of system, and damage resistance of infrastructure and services. Various other approaches for defining security objectives and performance measures may also be logical in the context of the overall strategy for objective development.

2. Conditions Assessment - Just as planning benefits from a rich understanding of current conditions, so too will it be important to have a data base that can identify the current conditions as it relates to security. This might include enrichments to various databases that would specifically address relevant considerations such as vulnerability. Many of the system inventory data items may have traits appended that address security considerations. Items may include such things as share of facilities that are secured, proximity to sensitive sites, critical links or susceptible structures (tunnels, bridges, etc.). Information on volumes/units of hazardous materials by route may be compiled and the roles of various facilities in evacuation may be compiled. The status of employee and contractor security efforts may be itemized as well as initiatives to secure transportation information may be itemized. Other

summaries of security relative to established security performance standards may also be itemized in the conditions assessment.

3. Needs Assessment - The needs assessment process determines how current trends and forecasts influence the performance of the transportation system for the design year of the plan. In this step of the process the planner would have to forecast future travel behavior and as such would need to incorporate evidence or forecasts of changes in travel behavior as a result of security concerns. Thus, if there were evidence of changes in trip generation, mode choice, trip distribution or trip assignment as a result of security concerns, these changes could result in different needs assessment findings than might otherwise be the case. These changes could be direct, for example fear of flying that results in lower airline travel, or indirect, for example slower and more expensive air travel and thus greater use of alternatives. The needs assessment process requires forecasts of conditions twenty years in the future and hence it is difficult to extrapolate or deduce from security based impacts on the relatively modest level of information available to date. Obviously, the magnitude of the impacts is very dependent on the prospect of future incidents and the pubic response. Even the consequence of security initiatives is difficult to determine at this point in time as technology and procedure changes will be refined and their consequences in terms of time and cost for various types of travel remain to be seen. Close monitoring of the consequences of security initiatives is certainly appropriate in order to develop a database of changes in system performance and traveler response. This response is not limited to individual travelers. As or more important is its influence on freight and commercial traffic.

4. Project Identification - The project identification step is the essence of planning in that it uses the knowledge of needs and the knowledge of possible solutions to come up with specific proposed solutions to particular needs. This step involves the creative energies of planners in conceiving specific plans. The design and location of transportation solutions may be affected by security concerns. For example, alignments may be altered to avoid sensitive locations and aspects of the design may be modified to reduce the prospect of damage from an incident. In the case of statewide planning the actual plan development may be occurring at the local or regional levels and are then assembled into statewide plans at the state level. Other projects may be developed specifically to respond to security concerns. These may be initiatives to secure existing facilities, modify designs to minimize damage, or enhance incident response.

5. Project Selection - The final element in traditional planning is the selection of projects to be part of an overall program of actions. In this step, the projects that best respond to the collective goal set are chosen for implementation. The decision-makers will have to find ways to evaluate the relative merits of various project proposals in light of the set of goals. Thus, the importance of security in the context of other priorities such as safety and capacity will need to be determined. This resource programming activity forces tradeoffs and implicitly requires judgments or quantification of the value of security investments. Priorities can be dramatically influenced by federal mandates or requirements. Local public and political pressures may also influence project selections. In the case of security initiatives federal mandates may significantly influence decision-making. It remains to be

seen how the general public rates security investments in the context of real tradeoffs between other projects or new revenues.

As the discussion above indicates, security concerns will influence how each of the five traditional steps in long-range planning is carried out. Similarly, security considerations will impact short- and mid-range planning, operations and maintenance activities, research agendas, and regulatory and administrative aspects of the operations of transportation agencies. A significant share of the influence will be determined by federal guidance and input by enforcement agencies; thus, the magnitude of the response to security concerns is only partially in the hands of state transportation officials.

GENERAL OBSERVATIONS ON SECURITY PLANNING

The response of transportation agencies to security concerns will encompass all aspects of agency operations from day to day operations and administration to midterm planning to long-range planning. Security assessments and enhancements for operating facilities will impact current operations the greatest. Beyond the near term the largest influence on planning is likely to be the impact on resource availability. The available resources influence the program of transportation investment and diversions of funds to support near-term security initiatives may have a significant impact on long-range planning initiatives.

THE STATE OF KNOWLEDGE AND UNCERTAINTY

The memories of the incidents of September 11th are very fresh, yet the country has a very limited history of terrorism incidents that can form a meaningful knowledge base. This knowledge base is being supplemented with international experience and scenario development such as explored in Table 1. Nonetheless, there is far from a consensus on the various tactics and priorities for reducing security risks. While it is important that energies be invested in understanding the security risks in our transportation systems and responding with prevention and response capabilities where evident, there are other aspects of security preparedness or prevention that have huge implications in terms of resource commitments that may not be prudent based on current knowledge levels. For example, some of the transportation initiatives being proposed are actions intended to provide a contingency transportation capability in response to a transportation terrorism attack. Network redundancy or alternative modes can help do that but these are very high cost options that don't reduce the prospects of an incident or minimize the probability of loss of life, only facilitate a return to normality after an incident. It may be premature to program these extremely expensive responses as other, not yet detailed or identified responses may be more effective and efficient. While terminology like "the war on terrorism" and the freshness of the memories of September 11th encourage a tendency to do everything possible to reduce security risks, resource constraints, both financial and other, will quickly require a more selective strategy.

In the immediate aftermath of a tragedy there is also a temptation to do things that one is knowledgeable about or able to do. Thus, the transportation industry with knowledge in areas such as disaster response and network design, are tempted to apply existing solutions to these new problems. While these tools and tactics will have a place in a comprehensive response to terrorism, developing a rich understanding of the role of transportation in terrorism and careful and systematic evaluation of various responses is likely to offer the most rational long-term response. The emotions inherent in dealing with a subject of this type are understandable;

however, just as the transportation community has developed measured and data based responses to transportation safety problems, so too, is it necessary to develop the information and expertise base that will enable a response to terrorism in appropriate and effective ways. Clearly, this speaks to a need to invest in learning, research, and information collection at this point in time while simultaneously increasing security in areas where it is obviously necessary and possible.

DEFINING ROLES

Perhaps the best parallel to security planning for transportation agencies is the experience in planning for emergency preparedness and incident management. Terrorist's threats and incidents are an example of an emergency of the type that transportation agencies in concert with law enforcement, the private sector, and other agencies have experienced. These types of initiatives require coordination across functional and jurisdictional lines and as such are communications and process intensive activities. The agencies have very different cultures and perspectives and thus, resource, turf and ego issues will inevitably evolve. Reiterating the critical shared mission and utilizing the lessons learned in prior collaboration intensive initiatives will be necessary. The diversity of involvement is well exemplified by looking at the diversity of ownership of transportation infrastructure. The roadway system has broad-based ownership and this is compounded by the private sector ownership of vehicles and terminal facilities.

Roadway Ownership (Center Lane Miles, 1995)

Under Federal Control	*171,967*
Under State Control	*802,733*
Under Local Control:	
Counties	1,744,514
Other Jurisdictions	*1,193,012*

Excludes federal park, forest and reservations mileage.
Source: Highway Statistics, 1995, Table HM-

September 11th reiterated the importance of coordination and communication among the many different operating agencies in a region and across the nation in response to an incident. Such coordination is needed to allow enforcement/security/safety responses to occur in an expeditious manner, while at the same time still permitting the transportation system to handle the possibly overwhelming public response to the incident. While coordination and communication are critical to facilitate responses in a crisis mode, coordination and communication in planning for security is important to insure effective and efficient security risk investments. Security responses are also challenging some state officials who are being asked to make major short-term investment commitments that challenge TIP and National Environmental Policy Act (NEPA) approval processes. Cross-agency coordination and communications will also be necessary to insure rule modifications and expedited approvals where necessary.

PRIORITY SETTING AND TRADEOFFS

The security risk equation provides a helpful way to think about how security risk can be minimized. Transportation planners have opportunities to influence each of the factors that contribute to the overall security risk. Careful analysis of how each possible action might influence the overall security risk will be a helpful strategy in ensuring that resources are directed in the most appropriate direction. Transportation agencies regularly make these types of rather complex and somewhat subjective tradeoffs for safety investments where options include

Security Risk = Probability of Incident Attempt × Vulnerability × Damage

near-term operating costs for enforcement, mid-term opportunities for education initiatives and maintenance activities, as well as longer-term investments in facility and vehicle design. Similar multifaceted tradeoffs will be required to prioritize security resources both among competing security investments and between security goals and other transportation goals such as safety.

As immediate and near-term efforts focus on operational spending to reduce vulnerability, the most immediate planning challenge will be determining which, if any, significant longer-term capital investments to make to enhance security. Defining how various investments contribute to security such that their contribution can be evaluated and tradeoff decisions made will be the most challenging aspect of post September 11th planning. Expert judgment and multiagency collaboration will be required as agencies throughout the country work to develop experience in security investment evaluation.

While many issues involving security are common across agencies and geography, each state and locality will also have unique conditions that will influence both the security risks that they face and the institutional context in which they do security planning and adapt transportation planning to incorporate security concerns. One element of uniqueness can be the nature of unique or specific threats that an area may face. Some of these items are addressed below.

CRITICAL NETWORK SEGMENTS AND HIGH PROFILE TARGETS

One element of transportation security involves identifying areas that would be probable targets based on the prospect that an incident in that location could have a significant impact. Thus, locations where the damage to people or property would be greatest may be high profile target locations that merit consideration for precautions or other initiatives to minimize the impacts of an incident. Several traits might be considered in identifying critical segments. Specific roadway links that are vulnerable, or if damaged, could cause expensive and prolonged disruptions in accessibility are examples of critical network segments. Bridges, tunnels or other critical links might be deemed critical links. The circuitry introduced if such a facility were out of service might be a consideration as well as cost to repair or replace.

Other critical network segments might be defined based on the presence of alternative mode or path access to specific locations. For example, access to military facilities, nuclear facilities and other critical locations might increase the motivation for redundancy in access opportunities. Finally, critical links might be defined based on the nature of the traffic flow and the opportunities this presents for terrorist opportunities. Routes with hazardous materials, routes with significant commercial traffic or military materials movements might be such routes.

CONCLUSIONS

Over the next several years, security considerations will result in changes in how transportation is planned, designed, implemented and operated. Transportation goals, planning processes, databases, analytical tools, decision-making considerations, and organizational structures will change due to security concerns. Transportation will be on the front line in responding to security risks. The response to security concerns will cross-jurisdictional and functional lines and be among the most complex and important challenges to transportation professionals. While it may be too early to begin changing our long-range infrastructure network plans in response to

security risks, there will be changes in spending priorities in the near term and most probably over a longer period of time.

It will be important for transportation planners to monitor closely the changes in travel behavior and try to fully understand their underlying causes. This will help planners assess the potential for longer-term shifts in behavior as a result of security-induced changes. Similarly, planners should closely monitor the performance of our transportation systems with regard to time and cost factors as well as security, so as to be able to make informed extrapolations of how these system and service changes might be impacting travel behavior. It will be important to take steps to ensure that the September 11th tragedy does not slow our progress toward a true multimodal transportation system. Nor should these events serve to further polarize modal prejudices or be used as an emotional springboard to advocate investments whose merits should be scrutinized with clear thinking. Initiatives should be put in place to monitor how September 11th and subsequent security concerns actually change U.S. travel behavior and transportation needs.

As transportation planners have struggled to find adequate resources to fully fund capacity and safety goals, a major challenge of security concerns will be ensuring that the immediate emergency diversion of time and resources does not hinder the long-term capabilities of transportation planners to respond to transportation needs. Public recognition of the cost of providing enhanced security and public support for additional funding if transportation resources are diverted to security investments may be required to ensure that the price of security is not a rapid decline in the condition and performance of our existing transportation system.

In the meantime, transportation operating agencies will be busy providing near-term responses to security concerns. The transportation planning profession has a significant knowledge base and capability in various areas such as incident response, hazardous materials transportation, and disaster response and recovery that provide a strong springboard for providing enhanced security and incident response. Transportation planning has grown over the past several decades to encompass far more than providing cost-effective, safe transportation capacity. Transportation has embraced a broader goal set including social and environmental factors. Thus, transportation planners are knowledgeable in integrating additional considerations into the goal set for planning transportation facilities and services. As experts in dealing with travel safety concerns, transportation professionals have an understanding of how complex tradeoffs between short- and long-term and capital and operating/enforcement decisions can be made. The new challenge will be applying the lessons learned in developing these capabilities to incorporating security considerations into the transportation planning process.

REFERENCES

Badolato, Ed. "Cargo Security: High-Tech Protection, High-Tech Threats." *TR News* 211, November-December 2000. http://www.nas.edu/trb/publications/security/ebadolato.pdf (2002).

Bonner, Robert C. "Speech Before the Center for Strategic and International Studies (CSIS)." Washington, D.C. 17 January 2002. http://www.customs.ustreas.gov/about/speeches/speech0117-02.htm (2002).

Boyd, Annabelle, and Jim Caton. "Securing Intermodal Connections: meeting the Challenges of Rail Aviation Passenger Facilities." Salt Lake City, Utah, 12 September 2001. http://www.nas.edu/trb/publications/security/intermodal_facilities.pdf (2002).

Boyd, Annabelle, and John P. Sullivan. "Emergency Preparedness for Transit Terrorism." *TR News* 208, May-June 2000. http://www.nas.edu/trb/publications/trnews/transit_security.pdf (2002).

Flynn, Stephen E. "Transportation Security: Agenda for the 21st Century." TR News 211, November-December 2000. http://www.nas.edu/trb/publications/security/sflynn.pdf (2002).

"Global Intermodal Freight: State of readiness for the 21st Century: Report of a Conference; February 23-26, 2000; Long Beach, California." Transportation Research Board and National Research Council, 2001. http://www.nas.edu/trb/publications/security/cp25.pdf (2002).

Jenkins, Brian Michael. "Protecting Surface Transportation Systems and Patrons from Terrorist Activities Case Studies of Best Security Practices and a Chronology of Attacks." IISTPS Report 97-4, December 1997. http://transweb.sjsu.edu/publications/terrorism/Protect.htm (2002).

Jenkins, Brian Michael, and Larry N. Gersten. "Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices." MTI Report 01-07, September 2001. http://transweb.sjsu.edu/publications/terrorism_final.htm (2002).

Mehan, Daniel J. "Information Systems Security: The Federal Aviation Administration's Layered Approach." TR News 211, November-December 2000. http://www.nas.edu/trb/publications/security/dmehan.pdf (2002).

Meyer, Michael D., "The Role of the Metropolitan Planning Organization (MPO) in Preparing for Security Incidents and Transportation System Response," Draft, January 2002.

Morgan, Daniel F., and H. Norman Abramson. "Improving Surface Transportation Security Through Research and Development." TR News 211, November-December 2000. http://www.nas.edu/trb/publications/security/dmorgan.pdf (2002).

National Research Council, Improving Surface Transportation Security, A Research and Development Strategy, Washington D.C: National Academy Press, 1999; originally in U.S. DOT, Surface Transportation Vulnerability Assessment, Final Report, Washington D.C. May, 1998.

O'Neil, Daniel J. "Statewide Critical Infrastructure Protection: New Mexico's Model." TR News 211, November-December 2000. http://www.nas.edu/trb/publications/security/doneil.pdf (2002).

Polzin, Steven E. "Transportation Planning After September 11th, 2001." The Urban Transportation Monitor, December 7, 2001.

TRANSPORTATION SECURITY: IDENTIFYING VULNERABILITIES THROUGH SPATIAL ANALYSIS OF RISK PERCEPTIONS

Asad J. Khattak, Ph.D
Carolina Transportation Program
University of North Carolina at Chapel Hill

INTRODUCTION

The September 11th events and the associated loss of life and property as well as the psychological harm have increased the importance of security in the United States. While security was always a concern within the transportation community, it has not received wide attention from transportation researchers. (Instead, they have focused on the technical, economic, social and environmental aspects of transportation.) However, the weaknesses of the transportation system in terms of security have become more apparent.

People who want to inflict intentional harm on others have recently used an array of transportation modes. For example, in the September 11th attacks, hijacked planes were used as weapons, in the attack on USS Cole a boat was used, and to bomb the Federal building in Oklahoma a van full of explosives was used. Most of these incidents were "successful" because of security violations and elements of "surprise," That is, they were largely unexpected. Gaps in our knowledge include specific vulnerabilities and security hazards within the transportation system, the preparedness of the city/governments to prevent security violations and surprises, and the perceptions of the population regarding security risks. Furthermore, we do not know much about the spatial distribution of high-risk locations and their accessibility to those who inflict intentional harm. For example, are there locations and situations that perpetrators can access relatively easily and maximize the damage and disruption?

This paper deals with these research aspects of transportation security. We propose a methodology that will allow us to understand the risk perceptions of people and the transportation risks "reported" by cities and law enforcement. Importantly, we will first develop a conceptual structure that integrates information about perceived and reported risks to plan proactively and improve future security. From a planning perspective we must attempt to prevent security violations and explore the means of mitigating associated damage, if violations do occur. One way to prevent security risks is by understanding the "weak and vulnerable" locations that can be potential targets.

The paper explores the perceptions and preferences of the two key actors involved, i.e., the general public and cities/government. We want to understand their motivations and choices and how they can be informed in the future. Our conceptual model identifies the players and the risks they face. We will understand how the general public and government agencies perceive security and what facilities the law-enforcement and government feel are most vulnerable. We will further develop a range of security scenarios that can help avoid future surprises, and suggest the creation of a pool of research-based knowledge that can be used to prevent security violations and deal with crisis situations, if they do occur. This paper suggests the need for collecting

various types of empirical data and providing new research directions to integrate reported and perceived security to get a more complete picture of security risks.

DEVELOPMENTS

We could not find substantial published literature on transportation security, but identified several developments since September 11th Table 1 summarizes some of the results from our Internet search. Due to the use of US airliners as weapons on 9/11, the Congress enacted the Aviation and Transportation Security Act. A new agency called the Transportation Security Administration was formed. "Go-Teams" were established to work intensively on specific tasks and present their findings.

TABLE 1: LITERATURE ON TRANSPORTATION SECURITY

Author	Year	Who Published Article	Key Ideas	Mitigation Suggestions
Michael P. Jackson, John Magaw, Jane Garvey, Adm. James Loy, Bruce Carlton, Joseph Clapp, Mary Peters, Jennifer Dorn, Allan Rutter, Ellen Engleman	2002	TRB Annual Mtg. (Audio)	9-11 changed transportation world, Security was always a goal, Need to rebalance, New lines of communication within transportation with coordinating group NISC – breaks down into small categories	+
Flynn, Stephen E.	2000	TR News	Beware in 2000 of terrorism	+
Mosley, Bill	2002	DOT	Measures to protect GPS	+
Macko, Steve	1998	ERRI Daily Intelligence Report	Contemporary terrorists have made public transportation a new theater of operations	+
Honea, Bob	2000	TR	We have shrinking excess capacity in US Transportation system; impact during a military crisis can be severe	+
Boyd, Annabelle & John P. Sullivan	2000	TR	Transit terrorism can be a large problem; assessment of risks and vulnerability	+
Badolato, Ed	2000	TR	Cargo Security is important	+
Congressman Clay Shaw – FL	2001	FDCH Press Release	Seaport security measures important; study of vulnerabilities of ports	-
Committee on R & D Strategies to improve Surface Transportation Security	1999	National Research Council	Looked at DOT methods for assessing risk	-
Magaw, John	2002	Statement to Aviation subcommittee	"Go-Teams" formed	-

Interestingly, prior to September 11th there were some people writing of their concerns about security, though they did not identify the method used in the September 11 attacks. For example, Macko (1998) reported that US transit systems were vulnerable to a threat. In 1999 the National Research Council produced a report on improving surface transportation security (after the fatal Sarin gas attack on Tokyo's subway in 1995). It was a study of how well the DOTs vulnerability study of 1998 had been executed and points out that DOT avoided assigning probabilities to any of the attacks laid-out in their report. In the November/December issue of 2000 *TR News* some authors expressed concerns about transportation security. They expressed concern of the imminent danger of an attack on the transportation system.

However, a comprehensive security-based approach toward different modes of transportation that include Air, Marine, Cargo (freight by truck), Highways, Transit, and Rail did not emerge. Also, specific measures that could be undertaken for mitigating possible attacks were not clearly identified. Furthermore, interdependencies of transportation systems with other systems, in particular, communication and energy are critical. However, there is limited discussion within the transportation researchers and professionals concerning communications and energy supply, which are critical to sustaining transportation systems. On the communications end, DOT has released an action plan for transportation that relies on Global Positioning System (GPS) stating that they need to ensure that adequate backup systems are maintained and they should work with the Department of Defense to continue modernizing GPS and facilitate the transfer of appropriate anti-jam technology. While government agencies seem to be working to better protect infrastructure and people, we need to understand where people think security risks are and where the agencies report the risks to be and if there are mismatches.

METHODOLOGY

Developing a comprehensive understanding of the security problem and possible solutions is critical. Specifically, the objectives of this paper are to understand the transportation security problem as perceived by individuals and cities/government agencies and suggest strategies to protect human life from intentional harm as well as avoid damage to people and property. Our hypothesis is that there are some locations and modes where public agencies have not anticipated transportation security risks. Public perceptions can be used to uncover some of these "surprise" scenarios so that governments can anticipate and treat these perceived transportation security risks.

Understanding Risk Perceptions: A Behavioral Model

As a first step, it is important to understand how people perceive and respond to security risks. Risks can be characterized in terms of frequency of event occurrence and nature of the consequences, e.g., physical harm, property damage and lost time. Figure 1 (see page 11) indicates that traffic incidents in urban areas are an example of (relatively) high-frequency low-consequence risks. On the other hand, intentional harm situations such as attacks are low-frequency and high-consequence events (at least in the US). Actual risk probabilities can be found only for events that have a long recorded history but not for rare events (Mehta 2002). So, for events such as 9/11, it is difficult to estimate the actual risk, though researchers can rely on perceived risks to get a good idea of peoples' state of mind.

Figure 2 (see page 12) presents a behavioral model that can help us understand security risks and behavioral responses. It shows that people perceive transportation system risks by direct observation and contact with others and through the electronic media/images. These form their perceptions of risk, which may or may not correspond to actual risks. Personal factors such as age and gender and psychological factors such as attitudes toward risk (e.g., risk seeking, risk avoiding and risk neutral) along with perceptions, determine a person's preferences for activity participation and travel decisions (which include destinations, modes and routes). Psychological aspects can also be represented by the attitudes that people develop towards security on various transportation modes/locations as well as the stress and anxiety they experience using the modes and accessing those destinations. People's preferences in turn can influence their actual (revealed) activity/travel choices. Preferences then lead to individual's choices and in certain cases, if the person perceives a risk too high using a mode or at a destination, e.g., in the case of air travel, then the person is unlikely to use it. People's activity and travel choices have changed due to heightened security risks (which seems unevenly distributed across modes and destinations) though we do not know very well in what ways.

Often, people who have been traumatized perceive higher risks than is actually present. For example, after witnessing or viewing the events of 9/11, people likely perceive the risk associated with flying to be greater. (Though some people might avoid air travel for other reasons, such as an unwillingness to deal with the inconvenience at the airports.) They may also be less likely to use public transit or places where people congregate due to higher perceived risks. In the case of events such as 9/11 or the subsequent anthrax scare, statistical odds of the event actually happening to a person have little relevance to people. Due to information from the media and other people as well as the "dread-factor," people are likely to perceive higher risk outcomes.

The literature on risk perceptions provides some empirical insights. For example, Slovic (1988) identifies and examines gaps that often exist between the experts' view of risk and public perceptions of it. There are often public misconceptions of risk. For example, a study by Schneider et al. (2002) indicates that where pedestrians perceive higher risk is not necessarily the place where actual pedestrian crashes have occurred. So educating the public about risks is important. Furthermore, perceptions of risk evolve over time, e.g., in the case of cigarettes people in the US have become more aware of the link with lung cancer, though some years ago cancer risk was perceived quite differently.
Information plays a key role in peoples' risk perceptions. This role can be negative or positive. For example, exposure to promotional cigarette advertising can lead people to associate smoking with popularity and relaxation and these associations can overcome the negative perceptions of risks from lung cancer and other health-related problems. On the other hand, people can benefit from reliable information and education about health and security risks.

To assess peoples' response to security risks, we will use survey research. The survey will be designed to uncover the locations and scenarios within a region's transportation system that are most likely to be attacked. The questions to be explored are:

- Do they think that security threats are high when traveling by certain modes and to certain destinations?

- How have people changed their travel decisions due to higher security risks?
- How willing are they to report suspicious activity to the authorities?
- Whether and how they have minimized security risks? That is, what are some of the self-protection experiences and strategies that people use (e.g., what are the situations where they have felt most vulnerable and how have they managed to avoid them? Do they avoid locking into predictable travel patterns? How much do they rely on surveillance and communications technology to counter security threats to them?).
- What are the psychological costs of higher security risks?

These questions will determine if people are actually changing their travel patterns because of higher perceived risks. This will help us understand not only changes in people's behavior, but also the economic consequences such as decreased airline/public transportation ridership, lost tourism dollars, and more health problems due to stress. We will ask what specific locations they have avoided in the last year because of the events of 9/11. Additionally, we will ask if there are specific locations where they have felt anxiety because of higher security risks and what would make them feel more secure.

Understanding Risk Reported by Government Agencies: A Systems Model

Figure 3 (see page 13) shows the conceptual structure from a systems perspective. Government agencies and cities are likely to collect information about transportation system risks through surveillance and intelligence. Some cities do risk assessment, where risk depends on the likelihood of occurrence of certain events, the consequence of the event (if it occurs) and 1 - (one minus) system effectiveness. Moreover, cities/government agencies sometimes do scenario analysis, which looks at various modes of attack and the potential for "surprises." Cities can have preferences for various prevention, mitigation, response and recovery strategies. Each of these strategies can include measures related to engineering, enforcement, encouragement and education. Ultimately, these strategies are meant to minimize loss of life and property while allowing the transportation system to operate effectively and efficiently.

From the perspective of the cities and government agencies, we can explore the "reported" security risks within the transportation system. That is, which transportation systems within cities do officials believe are the most likely targets? Which ones are most vulnerable? Has the city done a security risk assessment? If so, how did they do it and what was the role of agencies such as law enforcement (police) and the federal government. This survey would collect information about the locations and scenarios within a region's transportation system that are receiving security funding and modes/destination that the city would like to make more secure in the future. We will compile information on existing state and city guidelines, practices and plans regarding transportation security and crisis response, (including an assessment of how security funds are allocated among transportation modes and agencies), identify areas of consensus (e.g., do most cities feel that their airports or transit systems pose the highest security risks), and have cities thought of potential "surprises."

Integrating Behavioral and systems perspectives: Spatial Analysis

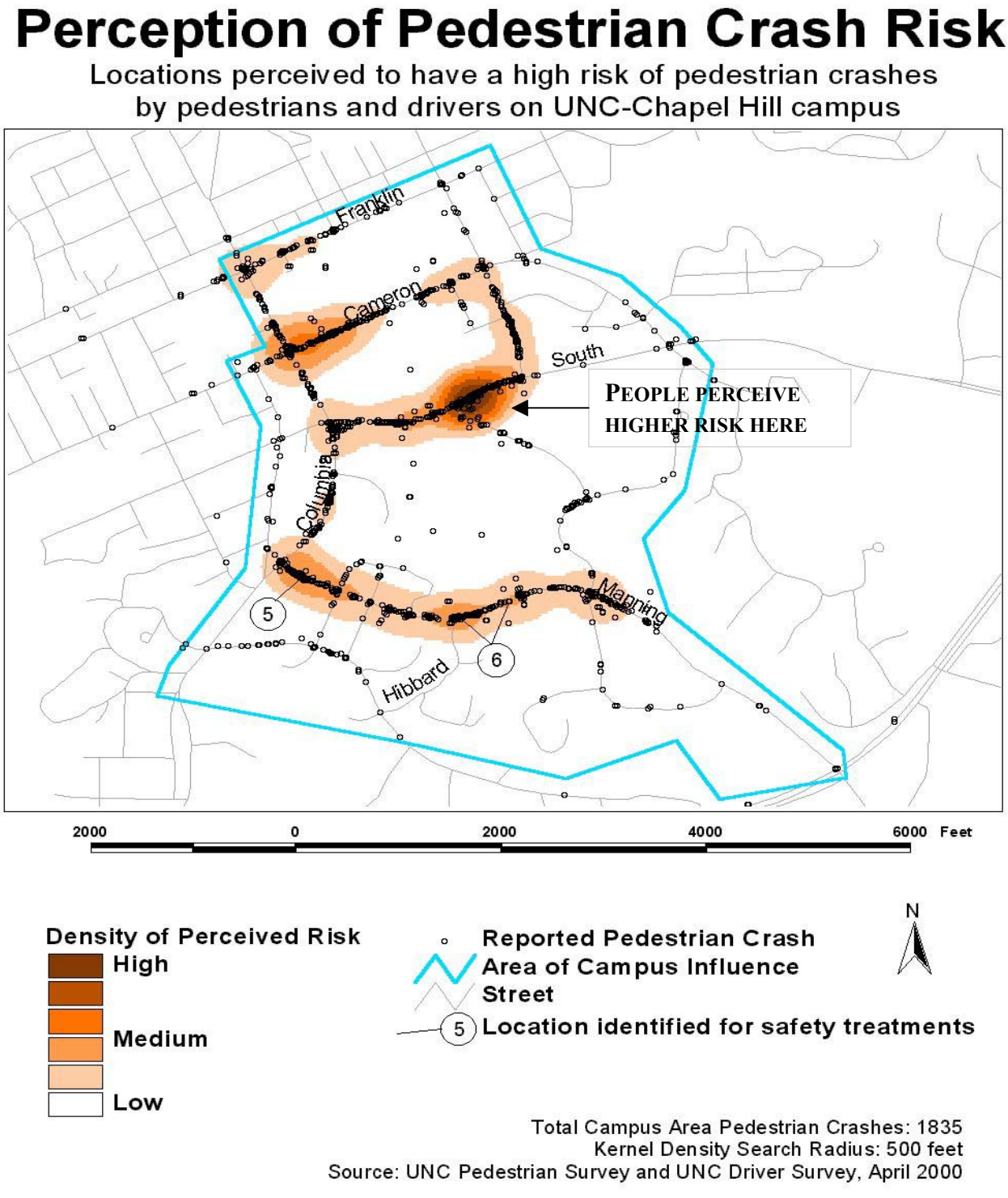
A comparison of the perceived security risks (obtained through the survey results) with city-and government-reported security risks will allow us to obtain a more complete picture of where potential hazards are concentrated within an urban region. This perceptions data can identify additional risks that people perceive, but may not yet be apparent to the city/government. This information will then be combined with the "surprise" scenarios to see where security violations are most likely to occur and how to plug the gaps.

Though a nationwide study will be desirable, it will be difficult to obtain the cooperation of the relevant cities and agencies. To pinpoint locations and factors associated with security risks, we need to work with government agencies within cities that deal with problems at specific locations and survey citizens who know the local transportation system well enough to pinpoint security risks. GIS analysis and citizen perception surveys can be done appropriately at this scale. Also, law enforcement jurisdictions are typically incorporated within cities and counties, so our scale should be urban regions or counties.

Both surveys would identify top locations of perceived and reported security risks. Models will identify statistically significant qualities of these locations (i.e. transportation modes, tourist/government/educational/athletic venues nearby, surrounding population density, proximity to CBD and surrounding population). Through our analysis, we will explain and interpret the transportation security results, pointing out transportation security gaps and potential strategies.

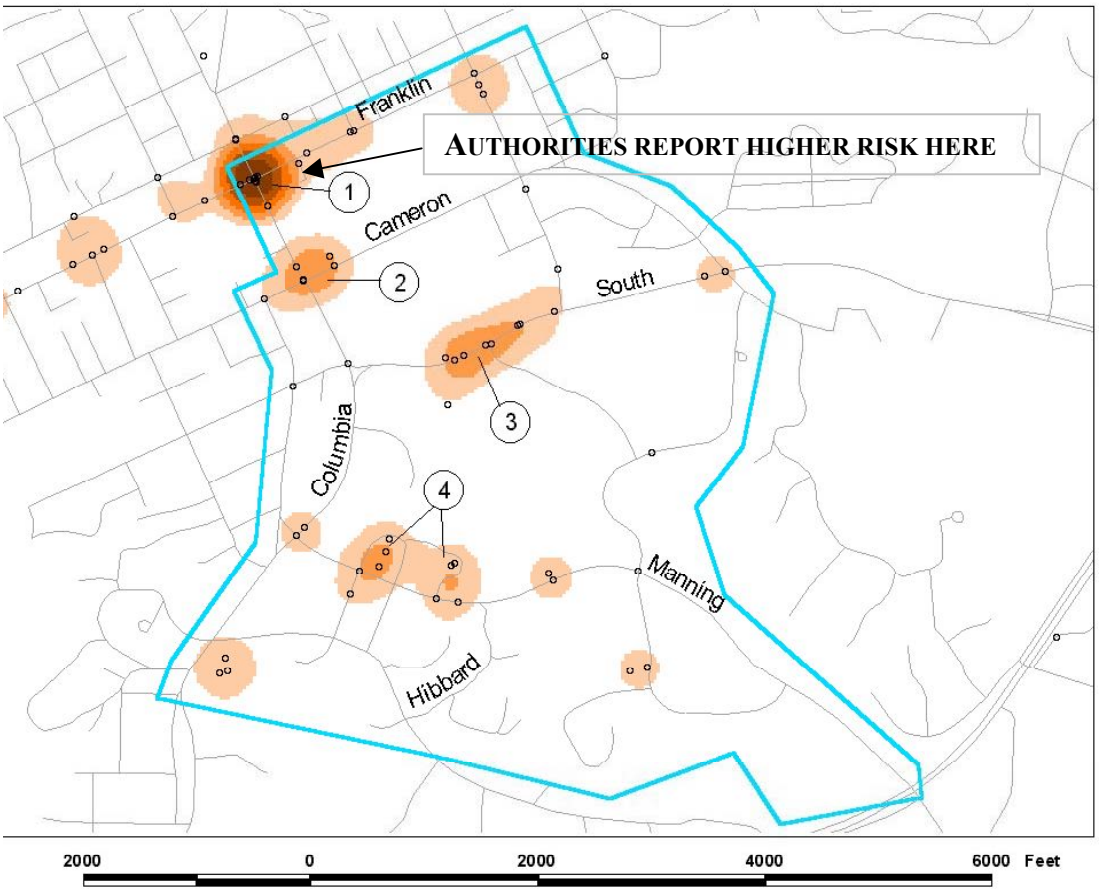
The spatial analysis of the data will compare the distributions of perceived security risks on various transportation modes and at various locations (Figure 4 is based on our earlier work in safety, but it is adapted to show a hypothetical diagram of where people could perceive greatest security risks) with the police/city-reported security risks (see Figure 5). If there is consensus between the public's perceptions and the reported security risks, then the high-risk locations are properly identified. If the two distributions are statistically different (more likely to be the case), then it may imply that certain modes and locations are perceived as higher security risks, though security violations have not yet occurred there, and perhaps there are modes and locations with city/government reported security risks that are not perceived to be dangerous by people. The analysis may further show that certain modes (e.g., transit and air) and high pedestrian/vehicular volumes and certain infrastructure features are associated with greater perceived and police-reported security risks. Moreover, people may perceive a higher security risk near some land use types, such as landmark buildings and stadiums. Our methodology can identify problematic modes and locations where certain preventive and response strategies may be most effective. As stated before, the strategies can encompass awareness and education of the public and stakeholders, to monitoring and enforcement, encouragement and infrastructure changes.

FIGURE 4: HYPOTHETICAL PERCEPTIONS OF HIGHER RISK DENSITY AS REPORTED BY PEOPLE



Reported Pedestrian Crash Density

UNC-Chapel Hill, 1994 to 1999



Pedestrian Crash Density
High
Medium
Low

Reported Pedestrian Crash
Area of Campus Influence
Street
1 Location identified for safety treatments

N

Total Campus Area Pedestrian Crashes: 57
Kernel Density Search Radius: 500 feet

CONCLUSIONS

This paper suggests that we need a comprehensive approach to understanding transportation security risks as they are perceived by individuals and reported by cities and government agencies. A behavioral approach to understanding risk perceptions is critical, given the rare nature of such events and given the fact that people need to feel secure about traveling by using various transportation modes. Cities and government agencies need to plan their systems with much greater emphasis on transportation security. In this environment, we need methods that can help us explore risk perceptions and point out possible strategies that can help cities deal with the transportation security problem. Such an approach is proposed in this paper and can be very valuable for cities and government agencies in planning to prevent security violations. Through input from people and cities/government agencies, it will identify the spatial distribution of "weak and vulnerable" transportation modes and locations that can be potential targets. The study will contribute by examining the spatial distribution of high-risk locations and their accessibility to perpetrators. Ultimately, the application of the methodology and results can help us plan better to enhance transportation security, while achieving the fundamental goals of the transportation system, i.e., moving people and goods. Finally, we will need test case cities to implement our spatially oriented security risk analysis methodology.

ACKNOWLEDGEMENTS

We acknowledge Southeastern Transportation Center's financial support. Mr. Robert Schneider was critical to the development of the key ideas and Ms. Rhonda Ryznar helped develop the safety methodology on which a lot of this work is based. Ms. Susan Faulkner helped summarize the "developments" presented in this paper.

REFERENCES

American Psychological Association. "Handling Anxiety in the Face of the Anthrax Scare." Psychology in Daily Life. Contributing Experts. 18 Mar. 2002. http://helping.apa.org/daily/anthrax.html Accessed on 3 Mar. 2002.

Bagdolato, Ed. "Cargo Security." *TR News.* On-line. Nov.-Dec. 2000 www.nationalacademies.org/trb/publications/trnews/trnews211.pdf Accessed on 10, Mar. 2002.

Boyd, Annabelle and John P. Sullivan. "Emergency Preparedness for Transit Terrorism." *TR News*. On-line. May-June 2000. www.nationalacademies.org/trb/publications/trnews/transit_security.pdf Accessed on 10 Mar. 2002.

Committee on R&D Strategies to improve surface transportation security. Improving Surface Transportation Security. National Academy Press. Washington DC. 1999.

Cross, Frank B. "The Risk of Reliance on Perceived Risk" www.flpc.edu/RISK/vol3/winter/cross.htm Franklin Pierce Law Center. Concord, NH. 1992. Accessed 3 Mar. 2002.

Flynn, Stephen E. "Transportation Security: Agenda for the 21st Century" *TR News*. Nov. – Dec. 2000. On-line. www4.trb.org/trb/homepage.nsf/web/security Accessed on 10 Mar. 2002.

Libaw, Oliver. "Weighing the Risks: Experts Say Widespread Concern Over Anthrax is Appropriate." ABCNEWS.com 25 Oct. 2001. http://abcnews.go.com/sections/us/DailyNews/anthrax_weighingrisks011025.html Accessed on 3 Mar. 2002.

Macko, Steve. "DOT Report Says U.S. Transit Systems Vulnerable to Terrorist Threat" excerpted from *ERRI Daily Intelligence Report*. 28 Feb. 1998 Vol. 4 - 059.http://www.emergency.com/transt98.htm Accessed on 18 Mar. 2002.

Macko, Steve. "GAO Says Cities Should Conduct Risk Assessment of Terrorism Threats." http://www.emergency.com/gaombio.htm Excerpted from *ERRI Daily Intelligence Report* - ERRI Risk Assessment Services – Monday May 11, 1998. Vol. 4 – 131. Accessed on 16 Mar. 2002.

Magaw, John. "Statement of John Magaw, Under Secretary of Transportation for Security before the Aviation Subcommittee." 23 Jan. 2002. On-line. http://199.79.179.73/tabula/test/Magaw1.htm Accessed on 20 Feb. 2002.

Mehta, Michael D., PhD. "Chemical or Biological Terrorism: Is the Threat Real?" PowerPoint presentation on the web of unknown date of authorship. University of Saskatchewan. http://www.art.usask.ca/policynut/bioterror.Ppt. Accessed on 3 Mar. 2002.

Mosley, Bill. "DOT Announces Action Plan for Transportation Infrastructure Relying on GPS." DOT 22-02. 7 Mar. 2002. http://www.dot.gov/affairs/dot02202.htm Accessed on 19 Mar. 2002.

Nelson, Kurt. R. "Policing Mass Transit." FBI Law Enforcement Bulletin. Jan. 97. Vol. 66 Issue 1. ISSN: 00145688. AN: 9702165696. Accessed on 19 Feb. 2002 through EBSCOhost.

Slovic, P. Perception of risk. Science, 236, 280-285, 1987.

Schneider R. A. Khattak and R. Ryznar, Factors associated with pedestrian crash risk: Integrating risk perceptions and police-reported crashes, Paper presented at the 81st Annual Transportation Research Board Meeting, On TRB CD-ROM, 2002.

TRB Panel for Session 148. "Spotlight on Security and Recovery." Transportation Research Board. 14 Jan. 2002. http://gulliver.trb.org/am/session_148.asp Web audio presentation accessed on 3 Mar 2002.

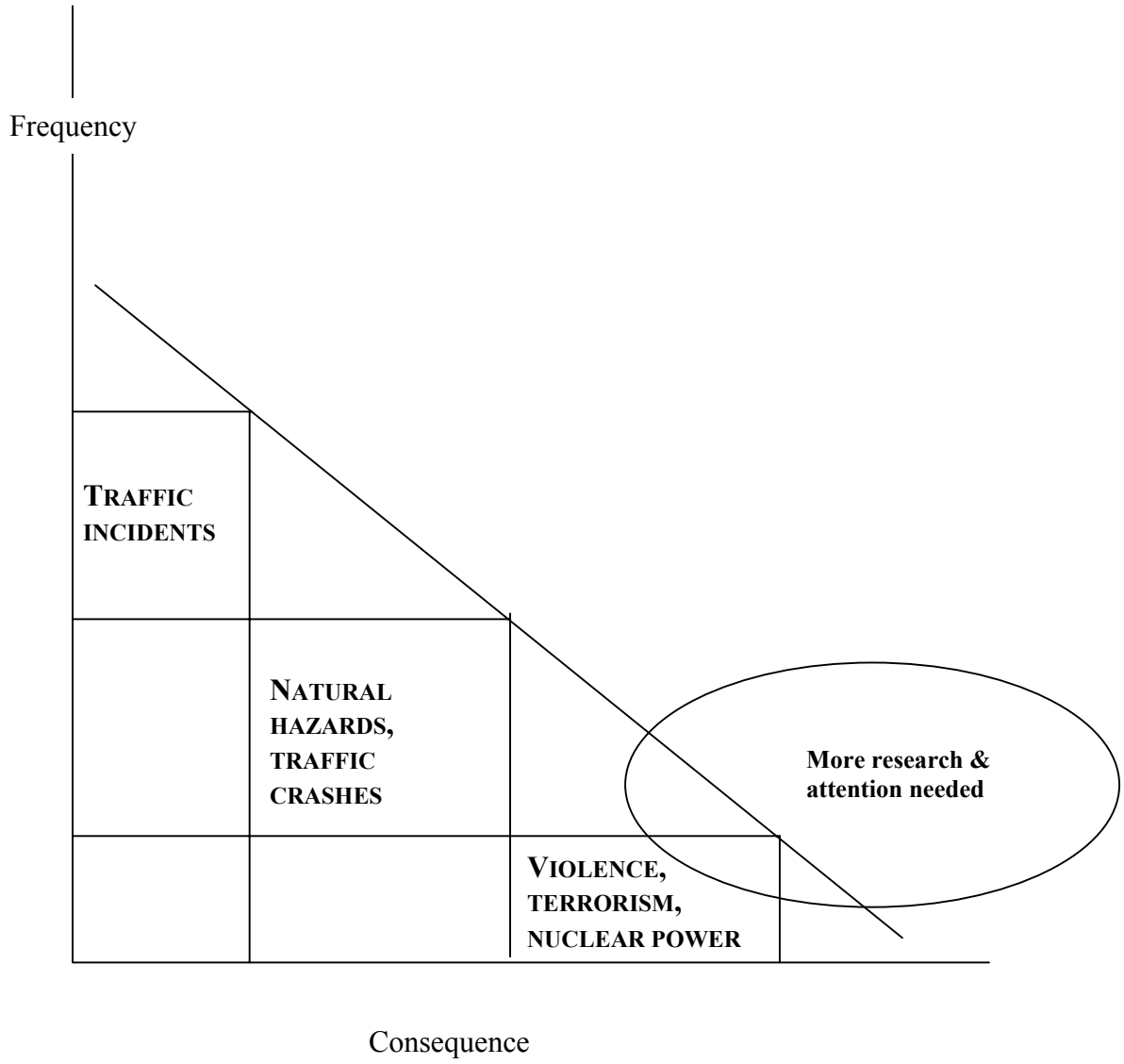


FIGURE 1: FREQUENCY AND CONSEQUENCES OF RISKY EVENTS.

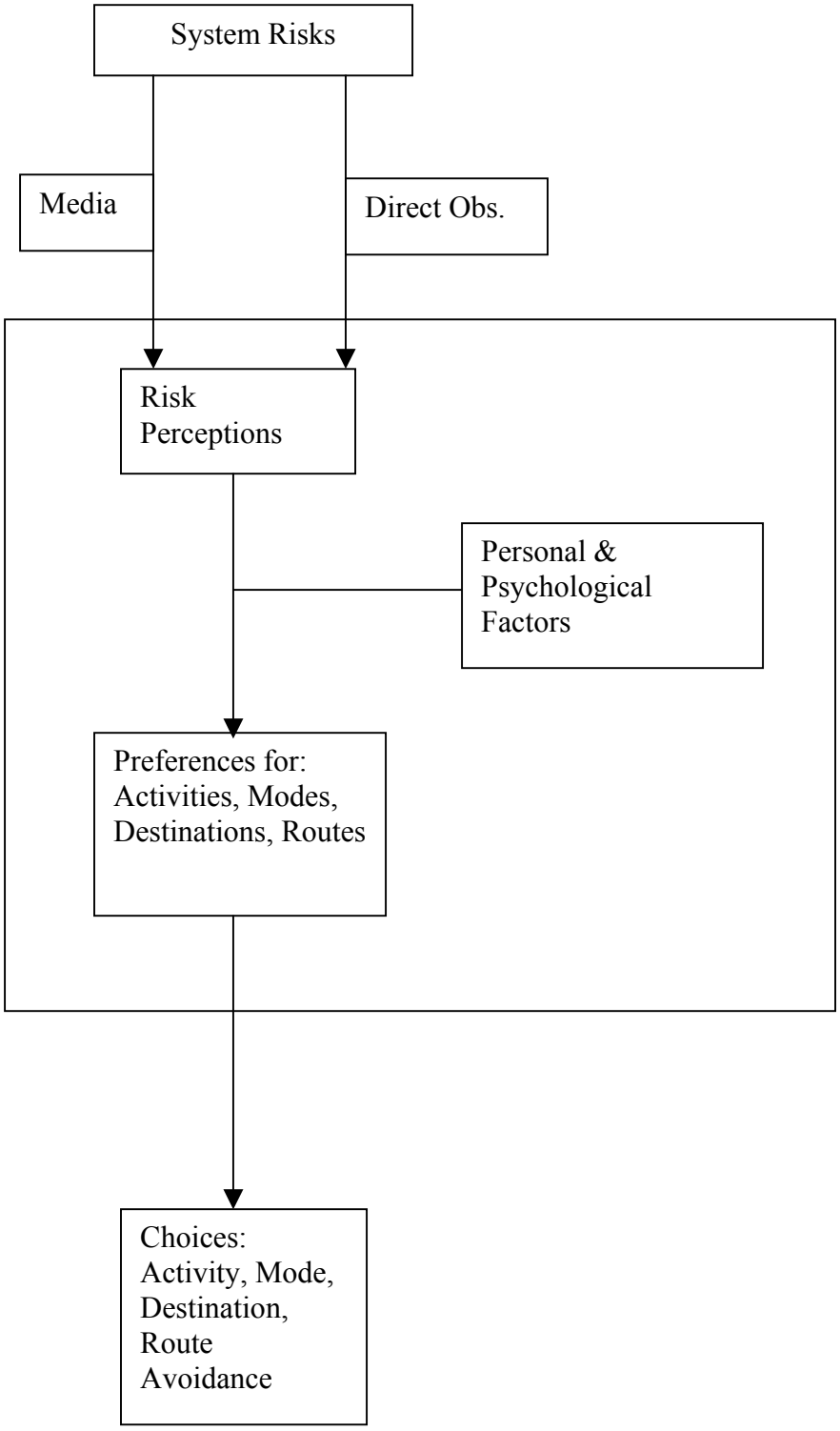


FIGURE 2: A BEHAVIORAL MODEL OF RISK PERCEPTIONS AND DECISION MAKING

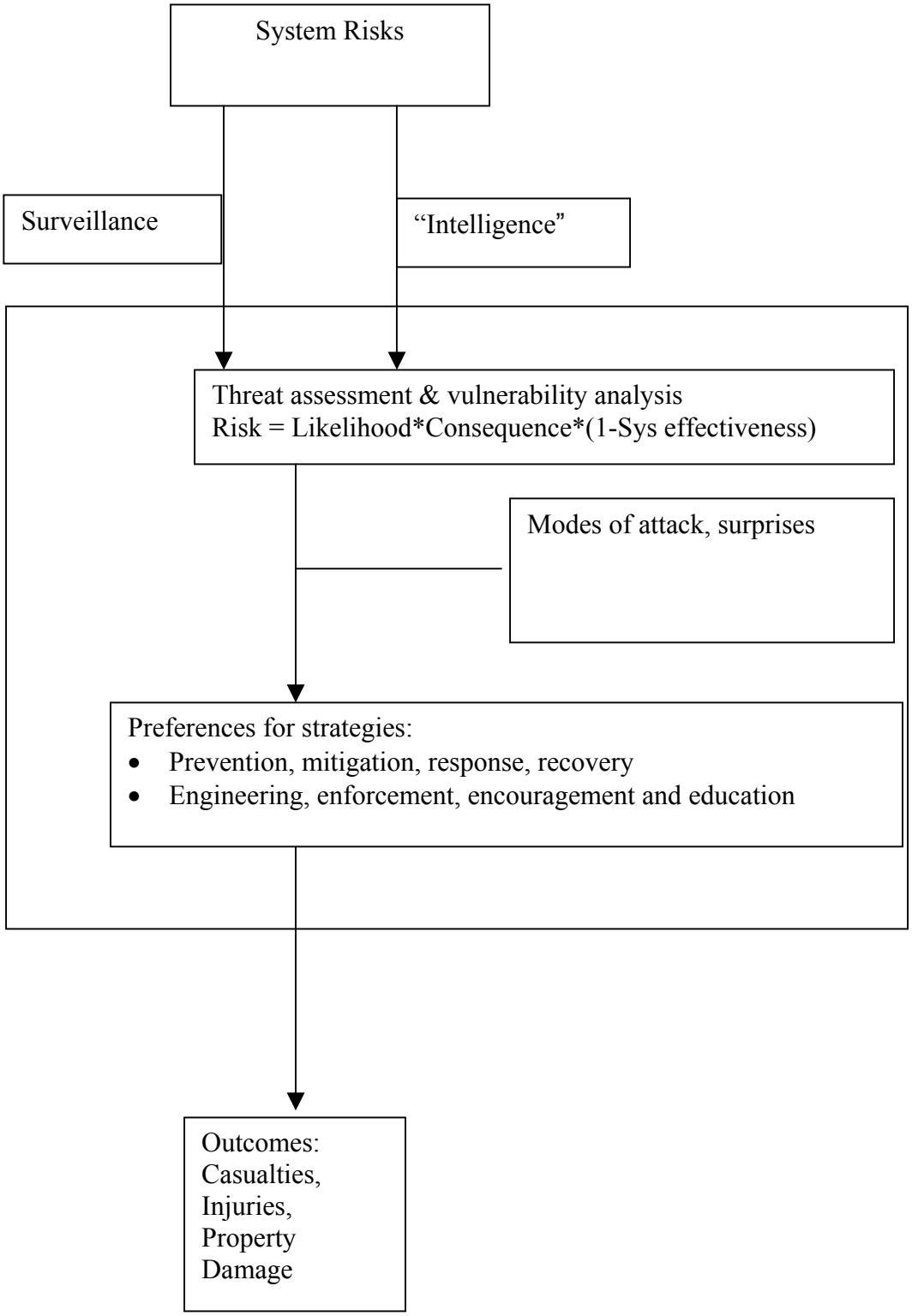


FIGURE 3: A SYSTEMS MODEL OF REPORTED RISKS

THE ROLE OF TRANSPORTATION MANAGEMENT CENTERS (TMCS) IN HOMELAND SECURITY

Michael C. Pietrzyk, P.E.
Patricia Turner
University of South Florida

INTRODUCTION

The events of September 11th, illustrated that when the Pentagon was attacked, the Northern Virginia Transportation Management Center (TMC) not only served to restore and maintain transportation services, but also served as the communications hub and centralized control point for all security and emergency response activities related to that act of terrorism. Planning for transportation related contingencies and taking the necessary steps in advance that might minimize the negative effects of disruptions to transportation services, is paramount to the functionality of TMCs. Furthermore, given the extent of communications and control infrastructure typically operated through a TMC, and the extent of multiple agency coordination for transportation emergency response directed through a TMC, it is beneficial to determine how TMCs can be effectively utilized in the event of any future homeland security threats.

As a result of 9/11, many communities have started to re-examine the potential for threat in their regions as well as their response capabilities. When emergency service providers and TMCs share information, each is capable of performing more effectively thereby improving public safety. In addition, resource sharing improves efficiencies; response times and maximizes limited resources.

Fortunately, for most communities, the waters have not been tested in the event of a terrorist attack. However, during any future homeland security threats, TMCs must be fully prepared to manage the roadways and make sure that people remain out of harms way and that first responders safely reach the scene. This white paper examines possible roles that TMCs can play in the event of homeland security threats and raises other questions that should be considered in the design and operations of existing and future TMCs. Procedures, policies, and communication protocols that should be in place between the TMC and the Emergency Operations Center (EOC) during potential terrorist attacks are discussed. Information that should be monitored, and how that information is verified, shared, and disseminated is also discussed. Finally, this paper recommends improvements to the existing protocols to maximize communication and coordination between the EOC and TMCs during homeland security events.

As a reality backdrop to this investigation, the authors interviewed key individuals from the Office of Emergency Management (OEM), Florida Department of Transportation (FDOT) Transportation Management Center, and SunGuide/SmarTraveler Advanced Traveler Information Services (ATIS) in Miami Dade County, Florida to determine the roles of the EOC

and the TMC in preparing for potential homeland security threats[8]. Information was gathered about existing communication procedures between the EOC and the TMC, potential security incidents that trigger information exchanges, current methods to gather and verify information, types of information exchanged, methods of information dissemination, and capabilities or infrastructure for providing adequate safety and security that were lacking.

EMERGENCY MANAGEMENT IN FLORIDA

In the aftermath of the recent terrorist attacks on the World Trade Center and the Pentagon, Florida and other states have begun to look far more closely at ways to protect and monitor what are considered to be vulnerable services and industries. While there have not been any successful acts of terrorism committed in Florida, the potential is high because of the number of facilities within the State associated with tourism, the military, and State and federal government activities. Transportation and commercial infrastructure, cultural, academic, research, military, and athletic facilities also constitute ideal targets for terrorist attacks with the intent of causing catastrophic levels of property and environmental damage, injury, and loss of life.

Because Florida is vulnerable to a variety of hazards that threaten our communities, businesses, and the environment, the State's *Comprehensive Emergency Management Plan (CEMP)* ensures that Florida is adequately prepared to deal with these hazards. The CEMP outlines the roles and responsibilities of the State agencies, special districts, and local governments in a disaster, coordinates response and recovery activities, and unifies the efforts of all those involved to reduce the effects of the emergency and/or disaster. The Plan addresses the four phases of emergency management (preparedness, response, recovery, and mitigation) and is divided into three sections: Basic Plan, Emergency Support Function (ESF) appendices, and Hazard Specific annexes.

Florida has adopted the basic architecture of the Federal Response Plan that groups the appropriate agencies into a "support function" team managed by one lead agency. The Florida Department of Transportation is the lead agency responsible for ESF 1 – Transportation Appendix of the CEMP. The ESF outlines the responsibilities of the transportation system in assisting with evacuating persons from threatened or immediate danger; transporting response personnel, equipment, materials and supplies; monitoring and controlling traffic; reporting on infrastructure damage; and clearing obstructions and debris from the transportation infrastructure.

In accordance with Chapter 252.38 (1) of the Florida Statues, county governments are responsible for maintaining an emergency management program that includes all government, private and volunteer organizations involved in emergency management. County governments must also prepare and adopt an annex for terrorism incident response as part of their local comprehensive emergency management plan. Guidelines for developing the annex are contained in the CEMP Terrorist Incident Response Annex, which defines statewide policies, program, and procedures for local agencies to follow to prepare for, respond to, and recover from a terrorist or cyber terrorist attack.

[8]The authors interviewed Chuck Lanza, Director of the Miami-Dade County Office of Emergency Management, Jesus Martinez, the FDOT ITS Manager in the Miami District office, and Fred Levinson of SmartRoute Systems in Miami on February 22, 2002.

DEFINING THE TERRORIST THREAT

Terrorist attacks not only hold the potential for massive destruction, but also require a response from a multitude of organizations, from law enforcement and emergency services to engineers and heavy equipment operators. In order to coordinate the appropriate response, the EOC must first determine whether an incident can be classified as a terrorist act.

Detecting a known, suspected, or threatened terrorist attack is the first step in the terrorism event response process. Detection may occur through communication centers, law enforcement intelligence efforts, warnings, or announcements by the perpetrators, characteristics of the event, such as an explosion or chemical recognition, etc. Next, proper agencies are notified and a threat level established as either minimal, potential, credible, or a Weapon of Mass Destruction (WMD) incident. Each threat level provides for an escalating range of actions to be implemented concurrently for crisis and consequence management. Minimal threats may involve normal liaison notifications and/or placement of resources on a heightened alert. Potential threats are intelligence or an articulated threat not yet verified as credible. Credible threats are likely to occur and may involve a weapon of mass destruction. A WMD incident is confirmed by the occurrence of the event, and response is primarily directed toward public safety and preserving human life.

Terrorism response mechanisms may be triggered by several criteria, including[9] 1) a credible threat or actual event involving cyber, biological, nuclear, incendiary, chemical, or explosive agents; 2) a call received with information regarding an incident of unknown origin, which has created a large number of casualties in a short period of time; 3) arrival of a unit finding victims displaying signs and/or symptoms of a biological, nuclear, or chemical event; 4) any incident in which a group of victims seem to be affected with similar symptoms for which the cause is unknown; 5) any sudden or repeated occurrences of any illness or disease not typically seen in a geographical area; or 6) any incident that indicate cyber intrusions or cyber attacks.

The greater Miami area serves as the "gateway to South and Central America", particularly in regards to international commerce and banking. There are numerous potential terrorist targets in the South Florida region including two nuclear plants, Turkey Point in South Miami-Dade County and one in Palm Beach County, water treatment plants, courthouses, seaports, airports, federal buildings, SouthCom and other military installations. Miami handles the bulk of all U.S. trade with Latin America and is also heralded as the "Internet Coast", ranking 5th in the world among telecommunications centers. The Miami International Airport handles more than 33.8 million passengers and is the number one international freight airport in the U.S., and the Port of Miami is the cruise ship capital of the world. Any act of terrorism to this area would require an immediate and regionally coordinated response action.

EMERGENCY MANAGEMENT AND TERRORISM RESPONSE PLANNING IN MIAMI DADE COUNTY

The Miami-Dade County Office of Emergency Management (OEM) coordinates disaster response in South Florida by maintaining comprehensive emergency management plans (CEMP) for the County and 30 municipalities and maintains a high state of readiness. As part of the Plan, the OEM maintains a Local Terrorism Incident Response Annex, which outlines plans and procedures for responding to acts of biological, nuclear, incendiary, chemical, or explosive

[9] State of Florida Division of Emergency Management, *Local Terrorism Response Annex*, May 8, 2001, p. 12.

terrorist incidents. The Plan also contains a Transportation ESF-1, which addresses transportation support functions during the preparedness, response, and recovery phases of an incident or disaster. Emergency response partners include members of public safety, human services, infrastructure, operations and recovery, and planning and information and resource management.

A new 22,000 square-foot Emergency Operations Center (EOC) was opened in May 2000 to improve coordination by disaster preparedness agencies. The EOC, located in the Miami-Dade County Fire-Rescue Department headquarters building, has network capable computers, upgraded telecommunications, a media center with direct video feed, a 38 station call center, seven (7) conference rooms, closed circuit video, media monitoring stations, and electronic information displays.[10]

Miami-Dade County prepares for homeland security threats by maintaining several departments and agencies with the expertise, training, equipment, and plans including: three (3) hazardous materials response teams, two (2) urban search & rescue task forces; fire suppression; medical treatment, triage and transportation; tactical extrication, first line specialized medical care; Environmental Crimes Investigation; Special Weapons and Tactics (SWAT); bomb squad; intelligence and evidence gathering coordination (local, state and Federal); hostage negotiators; evacuation crowd control; biological and chemical agents laboratory; special events command and control; and on site decontamination equipment.[11]

To maintain readiness for deployment and emergency response services, the OEM regularly conducts annual and bi-annual mass casualty and incident drills with city and county departments, hospitals, fire departments, law enforcement, power companies, nuclear plant, rail, seaport, and airport. Through these drills, agencies rehearse the necessary operational and communications procedures. Some recent training and drills include:[12]

- WMD training for first responders
- Turkey Point Nuclear Power Plant (one of four nuclear plants in Florida) drills
- Medical scenario drills
- Quarterly drills with Florida Power and Light
- Chemical Weapons full field exercise
- Biological /Weapons of Mass Destruction Table Top drill
- Local Emergency Planning Committee (LEPC) drill (HAZ MAT)
- Civic Center Mass Casualty Disaster drill for hospitals
- Bi-annual Amtrak / Tri-Rail (commuter rail) drills
- City of Hialeah Biological Tabletop Exercise
- Seaport Weapons of Mass Destruction drill
- Annual Miami International Airport drills

Local law enforcement has monitored terrorist activity for years partly due to the large anti- and pro- Castro groups in the Miami-Dade area. Because many of the suspected 9/11 terrorists had a Florida connection, area law enforcement agencies formed a regional intelligence-gathering alliance called the Anti-Terrorist Homeland Defense Regional Intelligence Network. The Miami Police Department created an Anti-Terrorist Security and Intelligence Task Force – made up of

[10] Miami-Dade Office of Emergency Management*, Emergency Preparedness Report*, August 2001.
[11] http://www.co.miami-dade.fl.us/oem/home.htm
[12] *Ibid.*

municipal police units as well as county, state, and federal agencies – to work with the alliance to establish a regional network of intelligence sharing, identify potential domestic and foreign security threats, identify potential targets and conduct threat assessment, conduct security surveys at key installations, and make recommendations to tighten against intrusion.[13] Other activities since 9/11 include the OEM more closely examining Miami's critical infrastructure such as water supplies, reservoirs, treatment plants, nuclear power plants, major ports and airports, key inland waterways, and critical bridges; adding a biological component to the local Terrorism Response Annex; scheduling more mass casualty, biological, and incident drills; and heightening building security.

TRANSPORTATION MANAGEMENT IN MIAMI-DADE COUNTY

Traffic management centers (TMCs) monitor real-time information obtained from various components of ITS and share the information to improve incident response time and coordination, adjust traffic controls, and keep motorists informed of traffic and weather conditions. TMCs serve as the focal point for monitoring, controlling and coordinating various functions for managing a regional transportation system. At a TMC, information about the region's freeways, traffic signals, or transit services is collected and processed, and combined with other operational and control data to initiate control strategies to effect changes in operation. It is also a center for communicating transportation related information to the media and the traveling public.[14]

In the Miami area there are currently three (3) TMCs responsible for operating and maintaining major transportation facilities or properties, including freeways, arterials and transit properties. These include: the Florida Department of Transportation (FDOT) District 6 Freeway Management Center, Miami-Dade County Traffic Control System Center, and Miami-Dade Transit Agency Central Control, Special Transportation Services, and Customer Information Centers. For the purposes of this white paper, only the FDOT TMC is discussed.

FDOT District 6 Freeway Management Center[15]

Currently, the FDOT operates a very small (interim) freeway management center for the Miami area. However, construction is underway on a new $6M building (32,000 square feet) where the Florida Highway Patrol will share space with regional highway and transit agencies. The center, to be completed by late 2002, includes a wall for 12 integrated video screens to monitor real-time traffic, as well as management software that eventually will coordinate automated incident detection and traffic system management in Palm Beach, Broward, and Miami-Dade counties. Four Variable Message Signs (VMS), 16 detector stations, and 27 CCTVs are now in an operational testing phase and 15 more freeway and arterial VMSs, trail blazers, and ramp meters are planned.

The TMC's planned infrastructure includes: closed-circuit television cameras for traffic monitoring; advanced traffic signal control for better timing and incident response; emergency dispatch management centers with dispatch assisted by Geographic Information Systems (GIS);

[13]De Valle, Elaine. "Region Pooling Security Efforts", *Miami Herald*, September 27, 2001.
[14]Center for Urban Transportation Research, *Miami-Dade County Transportation Management Center Functionality Study*, December 2001.
[15]*Ibid.*

freeway service patrols with fleet tracking and dispatch assisted by Automated Vehicle Location (AVL) systems; real-time transit system information, with AVL-assisted fleet tracking and dispatch; VMS's to advise drivers of traffic and weather events; fiber optic and wireless communication systems to assist interoperability; and highway advisory radio.

The existing control center (for freeway and incident management) is 2,600 square feet. The control center operates on a UNIX platform, and the language code is C. Workstations are being upgraded to Windows 2000 platform. Incident data is gathered through both video image detection and inductive loops. The data collected is processed in the local 170 controller and transmitted back to the interim control center via leased BellSouth lines (leased lines from hubs to control center, FDOT fiber from devices to hubs). The data gathering process is fully activated at this time. However, additional detectors will be added in July to the enhance detection capabilities.

The FDOT's TMC is currently connected to FHP's computer-aided dispatch (CAD) system, which enables the FDOT control center operators the ability for near real-time monitoring of incidents FHP is handling. FHP can view the video images of the incidents FDOT is monitoring, plus FHP is capable of controlling the FDOT cameras if needed. The TMC shares information over the phone with Miami-Dade Public Works, Shadow Traffic, and the fire department during incidents. The TMC also is equipped to communicate with its continuously patrolling, 25-vehicle fleet of Road Ranger vehicles, each equipped with RF-based AVL, to respond to freeway and expressway incidents.

The only formal information sharing with other agencies that currently exists is during the local freeway incident management meetings, where crash response procedures are reviewed. The Freeway Incident Management Team meetings are scheduled every other month, and include members of FDOT and its TMC, Florida Highway Patrol, Department of Environmental Regulation & Monitoring, Miami-Dade Public Works, Fire, Miami-Dade Police Department, City of Miami Police, and the Southwest Florida Water Management District.

Partnership success with SmartRoute Systems, Inc. for South Florida Advanced Traveler Information Services (ATIS), which initiated SmarTraveler, a traveler information service in May 2001, will be critical toward establishing coordinated freeway and incident management in the area. SmarTraveler disseminates a range of real-time information services to travelers in the three counties through a variety of media, including radio, television, Internet, toll-free telephone lines, message signs, and customized blast emails. Travelers receive information on issues such as: highway travel times, incident locations, construction locations and schedules, transit conditions and schedules, special events, HOVs, parking, tourist travel, and transportation agency contacts. Also SmarTraveler's interactive voice response (IVR) telephone system allows travelers from Miami to West Palm Beach to get real-time traffic information by dialing into the system from a cell or landline telephone. In the future, it is anticipated that callers in the region will be able to access the system by dialing 511 (the U.S. DOT initiative to establish a nationwide three digit call number for traveler information).

TMC ROLES DURING HOMELAND SECURITY EVENTS

Disaster response is one of the most crucial elements of any government as citizens look to the local, state and federal governments to be fully capable and prepared to respond to disasters including any future terrorist incidents. During the Pentagon attack, 50 local, state, and federal public safety agencies responded to the incident[16].

By Statute, the Miami-Dade OEM coordinates disaster response and planning for the residents of the County and works with public and private agencies to develop plans, programs, and projects that support the four principles of emergency management: mitigation, preparedness, response, and recovery. The guiding documents to prepare for, respond to, and recover from disasters and terrorists incident are the Miami-Dade CEMP and corresponding Terrorist Incident Response Annex.

Support roles for transportation agencies are detailed in the County's ESF-1 Transportation Standard Operating Procedure (SOP). Historically, the transportation component, in which Miami-Dade Transit Authority is the lead agency, has been utilized to evacuate vulnerable populations during hurricanes, assist public safety in traffic control, clear debris from infrastructure, conduct emergency repair and maintenance on infrastructure, and inform the public by providing transportation information and maps. The SOP has not been updated since the 9/11 terrorists attacks.

The following sections explore existing communication between the EOC and the TMC, potential security incidents that trigger information exchanges, methods to gather and verify information, types of information exchanged, and methods of information dissemination.

Communication Protocols

Currently, there are no capabilities to directly and automatically share data or video between the FDOT TMC and the Miami-Dade County EOC. The SmarTraveler Center does have a "preliminary" communications relationship in place with the EOC and are continuing to examine ways to improve information sharing and coordination in order to get more information out to the public as quickly as possible. For example, during a recent HazMat event (a fire at an asphalt plant), the SmarTraveler Center deployed a helicopter and reported on wind and weather conditions and fire smoke patterns directly to the EOC. The SmarTraveler Center sends blast email and fax alerts to the EOC, and the agencies also have the capability to communicate with each other via NexTel Direct.

The FDOT and the EOC lack a formal structure within which to interact, however, each agency has representatives to provide the communication link for a coordinated response to a terrorist event. The EOC has two individuals that coordinate HAZMAT or radiological events. These coordinators recently visited with the SmarTraveler Center to examine ways to improve information sharing and coordination. The FDOT has a designated emergency operations coordinator. However, it was felt that if this individual were not available communication during emergency incidents would somewhat breakdown. According to the EOC, some County departments (not FDOT) do not cooperate in times of emergency operations due to political or

[16] Public Safety Wireless Program. A*nswering the Call: Communications Lessons Learned From the Pentagon Attack,* January 2002.

institutional "turfism". There was recognition that after the new FDOT TMC becomes operational; it will then be absolutely necessary to formalize communication protocols between the FDOT and the EOC.

The EOC believes they have the capabilities to respond to any event, but since 9/11 the county's emergency response plan, including FDOT's responsibilities, has not been upgraded. The EOC would cooperate with other adjacent counties during incidents that span across jurisdictions, and the county EOC geographically closest to the incident would take the lead. In the event of a roadway blockage, bridge or infrastructure explosion, the EOC would activate and communicate with the TMC.
The most critical component of any EOC is communications. Ultimately, to be fully effective before, during, and after their response, public safety officials, throughout all levels of government, must be able to communicate with each other. In Miami-Dade county, as might be the case in other metropolitan areas, all the necessary communication protocols are not yet in place, but the understanding to get them in place is.

Communication Challenges
Communication system interoperability to ensure clear communication within and among city departments and among federal, regional, state and local entities responding to disasters and terrorist threats or attacks is imperative. Many communities, however, lack the needed bandwidth for police, fire, emergency medical services, transportation, and other public safety personnel to communicate within their own agencies, much less across agency lines. There must also be reliable means for communication with the public to alert them to potential threats and provide them timely information on the status and effectiveness of response efforts. New opportunities for interoperability are possible since the FCC recently allocated the list of 5-9 GHz for use in transportation agencies.[17]

Alternative communication vehicles should be available in the event of power outages or other events that disable the primary communication mechanisms. Unfortunately, the importance of this particular point was fully realized during the Hurricane Andrew devastation of 1992 in Miami-Dade County. Since that time, the FDOT has purchased satellite radios, and invested in upgrading their microwave communications network. The EOC upgraded their radio system as well.

Information Gathering
Very little real-time information gathering exists (except for freeway/expressway speeds and travel times at the SmarTraveler Center), and sharing of real-time information, mostly video, does not occur among all the TMCs in Miami-Dade County at the present time. Normally, there is no real-time information gathering by the EOC, except just prior to, during, and after major storms. However, Turkey Point nuclear plant has sirens and recorded voice messages that can be remotely activated when the EOC detects a radiation level problem. No mobile video technology is being used in the County, however the SmarTraveler Center and the EOC air rescue fleet can transmit video.

[17]Public Technology, Inc., *How Can We Work Together? -A Guidebook to Smart Response through Coordinating Local Public Safety & Transportation Communications & Technology,* US Department of Transportation-Federal Highway Administration, p.8, 2000.

Information Verification
Information that the EOC receives is usually second or third hand, unless they have a helicopter at the scene. They usually receive about 20-30 calls about an event from observers or other public agencies. The SmarTraveler Center receives very few bogus calls, and blast emails that come from the EOC has an identifier in the message. The increasing number of freeway monitoring cameras and traffic detection devices being installed by FDOT, SmarTraveler Center, and others will add greater verification capabilities in the future.

Information Sharing
The EOC realizes that they need to "connect" to other centers (e.g., National Weather Center, FDOT, etc.) and need ALL the information that is available (particularly FDOT freeway video surveillance) in order to maximize their use of existing infrastructure. Blast faxing (thru email) is the most common form of information dissemination. An instructional video has been prepared as part of a public safety campaign. They also provide information on the County's Warning Point (24-hour hotline thru the police department).[18] Also, FDOT is currently exploring opportunities to share their fiber network, which would give the EOC the capability to receive video images from the TMC.

Information Dissemination
As mentioned previously, since May 2001 the SmarTraveler Center serving Miami-Dade and two other adjacent counties (Broward and Palm Beach) via public-private partnership with FDOT and several other regional public agencies is now the means for information dissemination from the TMC. They have more video and non-video data related to transportation than anyone in the area, and they disseminate primarily through the Internet and an interactive voice response (call-in) system. The FDOT, as it did during 9/11, can also communicate key information to the motoring public via roadside or overhead dynamic message signs. The video images from the TMC are soon to be shared over the Internet by the end of 2002. The SmarTraveler Center is also working with the EOC to simplify and assist their information dissemination needs because they already communicate with the general public as well as many local public agencies. Again, the eventual implementation of a single call for real-time transportation information ("511") will certainly aid in information dissemination.

POSSIBLE ROLES FOR TMCS DURING HOMELAND SECURITY THREATS

Not all TMCs are equipped and structured to gather and disseminate real-time traffic information like those in Miami. However, many of the emerging centers are following similar plans for design or upgrade. The element of advanced traveler information coupled with advanced traffic management serves best during times of incident management and any homeland security event. For TMCs that do have both capabilities, either directly or indirectly, possible regional roles and responsibilities such as those noted in Table 1 can be possible. Regional is typically defined as the total area of impact for a particular event or incident.

[18] *Miami-Dade County TMC Functionality Study*, prepared by University of South Florida-Center for Urban Transportation Research, p.21, December 2001.

TABLE 1. POSSIBLE ROLES FOR THE TMC DURING HOMELAND SECURITY THREATS

Response Element	TMC Role
Communication	**PRIMARY** (Only if the regional TMC includes advanced traveler information capabilities and formal communication protocols are established)
Information Verification	**INDEPENDENT** (Each autonomous TMC in the region that does exist should be responsible for verifying the information it is gathering BEFORE it is shared regionally)
Information Sharing	**AS NEEDED** (If a regional TMC can provide the mechanism for regional information sharing, most should be designed to, then each information gathering agency can establish their own formal relationship for sharing of information)
Information Dissemination	**PRIMARY** (Only if the regional TMC includes advanced traveler information capabilities and formal communication protocols are established)

CONCLUSIONS AND RECOMMENDATIONS

From this investigation, there is very little interaction (real-time sharing of information) among all the transportation management centers and emergency management operations, and an overall formal plan for establishing compatible communication interfaces and protocols between transportation management centers is yet to be developed. If this is the case in the greater Miami area, it most likely is the case in many metropolitan areas in the U.S. Emerging advanced traveler information systems, similar to the South Florida SmarTraveler Center, can provide the much-needed link for information communication and dissemination. In addition, and perhaps most importantly as a result of this investigation, it is also imperative to completely and formally involve EOC and other emergency response representatives in the planning, design, and deployment of regional TMCs in order to maximize homeland security capabilities.

TRANSPORTATION NETWORK VULNERABILITY ASSESSMENT: A QUANTATIVE FRAMEWORK

Karthik Srinivasan, Ph.D.
Vanderbilt University

INTRODUCTION

Even prior to the September. 11th attacks on the World Trade Center, the vulnerable state of infrastructure systems including transportation systems was highlighted in the report card on America's Infrastructure (ASCE, 2001). The events of September. 11th in retrospect, have revealed the extent of vulnerability and the massive and pervasive consequences of such attacks on transportation systems. These events have highlighted the fact that disruptions to transportation systems, be they man-made or naturally inflicted, have far-reaching consequences in terms of safety and security of citizens, massive infrastructure losses (Giuliano, 1998; Boarnet, 1998), mobility and accessibility of people (reduced demand for air-travel), economic viability of transportation system operators (e.g., airline companies), and the efficiency and the vitality of the economy. It is evident that the threat, the likelihood, and consequences of such disruptive system attacks are escalating drastically. Faced with these threats, there is an urgent need for systematic efforts to: i) protect the physical well-being and safety of users, ii) reduce the vulnerability of critical transportation infrastructure and services, and iii) minimize the economic impacts of such disruptions.

Despite this burning national need, there is a limited knowledge base and understanding of the likelihood, and consequences of such disruptive attacks on the transportation infrastructure. This shortcoming can be primarily attributed to a) lack of significant prior history and body of knowledge, and b) the absence of suitable technological and methodological tools to prevent, redress and manage these events. Unfortunately however, due to the current state of art, transportation managers and decision-makers are forced to rely on 'rules of thumb' and 'gut feel' in making these complex decisions that affect several lives and have tremendous socio-economic consequences. To make matters worse, these decisions must be made in a matter of few minutes, with limited information about the initiating events and possible current and future repercussions (a particularly tragic example was seen in the case of WTC attacks, where the fire-chief was forced to order rescue teams to assist in evacuation efforts due to inadequate information on risks and consequences faced by rescue personnel).

Despite these significant and unacceptable levels of risks, security considerations currently do not receive adequate attention in transportation planning, design, and operations literature or practice. Therefore, empirical insights, models, data, and decision support tools to analyze, assess, and reduce vulnerability of transportation networks are urgently needed. Further, given the small time frame for corrective action, and the massive adverse impacts, it is highly desirable to prepare operational and management plans for mitigating the impacts given such unfortunate occurrences.

Given these pressing needs, this white paper calls for the development of systematic measures and methods to i) assess the vulnerability of existing infrastructure, ii) prevent the occurrence of disruptive attacks (where possible), iii) reduce the consequence of attacks if they occur, iv) develop and organize a body of knowledge on security threats, impacts and control decisions, and v) increase the awareness of experts and users of the system alike on security issues, and vi) integrate security considerations as an integral part of the network planning, design, and operational efforts.

In achieving these long-term objectives, the following resources will be critical and necessary. It is essential to obtain data to identify the likelihood and consequence of various disruptive events on the transportation system. Models to assess and compare the influence of various contributive factors on component and system-level vulnerability under various disruptive events are needed. The success and effectiveness of these models, in turn, hinges to a large extent on the accuracy and usefulness of the underlying data. The data and models will provide the basis for informing decision-makers on the network wide vulnerability and security implications of various control strategies. The insights, models and data together, will ultimately lead to decision support tools to prevent, manage, and mitigate the impact of disruptive events.

The absence of a quantitative vulnerability measure at both component and system-wide levels remains a serious, if not the most significant challenge, to developing insights and systematic methods to improve transportation security. **Therefore, the proposed white paper intends to examine the need, scope, potential, and relevance of quantitative framework for the vulnerability assessment of transportation networks.** Further, the development of a systematic quantitative framework to analyze network security and vulnerability may be used to identify security critical system components, prioritize corrective action, evaluate impacts of alternative control strategies, and analyze trade-offs between security enhancement measures and traditional system operation metrics.

The network security and vulnerability problem, however, is unfortunately, a complex, non-linear, dynamic and stochastic problem (see Section 2.2 for a more detailed discussion). For instance, it deals with assessing security of large-scale real-world networks (Ben-Akiva, 1991), over several time-scales of interest (planning, operational, response etc.), interactions among multiple user classes with varied objectives (Mahmassani, 1997), in a highly uncertain environment (due to likelihood of disruptive events) and complex interdependencies among network components (Hu, 1997). Despite these challenges, the following opportunities may prove to be particularly vital in developing systematic solutions to this difficult problem.

The availability of richer information and data from monitoring traffic conditions and networks (ITS data) may enable better monitoring, quicker detection, and faster response than ever before. The advances in modeling methods (features captured, richer resolution, scalability of models, representation of dynamics etc.) are expected to play a key role in solving this complex problem. In this regard, the rapid increase in computational power, recently available, is also pertinent since the problem involves complex non-linear interactions in networks under uncertain and time-varying environments (Birge, 1997).

Since the uncertainty in these systems to a large extent may be attributable to human-agent decisions in these models, recent advances in user decision modeling may also be exploited to further increase model resolution and accuracy (Bhat, 1997; Srinivasan, 2001b). Experience and insights gained in allied fields and disciplines including incident management, reliability of large -scale systems, and risk management in various areas ranging from nuclear plants to aviation systems etc. will also serve as a useful starting points in addressing transportation network security and vulnerability problems. (Kaplan, 1981; Abkowitz, 1988; Saccomano, 1993; Mahadevan, 1997a,b).

The remainder of this white paper is organized as follows. Section 2 identifies critical data needs, empirical insights, and methodological challenges that must be resolved for a systematic analysis of the transportation security problem. Section 3 will discuss the essential elements required for a qualitative framework for vulnerability assessment. This qualitative framework will identify critical factors that affect the vulnerability of transportation system components including links, nodes, and terminals. Deriving from this qualitative framework, the next section, will discuss the potential for developing a quantitative framework. In Section 5, the application of the quantitative framework for system-wide vulnerability assessment and short-term risk reduction using network analysis techniques is discussed. The implications of the quantitative vulnerability framework for transportation practice will be described in the context of opportunities to embed security analysis into transportation design (of redundancies to reduce risk), planning (evaluating alternative countermeasures), and operations practices in Section 6, followed by a few concluding remarks in the final section.

Critical Gaps, Needs And Challenges In Transportation Security Analysis

From among the resources and needs identified in the previous section, this section identifies three critical elements; data needs, methods and models, and empirical insights, where advances are urgently needed. Progress in these areas will form the basis for systematic methods, models and tools to better understand, formulate, and assess and reduce transportation network vulnerabilities under various system disruptions.

Data Needs

As noted earlier, current efforts in transportation to characterize system vulnerability and threats have tended to be qualitative due to the absence of well-defined quantitative indices (for example, threat alerts are characterized as high, very high alert etc.). While these attempts at characterizing vulnerability are particularly useful in communicating the risk of threats to the public, they do not provide the necessary basis for careful comparison of various threats and trade-offs among possible alternative solutions. Such a quantitative scope becomes particularly valuable and inevitable especially given the large-scale and complex impacts of the transportation security and vulnerability problem. For instance, both threats and consequences have a range of important societal impacts on a wide range of dimensions including economy, mobility, safety etc., resulting in the need for comparing and assessing the impacts of various control actions. Given these needs, developing quantitative measures of vulnerability remains a critical, perhaps, the most important pre-requisite in formulating and solving transportation security problems systematically.

Several factors contribute to both the vulnerability and the ability to reduce risks and threats on the transportation network. An important factor, in this regard, is the integrity and resilience of physical infrastructure under disruptions. Therefore, data on physical infrastructure including, the nodes, the links, and various types of facilities are obviously necessary (Ortuzar, 1984). Also needed, are data on the type of construction, retrofitting, ductility, and associated structural strength, stability and robustness under various physical attacks. Another important but related aspect is data needs on the functional resilience against attacks. In this regard, the following data are pertinent: the extent of disruption in demand and supply patterns, the reversibility and elasticity of these changes, duration to recovery and rebound in demands (Abkowitz, 1988). Data are also desirable on incident response resources available to handle a disruptive attack if it occurs (Lepofsky, 1993). For example, information on access, location and capacity of nearest emergency medical resources from every link/component are important in reducing response time given an incident. Such data can prove to be the vital difference in ensuring the survival of victims of a disruptive attack.

While certain types of threats (both natural and man-made) may be localized in scope, and are targeted against specific facilities (e.g., bridge attack), other threats may have a more global impact. For example, disruption of a vehicle carrying hazardous material, biological attacks on planes or subway stations can propagate with flows on the network (Miller, 1998). Therefore, in these cases, it is essential to obtain flow-related data. Even with geographically fixed threats, flow data are needed and play an important role in evaluating the extent of disruption in service provision following a disruptive event and related performance measures. For instance, following the disruption of traffic on a bridge, the prior traffic on the bridge must be re-routed, thus significantly altering the vulnerability and performance of the rest of the network. Flow data are also important, since sabotage attacks may be directed specifically against flows with higher economic values or impact potential.

Data are also needed on types and classes of users on the network. The perception of vulnerability, security needs and concerns, performance measures of interest, organizational framework and control policies are expected to vary substantially across different user classes. For example, a freight company may be more concerned about the security of its hub and spoke network configuration than the failures of individual aircrafts, whereas, a passenger airline company might place a greater emphasis on aircraft and fleet safety. The security of the terminal on the other hand, is of a greater interest and responsibility of related federal agencies under the purview of FAA. Similarly, a local freight routing company, a hazardous material shipper, and a common passenger vehicle will have different security concerns and different decision sets all of which collectively and mutually affect system capacity and vulnerabilities significantly.

Collecting these diverse data and organizing them efficiently through databases will assist decision-making to enhance transportation security at various levels (Pijakawa, 1988). First, from an incident response perspective, these resources will enable significant reductions in response time and clearance times thus increasing the survival chances of victims. Second, these data, even without further analysis may provide

valuable heuristic guidelines for operational planning purposes. For instance, the decision on whether the victims need to be removed to care providers or vice-versa, might depend on access to these resources and the medical state of victims. These data may also be used to select simple but effective operational heuristics to manage traffic following disruptions. (For example, it was observed that following the attack on a greyhound bus in Manchester, TN, separation of truck flows to the freeway and cars on arterials was particularly effective in reducing incident congestion, NCTR, 2001). Third, gathering these data in database and serving these data using visual displays to appropriate decision-makers, may enable effective coordination of decisions across relevant system management agencies (medical, department of transportation, and city and local counties). Finally, and perhaps most importantly, these data will play a paramount role in defining quantitative vulnerability metrics at both component and system levels. The use of appropriate data for this purpose is critical, since errors in vulnerability indices which may result in significant loss of life and property could have been prevented.

Methodological Challenges

The problem of vulnerability assessment and consequent security enhancements raises several methodological questions and challenges that have not been recognized or addressed in transportation systems analysis practice and research. Some of these methodological challenges that need to be addressed include: 1) methods to analyze the likelihood and consequences of shocks imposed and propagated by disruptive incidents, a key deficiency in current equilibrium-based methods 2) performance metrics to be used in risk analysis, management, planning and operations to enhance network-level security, 3) models for analyzing the influence of shocks on travel and mobility demands and 4) methods to account for complex interdependencies over time and space induced by security enhancement measures and interactions between user decisions, and transportation system performance measures (congestion, trip time etc.).

In addressing these challenges, a transportation-system manager who aims to assess current vulnerability and take effective countermeasures to increase system security faces the difficult problem of solving a complex dynamic and stochastic problem in order to maximize security. The complexity of the problem coupled with the real-time constraints of user response, highlight the need for systematic, rigorous, and computationally efficient decision support tools at various levels including: network design, planning, operations and control, and incident response and management.

Possible models and methods addressing the security problem must consider network level impacts since failure to do so can lead to local improvements which may lead to global worsening of system vulnerability. Further, the failure to account for user decisions in response to disruptive events can, in turn, lead to erroneous decisions. In addition, the proposed models should account for the time-varying nature of the problem, since the likelihood of threat is likely to depend on distribution of flows on the network over time. Although several users (multiple user classes) of the transportation system are interested in the security of the system, the interest in specific strategies depends on the nature and type of users. For instance, it is quite likely that a freight delivery company has a different security priorities than a transit agency. Given these differences, it is

unlikely that there is a unique omnibus solution that may work for all underlying security sub-problems of various user classes. Furthermore, it is also essential to consider the interaction among these various user classes, since they affect the likelihood and consequences of disruptive events.

Since network vulnerability depends on complex interactions between users on the transportation network, it is expected that network analysis tools and methods will play an important part in any eventual solution algorithms and methodological advances. In view of the uncertainty and low probabilities of disruptive events, interdisciplinary methods drawn from statistical analysis and reliability principles are expected to be valuable in addressing these methodological challenges (Mahadevan, 2001). Further, due to the absence of experimental control for systematic analysis, and the limited time-frame any possible preventive or corrective action, it is not possible to rely solely on empirical real-world data on past experiences. Consequently, the use of simulation based techniques to identify alternative threat scenarios and their consequences is also envisioned to be an integral part of methodological developments (Law, 1991). Note that due to the broad and systemwide impact of security in terms of costs, safety, and efficiency and diverse objectives among various system users, the solution methods must optimize among competing and often conflicting objectives. Therefore, multiple-objective formulations and optimization techniques are likely to play an important role in the solution methodologies.

Existing Knowledgebase and Empirical Insights Needed

As noted earlier existing knowledgebase is sparse, if not virtually non-existent, in terms of empirical insights for assessing network level vulnerability and mitigating risks, especially under malicious attacks. Therefore, empirical insights are urgently needed to provide at least preliminary guidelines in the near-term, and more definitive answers in the long run, to the following substantive questions pertaining to design, operations and planning.

The first set of substantive issues that arise relate to efforts to prevent the occurrence and adverse impacts of disruptive events through systematic design efforts. Substantive questions in this direction include insights on: 1) What are the security implications of adding a facility or a lane on an existing facility? 2) How much reserve capacity is needed to meet emergency response needs under disruptive attacks? 3) Which network components nodes and links are more vulnerable? 4) Where and in what form should redundancies be provided to reduce local and global system vulnerability? 5) What would be the consequence of adding these redundancies and spare capacities on operational system performance? Answers to these questions will enable the development of engineering design-based solutions to reduce vulnerability and risk, and are important in view of the large infrastructure investments involved. Furthermore, the success and effectiveness of the following operational issues are also likely to be critically dependent on how these design issues are addressed.

The second level of substantive questions pertains to operational aspects. Specifically, these relate to the ability to reduce the consequence of events once they occur. Along this

line of inquiry, the following questions are important from the operations and control standpoint. How can advanced information and traffic monitoring technologies be used to enhance transportation security? Under what condition would providing information to users prove to be counter-productive to system security? What are possible control strategies to enhance security at the operational levels? How can risks be systematically redistributed on the network across various user groups to increase overall system security? To what extent can vulnerability be reduced through physical separation of various flows? Which routing strategies and control policies are effective in managing traffic following such a disruptive event and how can emergency management actions and measures be used to increase the survival likelihood of victims? The answers to these questions could prove to be vital in increasing the safety and security of users given an incident, not to mention the safety and security of emergency service providers (fire-fighters, medical response personnel, police at the incident scene). Further, addressing these issues effectively will ensure quicker recovery of the system following disruptive attacks, thus reducing the extent of mobility and economic losses.

Substantive insights are also urgently needed on policy questions and evaluation aspects pertaining to serious disruptions in the transportation system. In this category, it is essential to assess the likelihood and consequences of various sources of threats, and possible control strategies. More importantly, however, it is essential to track and identify pre-cursor events that provide decision-makers with adequate and timely warnings about the likelihood, nature and consequence of potential threats. This is critical, since it is typically too late to prevent or substantially reduce the consequence of an attack, once it has been initiated. Furthermore, it is also essential to establish mapping between threat sources and effective control actions to maximize system security and mitigate risks. Other substantive questions along this line include the identification of intermodal linkages and their effect on the vulnerability of the system, and equity issues regarding who pays and who benefits from security measures.

QUALITATIVE FRAMEWORK FOR NETWORK-WIDE SECURITY AND VULNERABILITY ASSESSMENT

This section identifies key factors influencing link-level vulnerabilities on a transportation network. Node level vulnerabilities and interdependency induced by network flows across various network components are examined. Further, this section also seeks to characterize alternative control measures to reduce system vulnerability, in terms of practical criteria including cost, timeliness of implementation, and scope and effectiveness.

Identifying Factors Affecting Link-Level Vulnerability

Several types of factors can affect the link level vulnerability in the transportation network. These factors include network attributes, threat attributes, flow attributes, and neighborhood attributes, as discussed below.

Among the network-related link level attributes, data on the scope of network and the types of links are of particular interest. Data on the type of facility on various links are important since they characterize the extent of access and mobility on different facilities.

The physical configuration and geometrics on the links are also pertinent. It is also essential to obtain data quantifying the nature and extent of failure on links under the various types of threats (i.e. whether failure is defined in terms of capacity reduction or complete blockage/disruption). Data on available alternatives to the given link in case of disruptive attack are also necessary. The extent of redundancy in the system and network design configuration (for e.g. role of link as a connector in a hub and spoke system) are also critical data elements. Further, information on the number of paths that share the given link, and the availability of alternative links for certain origin-destination pairs are needed to assess the extent of disruption on the given link. Another important network attribute is the number of intermodal connections supported by the link under consideration.

In addition to the network information above, data are also needed on the nature, likelihood, and magnitude of threats encountered on that link. This will enable identifying the most important threat sources (based on likelihood and consequences) and prioritizing corrective actions accordingly. Specifically, it is important to identify and classify the likelihood across various sources/types of threat including accidents, incidents, physical attacks, biological attacks, chemical attacks, hazardous material spillage or leakage, or natural disasters such as earthquakes etc. The severity and extent of damage faced by users and the system will vary depending on the type of threat. Furthermore, the population that is exposed, and whether the disruption occurs at a fixed location (physical attack) or has a wider network reach (chemical or hazardous materials attack), also depends on source and type of threat. In addition to the nature of threats, the emergency response preparedness to various threat sources can be assessed through data on nearby emergency management assets and facilities including distance, number and capacity of nearby hospitals.

A third set of factors that affects link level vulnerability relates to the nature of flows on the link. Certain links may be more likely to face attacks due to the large magnitude of flows, whereas, others could be targeted due to the economic value of flows therein. Therefore, the magnitude, type, and value of flows are essential factors that affect link vulnerabilities. Other types of threats may be targeted against certain classes of vehicles or users (trucks with hazardous materials etc.) instead. Therefore data on the composition of these flows by various user classes including commercial, passenger, transit, hazardous material etc. is also needed. While these factors may affect the likelihood and possible consequences of disruptive events, other flow-related factors may become important in the context of emergency response (Honea, 2000). For instance, the residual capacity on a network determines whether a given link could serve as a reliable and quick path for emergency evacuation or delivery of other emergency services. Note that, these flow factors and corresponding impacts on link vulnerability can be expected to vary over time (within a given day and from day-to-day).

Compared to the previous factors which relate to threat and transportation attributes, the following set of factors affecting vulnerability are not directly related to the transportation system. These attributes capture the influence of secondary threats that may be directed against facilities adjacent to or in the neighborhood of a given network

link. For example, the type and nature of land-use and population density in the neighborhood (residential, commercial, schools) etc. may be important in identifying the population that may be exposed to various attacks. These factors can also be useful in assessing the cost of additional transportation infrastructure (including land costs) that may be needed to enhance security. Furthermore, the mobility and access needs of the users and their travel patterns on the link may play a vital role in assessing the effectiveness and reliability of the link performance to support emergency response needs under disruptive events.

Factors Influencing Node, Junction, And Intermodal Vulnerabilities

In contrast to the traditional definition of nodes in highway networks (where it refers to intersections), the use of the term node below generalizes this definition to include terminal and intermodal facilities including transit stops, airports, etc. As with the link vulnerabilities, nodes or junctions with higher volumes of users are more likely to be subject to malicious disruptions due to the larger adverse impacts. Therefore, flow related variables including number of users, and class of users, and economic value of flows (cargo) are also pertinent for nodal vulnerabilities. In addition, the number of modes supported and interconnected at nodes is also a key determinant of vulnerabilities at junctions. For instance, the airport terminals serve as the primary transition points between the urban transportation road network, and the air transportation network, highlighting the security importance of this facility. The accessibility of a junction (measurable through the number of incident arcs at that junction) may also increase its vulnerability (due to increased likelihood of being a target), but may also reduce the impact of an attack due to several possible evacuation routes. On the other hand, a node which serves as a junction on the only path connecting two cities may be more vulnerable because of the lack of alternatives, if disrupted. Therefore, the presence of redundancies at a given node also affects its vulnerability. Other factors that could affect node-level vulnerability includes the facility type, the number of transfer facilities, and control policies (signals, transit frequency) at junctions.

Role Of Flow-Level Attributes On System Vulnerability: Effect of Demand/Supply Shocks

Disruptions at either the node-level or the link level can affect transportation system performance in two ways. On the one hand, the reduction or absence of certain link and node capacities can dramatically change both the configuration and routing of flows (supply-side shocks). On the other hand, the disruptions themselves may be of such a magnitude and nature to significantly alter the demand and modes of travel, in many cases inelastically, and possibly irreversibly (leading to demand shocks). Such demand/supply shocks in the system can lead to significant disruption of flows and degradation of system performance in the short-term. These disruptions can lead to significant cost to trip-makers and adverse economic impacts to private transportation service providers (time-sensitive freight, couriers etc.). In addition, there may be longer-term disruptions in system performance, which may have a more substantial, and longer lasting influence than the immediate impact. This cumulative degradation in system performance may be caused by lagged effects, users' adjustments in response to changed network conditions, and network-wide interactions between rerouted flows and original flows. It is essential to understand how these shocks and

resulting uncertainty are propagated in the network, in order to develop effective counter measures. Understanding the influence of demand and supply shocks is also critical for transportation management during emergencies such as routing for evacuation (e.g., floods, earthquakes etc.). In addition to these generating effects, the control policies and actions including routing strategies and information supply to users may also induce perturbations in the network demand and supply conditions. However, models and methods to analyze the system level shock propagation are needed since current equilibrium-based models cannot capture the effect of system shocks.

Characterizing Alternatives To Reduce System And Component Vulnerability

The final component of the qualitative framework aims at characterizing alternatives to reduce system and component level vulnerability under various types of artificial/natural threats. In particular identifying the cost, ease of implementation, extent of risk redistribution associated with each alternative will enable quick screening and selecting appropriate alternatives. Toward this end, threats to the transportation system may be classified as natural or man-made, with physical, chemical, biological attacks included in the latter category. Furthermore, threats may be classified as attacks occurring over fixed or localized regions, in contrast to threats or disruptions which are more global in impacts due to attacks on mobile systems or components (e.g. planes, or trucks carrying hazardous materials etc., or dispersion in chemical attacks). Clearly, different strategies need to be adopted in these two cases, with a greater emphasis on restoration and recovery in the former case. In contrast, in the latter, efforts must be channelized towards limiting the extent of exposure through risk communication, and evacuation.

Like the classification of threats, alternative control actions to mitigate and manage various threats may also be categorized into the following hierarchical levels. In this hierarchy, the strategies and decisions aimed at preventing the attacks and reducing the likelihood of their occurrence through systematic design efforts form the top-layer. Examples of these strategies include the addition of infrastructure facilities (links, junctions) or lanes to reduce vulnerability of a given system configuration. At the next level in this hierarchy are planning decisions that aim to reduce the consequences of possible disruptive events. Examples of these decisions include planning efforts to provide redundancy and residual capacity at a local level, in contrast to the network level considered above. Note that the planning actions also need to precede the occurrence of actual disruptive events in order to pro-actively prevent loss of life and property. The next level of control actions in this hierarchy consists of decisions taken at the operational stage to reduce the consequences of these events once they have been initiated. These could include re-routing and evacuation policies to minimize exposure, decisions to reduce emergency response and incident clearance times, and actions taken to reduce further threats (for instance - closure of airports or terminals, and suspension of transportation services in affected regions, as with the Sept .11th incidents). The final level in this hierarchy consists of actions aimed at educating and increasing the awareness of various user groups about the likelihood and consequences of possible disruptions, in order to reduce exposure and ensure more effective operations. As part of this effort, a critical examination of effective and ineffective strategies after the event may enable identifying best practices that are successful under certain threats.

The cost of alternatives in this hierarchy decreases from the design to the operational stages due to the large costs associated with network design and infrastructure construction activities. Consequently, the likelihood of rapid implementation decreases from the lowest to the highest levels in this hierarchy. In contrast, however, the maximal effectiveness in terms of reducing vulnerability and consequences depends largely on design and planning decisions. In particular, the success of reducing vulnerability depends on the effectiveness of both planning and operations stages in redistributing existing risk and vulnerability across facility types and user types in order to protect key assets, and enhance the safety and security of system users (NCTR, 2001). Such redistribution may be achieved through construction activities such as building additional capacity or facilities, or may be achieved through flow controls or restrictions. For instance, isolating certain more vulnerable users or flows, may reduce the risk faced by other users, whereas, combining vital and relatively unprotected flows with larger and less distinguishable commercial/consumer flows may also reduce risks of attack in some cases. Since the key to successful vulnerability assessment and reduction hinges on the ability to plan, design and operate transportation systems under various disruptive attacks, it is essential to define and apply quantitative metrics of vulnerability at these levels to maximize security and minimize risk.

QUANTITATIVE FRAMEWORK FOR NETWORK VULNERABILITY ANALYSIS

A brief overview of alternative methods to obtain a quantitative vulnerability index at the component level is provided in this section. The proposed methods seek to obtain a single quantitative metric of link and node-level vulnerabilities by combining the numerous factors identified in a previous section. Statistical calibration of the proposed models to determine and prioritize the factors contributing to vulnerabilities at the component level are described. In addition, methods to aggregate component level metrics to form system level metrics are also discussed.

Developing Quantitative Metrics of Component Level Vulnerabilities

In specifying component level vulnerabilities, the goal is to develop a single comprehensive and quantitative vulnerability index that accounts for the various sources of vulnerability, threats, and recovery potential discussed in Section 3.0. The contributive factors included in this metric may include deterministic and random factors, objective and subjective elements, quantitative and some qualitative measures, and some measure of uncertainty and reliability in data, in addition to time-varying factors such as flows. In order to simplify these diverse measures into a common scale, it is desirable to propose methods to formulate a single quantitative metric for each network component. Three alternative methods can be proposed for combining these individual attributes into a vulnerability index at the component level.

In the first method, experts and network managers may be asked to rate the vulnerability of a given or hypothetical facility on a fixed rating scale (say on a scale of 1 to 10) given the actual attribute levels (say, number of connecting paths = 3, flows = 2200/hr/lane etc.). Based on the vulnerability ratings by experts, one may develop a regression-based model identifying the relative importance of the contributive factors in the analysis. For instance, a simple linear regression model of the following form may be used:

$V(i) = \beta_0 + \beta_1 X_1 + \ldots + \beta_n X_n + \varepsilon$, where the relative importance of the various contributive factors ($X_1, \ldots X_n$) may be calibrated based on observed/reported vulnerability ratings for various levels of the contributive factors (vector X).

A second approach also takes the parametric approach to combining the contributive factors into a single vulnerability index for each system component. However, it explicitly recognizes the fact that the ratings of experts are naturally ordered and that different experts may not necessarily use the same scale (in other words a rating of 6 by one person may be equivalent to another person's rating of 8). In this approach, the observed/reported vulnerability rating is treated as an ordinal variable. An underlying continuous variable and a set of ordered thresholds are assumed to explain the ordinal vulnerability rating (Srinivasan, 2001a). It is assumed that a vulnerability rating of 1 will be selected, if this continuous underlying variable (U) falls below the first threshold δ_1, and a rating of 2 will be selected if it falls between the first and second thresholds (δ_1, δ_2) and so on. The thresholds and the continuous variable U are expected to vary systematically across different respondents as a function of the contributive factors. More specifically, the thresholds U are expressed as a function of the contributive factors as follows:
$U = \beta_0 + \beta_1 X_1 + \ldots + \beta_n X_n + \varepsilon$, and the thresholds are expected to vary randomly across observations as well. The relative importance weights of the various contributive factors are then derived by maximizing goodness of fit of the predicted model with actual ratings. The underlying function U, provides a continuous vulnerability index. Using this index, qualitative vulnerability levels (mild, low, etc…) scales may be obtained by comparing the continuous index U against suitable thresholds δ.

In contrast to these parametric approaches that require pre-determined calibration weights, the third approach enables a more flexible and non-parametric form for importance weights of contributive factors. For instance, in this scheme, the decision-maker may choose to employ one set of weights for analyzing the effect of spare capacity and flows for one application (say operations) and may use a different set of weights for another application (say planning or design). Further, the decision-maker may change these weights based on experience or specific problem needs. Although, this method is the less sophisticated than the previous two approaches, it also provides the greatest flexibility in deriving insights about system vulnerability under various projected scenarios, and applicability to decision problems faced by various user classes.

Calibration Of Vulnerability Index at the Component Level

The calibration stage involves the estimation of importance weights in the component level vulnerability index models above, and consists of two components. First, the relative weights of various contributive factors must be determined to develop a single quantitative vulnerability metric from the plethora of underlying factors. Once these weights are determined, then the vulnerability index for all components (nodes and links) must be determined by applying these weights to the levels of contributive factors (link flows etc.) to compute the vulnerability index for each component. Possible calibration methods for the first stage are discussed below.

The vulnerability rating data from experts can be used to develop and calibrate the vulnerability index models using a statistical framework (regression-based or discrete ordered response models) for the parametric equations noted above. For the more flexible non-parametric case, the choice weights obtained by the decision-makers may be directly used, without the need for calibration. The vulnerability index for each link can be represented by a function that includes network attributes (e.g. configuration, number of lanes) and flow attributes (e.g., volumes, economic value) etc as shown in equations in the previous section. The coefficients of each independent variable in the mathematical specification can be estimated using the Maximum Likelihood (MLE) technique for the parametric equations above. In MLE procedure, the parameters are estimated by maximizing the likelihood of observing the choices made by the decision makers in the sample. The magnitude, direction, and statistical significance of the estimated parameters along with the final form of the best fitting model with substantive theoretical interpretation, serve as the natural link between statistical model and research hypothesis (Srinivasan, 2001c). Key variables that affect experts' vulnerability ratings can be identified by their statistical significance in the model by performing t tests for individual significance and χ^2 tests for joint significance for groups of variables. Different functional specifications can be compared using goodness of fit measures. Chi-squared (χ^2) tests can also be used to test for significance of interaction effects, non-linear specifications, and market segmentation validation (testing significant differences between market segments).

Note that the calibration may be based upon data from only a few selected links on the network. To obtain vulnerability indices on other links, the models developed may be used in a forecasting/estimation mode. In this mode, the explanatory variables obtained for each link are used together with the parameter estimates obtained from the previous calibration stage to develop estimates of vulnerability indices for each component (not in the calibration data set). Due to variations in availability and accuracy of data on network components, techniques to statistically impute and correct inaccurate data will be needed. Once calibrated, validation is necessary to checking model error assumptions, assess predictive ability with a different data set, and to refine parameters based on real-world data.

Integration of Component-Level Vulnerabilities to Estimate Network-Wide Vulnerability Index

While the component level vulnerabilities provide some data on the risks and possible consequences under disruptive events, they only provide partial information at the network level. For instance, due to the complex network interactions, enhancing the security of a local component may lead to an increase in global vulnerability due to a drastic deterioration elsewhere. Furthermore, due to the time-varying and uncertain nature of flows on the network, the consequences and the likelihood of attacks can vary and propagate over time and space on the network. The need for network level metrics, in contrast to component level metrics is also motivated by the possibility of obtaining a more even and equitable redistribution of risks across users and facilities on the network. In view of these needs, three alternative methods are discussed below to aggregate the

quantitative component level vulnerability metrics to network-level vulnerability measures.

A naïve but computationally and intuitively appealing approach is to estimate network level vulnerabilities by aggregating component level metrics over nodes and links. While this cumulative index may give an aggregate measure of network security, it cannot be used to distinguish between alternative system configurations with the same aggregate index. Furthermore, it also provides no indication of redundancies available, and may not adequately capture dependence on flows. However, in view of its simplicity, it can provide a quick basis for judging local improvements that may be adequate for certain sketch-planning applications.

An alternative approach which remedies to a certain extent the shortcomings of the naïve aggregation method is to use flow-weighted average of component vulnerabilities. Thus, this method aims to account for the differences in flows across various network components as well as the time-varying nature of flows on a given link. In this method, vulnerability is treated as a cost experienced by each flow unit (vehicle, person etc.) on the component and is aggregated based on flows. Clearly, the methodological improvement comes at the expense of increased computational and data costs. For instance, the need to consider time-varying flows increases the problem complexity from a static network problem to a problem requiring analysis over several time-intervals. This approach may be extended and refined to account for changes in vulnerabilities due to flow variations over days (due to special events, or other seasonal effects).

The vulnerability model accuracy may also be enhanced by explicitly considering differences across multiple user classes on the network. One categorization of such user classes is based on origin-destination desires (OD) on the network. This characterization may be useful since certain O-D flows may encounter greater risk and likelihood of disruption due to their strategic location (downtown) and proximity to other physical targets. Network level aggregation to account for these user classes (distinguished by O-D pair) could be based on defining a vulnerability index corresponding to each O-D pair or corresponding paths. The advantages of this aggregation scheme relative to the flow-based scheme earlier, includes i) the ability to distinguish more vital and critical O-D pairs from others and, ii) the capability to account for the effect of vulnerability on demand (note that this differs from the earlier assumption that demand affects vulnerability but not vice-versa). Further increases in model resolution and sophistication may also be obtained by accounting for differences across users of various physical classes based on vehicle size (buses, cars, etc.), drivers (with and without information), behavioral propensities (divert routes, switch departure times, neither, both etc.), occupancy levels (HOV vehicles) etc.

Note that the schemes discussed above are generally static and do not vary over time, and may be suitable and sufficient for planning or design purposes. However, for operational and control purposes, estimates of how the vulnerabilities change over time are important. For instance, these are essential for determining which routes should be used for evacuating given an attack. In these cases, the aggregation procedure must account for

the fact that component (link and node level) vulnerabilities can change with flows and time, in a manner that is affected by security control measures as well as consequent user decisions. These network level interactions may be captured by further disaggregating component level and multiple user class level vulnerability indices over time (using suitable time subscripts). This increase in model sensitivity will enable answering a wide range of empirical questions posed earlier, but comes at the cost of significant increase in computational resource requirements. Essentially, the problem size now expands manifold due to large number of time-intervals, multiple user classes, and several possible threat scenarios, necessitating recourse to computationally expensive Monte-Carlo simulation techniques.

Identification Of Security Critical Network Components

The application of quantitative component and system-level metrics to address important practical and substantive research issues is discussed in this section. Specifically, this section will explore the use of network analyses techniques including shortest path and minimum cost formulations in conjunction with these metrics to identify security critical components in the network. Identifying these components is critical for prioritizing resource allocation decisions to reduce risk and increase security.

The vulnerability index calibrated (as proposed in Section 4.3) using the quantitative metrics above can be treated as a vulnerability-related cost on each arc in the network. An important generalization of link level vulnerabilities is the notion of a path level vulnerability index. This may be defined for a given path by aggregating the link and node level vulnerabilities on components that constitute that path. In identifying security critical components it is essential to identify the most vulnerable paths (MVP) on the network. Corrective control and planning action in the near-term can be directed at enhancing the security on the most vulnerable paths. At the same time, it is also essential to identify least vulnerable paths on the network (LVP). This is essential for guaranteeing the security and safety of mission-critical flows (for e.g., to ensure the delivery of emergency medical services, or increasing quickness of incident clearance).

In determining the most and least vulnerable paths, the proposed approach relies on standard network analysis algorithms (Tarjan, 1983). In this approach, the vulnerability costs are associated with each link. The most vulnerable paths may be determined by solving a network problem by finding the set of paths with maximum path vulnerability using a variant of minimum cost flow problem (Ford, 1958). On the other hand the least vulnerable path can be determined as the solution from a shortest path problem, where costs are again defined using vulnerability metrics (Dijkstra, 1959). Note that these analyses techniques are based on static network flow assumptions and do not take into account the time-dependent or uncertain nature of flows. Nevertheless these methods provide an indication (based on average flow states) of paths that require immediate attention and those that are less vulnerable, from a design or preventive standpoint. However, from an operational standpoint, the time-varying nature of flows must be considered.

By combining network analysis methods with quantitative metrics above, it is thus possible to identify strategic locations, provide enhanced security, and estimate system vulnerability as a function of component vulnerability. Through the identification of most and least vulnerable paths, it is possible to prioritize and implement system reliability enhancement measures. The methods proposed to identify MVP and LVP are expected to be computationally inexpensive, since the underlying network algorithms are known to be computationally efficient (polynomial time algorithms, Glover, 1985; Ahuja, 1993).

INTEGRATING QUANTITATIVE NETWORK SECURITY ASSESSMENTS INTO TRANSPORTATION PRACTICE

The implications of the quantitative vulnerability framework for transportation practice are described in this section. Specifically, this section explores possible opportunities to integrate security analysis into transportation design (of redundancies to reduce risk), planning (evaluating alternative countermeasures), and operations practices, especially in the context of low vulnerability benchmarks, and the use of advanced ITS technologies.

Design Applications:

From among the most vulnerable paths determined using techniques in Sections 4 and 5, it is possible to identify those arcs which when disabled will lead to the greatest increase in system vulnerability. These arcs can be referred to as most vital arcs (MVA), since their removal will result in the maximum increase in system vulnerability. From a design perspective, physical redundancy can be provided for the Most Vital Arcs to reduce overall system vulnerability. In a similar fashion, most vital nodes of the network may also be identified. Following their identification, design efforts can be focused towards reducing the likelihood and consequence of attacks at these security critical junctions, particularly in intermodal networks (Orlin, 1987).

Extensions to Planning and Evaluation:

Models that use the quantitative metrics of vulnerability may also be used to aid in planning and evaluation of risk reduction and security enhancement measures. One such example is the opportunity to identify additional residual capacity on existing facilities. Unlike most vital arcs, where additional supply/infrastructure may be needed for offering redundancy, certain arcs may only require expansion of capacity to provide for effective emergency operations. These arcs may be identified from the most vulnerable paths which have insufficient residual capacities. Potential candidates also include arcs on secondary most vulnerable paths (paths which can become the most vulnerable paths following the disruption of flow on a current vulnerable path). Planning methods may also be used to reduce nodal vulnerabilities. For instance, when certain nodes are vulnerable and are overexposed, the potential for redistributing risk through systematic design strategies (such as design of alternative or buffer links) or operational strategies (such as flow separation) can be evaluated.

Improving Operations:

Given that the system security is partially flow-dependent, the vulnerability of the network may be improved through systematic operational measures determined using the quantitative metrics. For instance, it is possible to identify flow characteristics and

configurations with more desirable security and vulnerability metrics, as noted below. It may be desirable to compare and modify current flow patterns towards these desirable/ideal benchmark configurations through suitable operational measures.

The operational extensions may be achieved by explicitly recognizing the flow-dependent nature of component vulnerability index, in contrast to the average or expected value treatment of flows in the design applications. One desirable flow configuration (from a network security perspective) may be obtained by finding that flow assignment which minimizes system-wide vulnerabilities. The rationale is to assign flows such that flows on used paths have minimal and equal marginal vulnerabilities, and other paths are more vulnerable (Sheffi, 1985). This provides a benchmark to compare the vulnerability of existing flows in relation to this minimum vulnerability benchmark. The deviations between currently prevailing flows and the ideal benchmark can provide a quantitative basis to identify opportunities for reducing system vulnerability through design and operational policies. This assignment procedure to minimize vulnerability can also be extended to identify maximal number of paths with minimal vulnerabilities.

Another opportunity for operational security improvements arises from the potential for using ITS technologies to quickly and preemptively detect pre-cursor events, through the collection of real-time facility and performance monitoring data. In the short-term, these data can assist in preventing certain types of disruptive events, and reducing the size of exposed population, and minimize clearance time following disruptions in other cases. In the longer term, linking these data and pre-cursor events with the vulnerability metrics will enable more accurate security assessments and, in turn, more effective control actions.

SUMMARY

In summary, current research and practice on network-wide security analysis and vulnerability reduction in transportation systems remains sparse and inadequate to support systematic security assessment and risk mitigation efforts. In particular, data, methods and insights are urgently needed to support systematic, rigorous, and comprehensive analysis and assessment of component and system-level vulnerabilities. A key weakness, in this context, is the absence of well defined supporting quantitative vulnerability metrics. To develop such a quantitative metric, data are needed on link and node-level vulnerabilities, and interactions among network components. Models are needed for determining quantitative indices of vulnerability at component, path, and network levels. These models must account for numerous factors that contribute to system vulnerabilities, ranging from network-related, flow-related, location and access-related factors. To be useful from an operational standpoint, it is absolutely essential to consider the mutual interactions between disruptive event consequences, control actions, and user decisions on the network.

Once quantitative metrics are established, they may be used to address specific decision problems that require immediate attention. For instance, these metrics may be used to determine vulnerability level of a given network configuration. A further analysis of sub-components (paths, nodes, and links) will provide valuable information on prioritizing

the selection of components for immediate security enhancements. Embedding flow considerations into vulnerability indices will enable the analysis of how these security enhancements will affect the vulnerability of transportation networks. Furthermore, the use of vulnerability metrics together with traditional performance metrics such as travel time and congestion may be jointly used to determine faster yet safer ways (routes/evacuation) to respond to disruptive attacks/events on the system.
Given the unacceptably high risk and serious and pervasive damage caused by the disruptive events, progress on modeling and empirical insights needs to proceed along three parallel directions. First, empirical data on factors that contribute to vulnerabilities (including emergency management assets) need to be collected on various system components and made available to appropriate decision-makers through organized databases linked to easily understandable graphical user interfaces. Second, due to the low probability of actual disruptive events, there needs to be a coordinated effort at mapping the linkage between pre-cursor events and actual disruptive events in order to detect them early and prevent them where possible. Finally, due to the inherent uncertainty in the nature of these events and their outcomes, sole reliance on past experience can be misleading. Therefore, it is necessary to develop and apply calibrated, quantitative and rigorous models to analyze and mitigate the consequences of disruptive events.

In summary, the transportation network security and vulnerability assessment problem is a complex and non-linear problem. In view of the unacceptably high risk of disruptive events, and the massive and pervasive consequences that follow, there is an urgent national need for sustained, scientific, and concerted action to:

i) protect the physical well-being and safety of users,
ii) reduce the vulnerability of critical transportation infrastructure and services, and,
iii) minimize the economic impacts of such disruptions.

The absence of a quantitative vulnerability measure at both component and system-wide levels remains a serious, if not the most significant challenge, to developing insights and systematic methods to improve transportation security. Therefore, quantitative metrics of component and system level vulnerabilities need to be developed to effectively meet the challenges posed by significant escalation in the potential, and intensity of physical and functional disruptions to critical transportation infrastructure and services. These metrics may be used in concert with network analysis and simulation models to address critical substantive questions on current network vulnerability states and to identifying control actions for security enhancements. Given the unacceptably high risk and massive adverse impacts of transportation system disruptions, integrating security considerations as essential elements of transportation design, planning and operations practice must receive the highest priority for current and continuing research in this area.

REFERENCES:

1. Abkowitz, M. and P. Cheng (1988). "Developing a Risk/Cost Framework for Routing Truck Movements of Hazardous Materials," *Accident Analysis & Prevention,* 20, pp. 39-51.
2. Ahuja, R., Magnanti, T., and Orlin, J. B. 1993. Network flows: theory, algorithms, and applications. Prentice Hall, New Jersey.
3. Ben-Akiva, M., De Palma, A., and Kaysi, I. (1991). Dynamic network models and driver information systems. *Transportation Research A*, Vol. 25(5), 251-266.
4. Bhat, C. R. (1997). Recent methodological advances relevant to activity and travel behavior analysis. Resource paper presented at the 7th International Association of Travel Behavior Research Conference, Austin, Texas.
5. Birge, J. R., and F. Louveaux. 1997. *Introduction to stochastic programming*, Springer-Verlag, Berlin.
6. Dijkstra, E. 1959. A note on two problems in connexioin with graphs. *Numerische Mathematics,* 1, 269-271.
7. Ford, L. R., and Fulkerson, D. A. 1958. Constructing maximum dynamic flows from static flows. *Operations Research* 6, 419-433.
8. Glover, F., Klingman, D., and Phillips, N. 1985. A new polynomially bounded shortest path algorithm. *Operations Research* 33, 65-73.
9. Honea, B. 2000. U. S. Military preparedness: Jammed in traffic. *T.R. News*, 211. December.
10. Hu, T.Y., and Mahmassani H.S. (1997). Day-to-day evolution of network flows under real-time information and reactive signal control. *Transportation Research C*, 5(1), 51-69.
11. Kaplan, S. and B. J. Garrick (1981). "On the Quantitative Definition of Risk," Risk Analysis, Vol. 1, No. 1, pp. 11- 27.
12. Law A.M., and Kelton, W. D. 1991. *Simulation modeling and analysis*. McGrawhill Publishers. New York.
13. Lepofsky, M., M. Abkowitz, P. Cheng (1993). "Transportation Hazard Analysis in Integrated GIS Environment," *Journal of Transportation Engineering* 119 pp. 239-254
14. Mahadevan, S. 1997. Physics-Based Reliability Models, Reliability Based Mechanical Design, (Ed. Cruse,T. A.), Marcel Dekker, 197-232.
15. Mahadevan, S. 1997. System Reliability Analysis, Reliability Based Mechanical Design, (Ed. Cruse, T.A.), Marcel Dekker, 233-264.
16. Mahadevan, S., R. Zhang, and N. Smith. 2001. Bayesian Networks for System Reliability Reassessment, *Structural Safety*, 23 (3), 231-251.
17. Mahmassani, H. S. (1997). Dynamics of Commuter Behavior: Recent research and continuing challenges. In Eds. Lee-Gosselin, M. and Stopher, P., *Understanding travel behavior in an era of change*, Pergamon Press, 279-314.
18. Mahmassani, H., and R. Jayakrishnan. 1991. System performance and user response under real-time information in a congested traffic corridor. *Transportation Research A*, 25(5), 293-307.
19. Miller-Hooks, E., and H. S. Mahmassani. 1998. Optimal Routing of Hazardous Substances in Time-Varying, Stochastic Transportation Networks. Technical

report prepared for Amarillo natural resource center for Plutonium. ANRCP-1998-8. July.

20. NCTR. 2001. Florida public transportation anti-terrorism resource guide. Prepared by national center for transit research, Center for urban transportation Research.University of South Florida. 2001. Oct. 5, 2001 (I-24 manchester).
21. Orlin, D. 1987. Optimal weapons allocations against layered defenses. Naval Research Logistics Quarterly. Vol. 34, 605-617.
22. Ortuzar, J. D., and Willumsen, L. G. (1995). Modeling Transport. Second Edition, John Wiley and Sons, New York.
23. Pijakawa, K., S. Foote and A. Soesilo (1985). "Risk Assessment of Transporting Hazardous Material: Route Analysis and Hazard Management," *Transportation Research Record* 1020, pp. 1-6.
24. Saccomanno, F., M. Van Aerde, and D. Queen (1988). "Interactive Selection of Minimum-Risk Routes for Dangerous Goods Shipments," *Transportation Research Record* 1148, pp. 9-17.
25. Saccomanno, F. and J. Shortreed (1993). "HAZMAT Transport Risks: Societal and Individual Perspectives," *Journal of Transportation Engineering* 119, 177-188.
26. Sheffi, Y. (1985). *Urban transportation networks: equilibrium analysis with mathematical programming methods*. Prentice-Hall, Englewood Cliffs, NJ, USA.
27. Srinivasan, K. K. (2001a). An ordered mixed logit model formulation for the analysis of accident injury severity. *Transportation Research Record, (In Press).*
28. Srinivasan, K. K. 2000. Dynamic decision and adjustment processes in commuter behavior under real-time information, Ph. D. dissertation, Univesity of Texas, Austin.
29. Srinivasan, K. K., and Guo, Z. 2001b. Day-to-day dynamics and disequilibrium induced by departure time dynamics, Working Paper, Vanderbilt Center for Transportation Research, Vanderbilt University.
30. Srinivasan, K. K., and Mahmassani, H. S. (2001c). Dynamics in departure time choices of commuters: a comparison of alternative behavioral mechanisms. Paper presented at the 80th Annual Transportation Research Board meeting and submitted for publication in *Transportation Research C*.
31. Tarjan, R. E. 1983. Data Structures and Network Algorithms. SIAM. Philadelphia, PA.
32. ASCE. 2001. Report Card for America's Infrastructure. Technical Report. http://www.asce.org/reportcard.
33. Giuliano, G. 1998. Impacts of Northridge Earthquake on Transit and Highway Use. *Journal of Transportation Statistics,* Vol. 1, No. 2.
34. Boarnet, M. G. 1998. Business losses, transportation damage and the Northridge earthquake. Journal of transportation Statistics, Vol. 1, No. 2.

THE ROLE OF SECURITY IN THE SURFACE TRANSPORTATION PROGRAMMING PROCESS

Frederick J. Wegmann, Ph.D.
Jerry Everett
University of Tennessee

INTRODUCTION

The most recent federal transportation authorization bill, the Transportation Equity Act for the 21st Century (TEA-21), became law in June 1998. This new statute enhanced the importance of safety and security issues in the statewide and metropolitan surface transportation planning process. The existing structure and process of metropolitan planning were retained, but the previous 16 planning factors were reduced to seven. Likewise the twenty-three statewide factors were reduced to the same seven factors as specified for metropolitan planning. One of the seven factors that Metropolitan Planning Organizations (MPOs) and Departments of Transportation (DOTs) are now required to address deals exclusively with safety and security.

Prior to September 11th most concerns were focused on how best to include safety considerations in the transportation planning process. For example, many MPOs and DOTs have fairly advanced methodologies for selecting projects to be included in the Transportation Improvement Program (TIP) or Statewide Transportation Program (STIP). Scoring techniques are frequently used by MPOs in prioritizing projects for inclusion in TIP. From a sample of 13 MPOs, it was not uncommon for safety concerns to represent 10 to 20 percent of the point allocation for highway projects, but little recognition was given to security issues. Safety was defined as, "actions required to reduce roadway crashes." Also, it was found that safety and security were frequently ignored in the prioritization of transit, intermodal, or enhancement projects. Those agencies that select all projects from one funding pot and do not stratify their programming evaluation into predefined modal or funding categories were more likely to explicitly include safety or security considerations when selecting non roadway projects. One interesting issue is how security measures can be defined and quantified for project selection. (1)

Security concerns are frequently included along with safety as a surface transportation-planning goal. For example, the Denver Regional Council of Governments (DRCOG) has included safety and security as one of seven factors to be considered in the TIP process. The DRCOG factor stated (2):

> "Increase the safety and security of the transportation system for motorized and non-motorized users."

While safety is included as part of DRCOG's evaluation criteria in the selection of highway, bicycle/pedestrian and transit plans, security is only considered in the transit development program. As demonstrated by DRCOG prior to 9/11, security in transportation planning was typically associated with violence or the fear of violence that may influence a persons decision to use public transportation, improving the transit work force's ability to function or provide the

ability to facilitate emergency evacuation, and emergency services response after a natural disaster (3). Specific examples of security factors are presented in the next section.

Examples of Pre-9/11 Security Programming Concerns

The authors conducted an analysis of the TIP process for 13 MPOs to determine how security issues were considered in programming decisions. Programming exists at the state and local levels in the form of STIPs and TIPs. These programs represent investment decisions made for a period of approximately two to three years, and are established to help move the organization in the direction of the goals and policies developed in their respective long range transportation plans. Projects are selected to address a series of considerations, typically including congestion mitigation, cost-effectiveness of the project, system continuity, air quality implications, opportunities to exploit intermodal opportunities along with safety and security.

Specifically, historical crash records are utilized to define safety concerns for highway projects however, it is more difficult to quantity security scores. For non-highway projects, incident data are collected by transit agencies such as in Portland's Tri-Met which identify incidents on the system (vehicles) or off-the system (at transit stops). These incident databases are not generally available or developed to the same sophistication level as highway crash record databases that are used to define the safety element for a highway project.

Transit, enhancement and intermodal projects tend to score security concerns using a subjective evaluation based on the potential merits of a proposed project as conducted in Dane County, Wisconsin and Little Rock, Arkansas. The Metropolitan Transportation Commission in the San Francisco Bay Area has defined roadway and transit safety/security scores as a multiplier of the severity of the safety/security problems and an impact value (the degree to which the proposed project would solve the problem). Project elements are stratified into high impact, medium impact, and low impact. Severity is defined based on crashes per million vehicle-miles for highway project and number of incidents reported in the Section 15 database for transit projects. Unfortunately, all too frequently security issues are simply ignored in the evaluation of roadway and nonroadway projects. Although it can be argued that security concerns are operational considerations for non-highway projects and may be addressed by actions such as dispatching additional police or adding lights, full integration of security concerns into the planning process requires that these elements be considered in each project being advanced.

The Central Arkansas Regional Transportation Study (CARTs) in Little Rock Arkansas expanded highway safety and security considerations not only to reflect crashes but also hazards. Projects are evaluated with a subjective score based on the project ability to eliminate hazards or mitigate dangers caused by floods, rock sides and other hazards. The Houston-Galveston Area council in its programming decisions considers if roadway project serves as a potential hurricane evacuation route. Roadway expansion projects received credit if projects are consistent with hurricane evacuation routes identified in the Hurricane Contingency Planning Guide produced by the Texas Department of Public Safety. New construction projects that serve as alternative routes to designated evacuation routes will also receive credit in the project selection process (4)

The Oregon DOT (ODOT) as part of the statewide transportation plan has defined a policy concerned with establishing "lifeline routes" as follows (5):

"Earthquakes, flooding, landslides, wild fires, and other natural and man-made disasters may destroy or block key access routes to emergency facilities and create episodic demand for highway routes into and out of a stricken area. ODOT's investment strategy should recognize the critical role that some highway facilities, particularly bridges, play in emergency response and evacuation. In some cases, the most cost-effective solution to maintaining security in these lifeline routes involves investment in roads or bridges owned by local jurisdictions. To the extent feasible, investments should be made without regard to roadway jurisdiction in order to provide the greatest degree of lifeline security for the available resources. ODOT will work with local governments to further define and map a network of lifeline routes. The lifeline network will focus on serving those communities which are particularly susceptible to isolation by virtue of their limited highway access."

The policy and associated actions are stated as follows (5):

Action 1
Define the criteria for lifeline routes to respond to short and long-term needs and, working with local jurisdictions, agencies, and emergency service providers, designate the lifeline network for the State of Oregon.

Action 2
Provide funds or establish state/local partnerships to make improvements to state and local roads and bridges on the lifeline network where supportive of the Lifeline Routes Policy and cost-effective relative to alternative strategies.

Action 3
Consider the presence of designated lifeline routes in system investment and management decisions and in coordination efforts with local land use and transportation planning activities.

Action 4
In planning for lifeline routes, focus on susceptibility of the route and improvements on it (bridges and other structures) to disasters such as earthquakes, landslides and flooding. In corridor plans and transportation system plans, emphasize improvements and other measures, which maintain a highway connection between regions or areas of the state in the event of major disasters. Consider a combination of measures to address identified hazards and elements such as appropriate advance maintenance, structural reinforcement, flood-proofing, emergency response planning and development of emergency alternative routes."

Outside of these limited examples, it may be summarized that prior to 9/11 MPOs and DOTs viewed security issues as operational concerns, not planning concerns. The principal responsibility for security concerned rested with law enforcement agencies. Transportation concerns were focused on hazard mitigation or emergency response plans. As summarized by Pedersen "security issues were not an issue in most state and MPO surface transportation

planning processes and TIPs did not contain allocations for security related issues"(6). A critical question is how has the events of 9/11 changed the consideration of security in the surface transportation planning process?

CURRENT ACTIVITIES

A search of more than 30 MPO websites was conducted in an attempt to discern the extent to which MPOs have begun to formally include security in a more direct way in their Transportation Improvement Program's. Based on the available documentation little change appears to have occurred in how security is considered in the transportation programming process since 9/11 at most MPOs. This is likely based on two primary factors– the first is the timing of the search. Most MPOs develop new TIPs only every two to three years. At this point in time only about 7 months have past since the terrorist attacks. Most MPOs have simply not updated their TIPs or changed the project evaluation criteria during that period. The second factor is that many MPOs simply have not yet decided how to redefine "security", much less formally incorporate it into the programming process.

Two examples of the types of security related projects that will likely become more common in future programming were identified. The Baltimore Metropolitan Council TIP has linked some ITS programs and projects to security issues. They note that emergency management services save lives and improves security through immediate notification of the precise locations of crashes and breakdowns. (7) The Metropolitan Planning Organization for the Miami Urbanized Area's TIP for 2001-2002 to 2005-2006 includes a section on Seaport Security. The following is an excerpt from that section:

> "In compliance with the state-mandated security requirements, Port security enhancements are budgeted in FY 2002 and 2003. These enhancements include: port-wide closed-circuit television, alarm systems, cargo area fencing, and access control systems. Furthermore, construction of additional INS and Customs office space in cruise terminals, a federal agency requirement, is included in the Security Enhancements." (8)

Transportation security has also become a major issue being discussed by policy makers and in the ongoing work activities of some MPOs. The November 2001 issue of the Puget Sound Regional Council's newsletter highlights the conclusions of the Northwest Freight Conference held October 7-9, 2001 at SeaTac airport. It was noted that in the wake of September 11th it is essential that security be improved at border crossings throughout the transportation system. Washington Governor Gary Locke urged, "a complete rethinking of how we approach transportation security, with freight security as an equal component. It was noted that this increased emphasis on security would likely make it even more difficult to move freight through major American cities. These concerns have not necessarily been translated into projects that can be programmed in a TIP at this point, but will clearly impact future transportation planning and programming. (9)

Though a consideration of security in transportation as redefined after 9/11 has not yet become part of the TIP for the New York Metropolitan Council (NYMTC) it is a strong component of next year's Unified Planning Work Program (UPWP). The issue is addressed in the document's Overview section as follows:

> "In light of the terrorist attack of September 11, 2001, which struck at the heart of the region and produced impacts which resonate throughout NYMTC's area and beyond, the importance of an integrated regional program of planning activities has increased. New themes have emerged in the aftermath of September 11th, which will alter the approach to the planning program. The 2002-04 Work Program reflects these emerging themes and changing priorities."

The following excerpt from the UPWP highlights how security issues will be addressed in their upcoming transportation planning efforts:

Emerging Themes

Although not formally part of the current Regional Transportation Plan, several broad themes emerging in the aftermath of the terrorist attack of September 11, 2001 are important considerations in the development of this Work Program as categories of short- and long-term planning activities. The major themes include the following:

Assessment of Impacts - the September 11th attack had far reaching impacts on the regional economy and transportation system. A good deal of attention is given to collecting data which will assess the impacts of the disaster on the operation of the regional transportation system, on economic conditions, and on the socio-economic forecasts which provide a foundation for NYMTC's planning process.

Transportation System Security - security considerations are an obvious emerging theme in the aftermath of September 11th Increased general security measures have had an impact on the transportation system through the need to accommodate security checkpoints throughout the region and through an increased emphasis on emergency contingency planning. Specific security measures focused on major components of the transportation system are also a consideration.

Transportation System Redundancy and Emergency Response Planning – the redundancy of major components of the transportation system is another major theme emerging in the aftermath of September 11th. The terrorist attacks closed or restricted use of several major components of the transportation system, underscoring the need for increased attention to and investment in system redundancy and the related area of improved emergency response planning.

Assessment of Risk - the September 11th attack has also drawn attention to the vulnerability of transportation system components to various forms of attack and the need to plan for responding to, mitigating or otherwise preventing such possibilities. Each of these themes is reflected in specific activities in the 2002-04 Work Program. Examples of this work include:

- NYMTC staff has been working with the U.S. Coast Guard and with relevant NYMTC members to coordinate an approach to a regional

Infrastructure Threat Assessment, which has been proposed by the Coast Guard.

- NYMTC's members are assessing travel modes and systems for their potential to improve system redundancy. Examples include efforts by the New York City DOT to perform various assessments of maritime and bus transit modes, and New York State DOT's assessment of the arterial roadway network.

- As an organization, NYMTC is assisting the Federal Emergency Management Agency (FEMA) in its efforts to respond to the September 11th attack. This work will continue and will include the collection of various data on changes to employment and travel patterns in the region, as well as a coordinated database of information on emergency response activities and projects.

- NYMTC staff will revise regional socio-economic forecasts, as well as the baseline assumptions of NYMTC's Best Practice Model. Once the assumptions and forecasts have been revised, the model will need to be recalibrated.

- Various aspects of emergency planning, emergency evacuation, system security and system redundancy will be considered and discussed, primarily by NYMTC's advisory working groups. (10)

Security issues have also received a great deal of attention from the policy makers at the Metropolitan Washington Council of Governments (WashCOG) since September 11th Initial evaluations revealed that each component of the Washington D.C. area's transportation system performed very well individually, but did not perform as well from a coordinated regional perspective. The Transportation Planning Board was charged to develop a coordinated emergency transportation response plan. This plan was not intended to be an evacuation plan, but a plan to address community transportation needs. The Council's board of Directors created a Task Force on Homeland Security and Emergency Response for the National Capitol Area in October of 2001. The mission of the task force as described its background information document dated December 13, 2001 is as follows: "To enhance regional preparedness and insure a coordinated regional response to future public safety challenges." According to the COG's web page the Task Force includes elected officials from the region, members of the Board of Trade, and Federal officials. Its structure includes five subgroups that relate to transportation, public safety, health, energy and water, and solid waste.

Each subgroup has developed a Regional Emergency Support Function (RESF) framework for the Regional Emergency Coordination Plan. The draft transportation RESF has the following purpose and scope:

"Purpose – Transportation, facilitates communication and coordination among regional jurisdictions and agencies concerning regional transportation issues and activities in anticipation of and following a regional emergency.

Scope – This RESF is intended to focus on disruptions of the regional transportation system requiring inter-jurisdictional coordination and information sharing. Transportation disruptions can occur as a result of direct impacts upon the transportation infrastructure (e.g. disasters) or from surges in requirements placed upon the transportation system by emergencies in other functional areas." (11)

Note that the Council sought $7 million dollars in designated Federal funding to develop and begin implementing this regional response plan.

POTENTIAL ROLE OF SECURITY IN THE POST 9/11 ENVIRONMENT

The events of 9/11 have broadened the concept of security focusing attention on terrorist activities in addition to natural disasters and transit security. The National Research Council has prepared a list of terrorism incidents that have implications on the functioning of the transportation system (Table 1). (12)

TABLE -1 Scenarios Considered in the DOT Vulnerability Assessment	
Physical Attacks	
	• car bomb at bridge approach
	• series of small explosives on highway bridge
	• single small explosive on highway bridge
	• single small explosive in highway tunnel
	• car bomb in highway tunnel
	• series of car bombs on adjacent bridges or tunnels
	• bomb(s) detonated at pipeline compressor stations
	• bomb detonated at pipeline storage facility
	• bomb detonated on pipeline segment
	• simultaneous attacks on ports
	• terrorist bombing of waterfront pavilion
	• container vessel fire at marine terminal
	• ramming of railroad bridge by maritime vessel
	• attack on passenger vessel in port
	• shooting in rail station
	• vehicle bomb adjacent to rail station
	• bombing of airport transit station
	• bombing of underwater transit tunnel
	• bus bombing
	• deliberate blocking of highway-rail grade crossing
	• terrorist bombing of rail tunnel
	• bomb detonated on train in rail station

	• vandalism of track structure and signal system
	• terrorist bombing of rail bridge
	• explosives attack on multiple rail bridges
	• explosive in cargo of passenger aircraft
Biological Attacks	
	• biological release in highway tunnel
	• anthrax release from freight ship
	• anthrax release in transit station
	• anthrax release on passenger train
Chemical Attacks	
	• sarin release in multiple subway stations
	• physical attack on railcar carrying a toxic chemical
Cyber and C3 Attacks	
	• cyber attack on highway traffic control system
	• cyber attack on pipeline automated control system
	• attack on port power and telecommunications facility
	• sabotage of train control system
	• tampering with rail signals
	• cyber attack on train control center

This vulnerability assessment helps fix the framework in which transportation institutions will need to respond. Meyer has identified three key actions MPOs can undertake in response to potential security issues (13):

> "Prevention: This has several components, ranging from the actual stopping of an attack before it occurs, to providing improved facility designs that prevent large scale destruction. Surveillance, monitoring, and sensing technologies will likely play an important role in the prevention phase of an incident.

Response/ Mitigation Reducing the harmful impact of an attack as it occurs and in the: immediate aftermath. This entails identifying the most effective routing for emergency vehicles and the evacuation of large numbers of people, as well as providing effective communication systems among emergency response teams and for general public information.

Monitoring: Recognizing that an incident is underway, characterizing it, and monitoring developments. Clearly, surveillance, monitoring, and sensing technologies would be critical to this phase of incident response, as would public information."

In response, the potential MPO and DOT roles can build on their traditional strength of technical analysis and traditional transportation planning involving project funding. Meyer has proposed the MPOs role could include the following specific activities: (12)

- "Conducting vulnerability analyses on regional transportation facilities and services.

- Analyzing transportation network for redundancies in moving large numbers of people (e.g., modeling person and vehicle flows with major links removed or reversed, accommodating street closures, adaptive signal control strategies, impact of traveler information systems), and strategies for dealing with "choke" points such as tollbooths.

- Analyzing transportation network for emergency route planning/strategic gaps in the network"

From these analytical studies it will be possible to quantify the extent to which projects address security concerns so MPOs and DOT's can make appropriate decisions on resource allocations in the TIP and STIP process. Data will be required which objectively describes vulnerability and how projects help mitigate the vulnerabilities. Security concerns should be explicitly expanded in the TIP or STIP evaluation process to consider terrorism activities. Points can be allocated for projects that:

1. Provide redundancies in the network for person and goods movement, especially at "choke points" such as bridge crossing, tunnels, major interchanges etc.

2. Add capacity or reduce congestion along designated evacuation routes.

3. Support the movement of emergency services and increase accessibility to military bases, hospitals etc.

4. Provide countermeasures to protect critical assets such as intermodal facilities, bridges, tunnels and other facilities having high vulnerability.

5. Support the movement of goods within and through designated areas with multimodal redundancy.

6. Expand ITS applications for security related issues, such as surveillance, information dissemination and development of evacuation plans.

7. Size the public transportation fleet to accommodate emergency evacuation and contingency movement during potential fuel shortages.

8. Identify projects such as traffic control centers that enhance monitoring of the transportation system and enhance communication between transportation and emergency service providers.

It is clear the events of 9/11 have changed the nation and will have profound impacts on surface transportation planning. Security issues, previously ignored, will move to the forefront and both TIPs and STIPs will contain allocations for security concerns. Security is no longer an operational consideration, but needs to be incorporated into the long-range surface transportation planning process. MPOs and DOTs must play a critical role in conducting vulnerability analyses, establish a mechanism encouraging communications between related parties, support the development of emergency response plans and use ITS for surveillance and control. It will be the prerogative of each MPO and DOT to define the specific security evaluation criteria and assign the appropriate weights to security issues. Each organization will need to define security concerns relative to other project selection criteria. However, in the short-term security issues will have to represent "add-on" concerns to projects already being advanced. Probably the security evaluation analysis will need to be qualitative and represent assigning bonus points. As technical analyses are structured, security can be incorporated into the TIP and STIP process as quantitative factors focusing on vulnerability, severity of impact and probability of occurrence of an event. For quantitative analyses to proceed, having security concerns reflected in the project screening and prioritization process requires that security concerns first must be included in the long range transportation planning process. In order to define trade-off among projects, security concerns needs to be defined as goals with associated objectives. Security issues can be expected to have direct impacts on capital programming and will force trade-offs with other priorities. Only through quantitative analyses framed by the appropriate goals and objectives can these trade-offs be defined.

REFERENCES

1. Chatterjee, A, et al. "Incorporating Safety and Security Issues in Urban Transportation Planning." Transportation Board Record 1777, TRB, National Research Council, Washington, DC, 2001, pp. 75-83.

2. "Intern Policy on Transportation Improvement Program Preparation." Denver Regional Council of Government, Denver, CO, May 1999.

3. Improving Transit Security – A Synthesis of Transit Practice." Transit Cooperate Research Program Synthesis 21 TRB, National Research Council, Washington, DC, 2001.

4. "2022 Metropolitan Transportation Plan." Houston-Galveston Transportation Management Area, Houston, TX, February 2000.

5. "1998 Oregon Highway Plan." Oregon Department of Transportation, Planning Section, Statewide Mobility Unit, Salem, OR, 1998.

6. Pedersen, Neil, "Considering Security Issues in Transportation Planning." Presented at TRB Annual Meeting, January 14, 2002.

7. "2002-2006 Baltimore Metropolitan Council TIP." Baltimore Metropolitan Council, Baltimore, Maryland, 2001.

8. "Dade County Transportation Improvement Program Fiscal Years 2001-2002 to 2005-2006." Miami Urbanized Area Metropolitan Planning Organization, Miami, FL, 2001.

9. "Regional View Newsletter." Puget Sound Regional Council, Seattle, Washington, November 2001.

10. "2002-2004 Unified Planning Work Program, Draft Program Digest." New York Metropolitan Transportation Council, New York, New York, March 2002.

11. "Washington Metropolitan Area Homeland Security and Emergency Preparedness Website." Metropolitan Washington Area Council of Governments, Washington, D.C., April 2002.

12. "Improving Surface Transportation Security, A Research and Development Strategy." National Academy, Washington, DC, 1999.

13. Meyer, Michael, "The Role of Metropolitan Planning Organizations in Preparing for Security Incidents and Transportation Response." Georgia Institute of Technology, Atlanta, GA, 2002

TRANSPORTATION RISK MANAGEMENT: A NEW PARADIGM

Mark Abkowitz, Ph.D
Vanderbilt University

INTRODUCTION

Over the past decade, risk management has been evolving into a core business practice in government and industry. In the transportation sector, the overarching risk management objective has been to reduce accident likelihood and severity. When hazardous materials shipments are involved, this mission extends to spill prevention and mitigating the consequences when a release occurs.

Until recently, the approach to transportation risk management assumed that when man-made disasters occurred, they were accidental in nature and not due to malicious intent. Terrorist activities, culminating with the tragic events of September 11, 2001, have dramatically changed this landscape. In particular, we have learned that assessment of transportation risk must be performed with a more expanded scope to accommodate terrorism scenarios that heretofore would have been considered so unlikely that they did not warrant risk management attention. Similarly, emergency response must be able to handle impacts far beyond what was previously imaginable in terms of number of victims, deployment of response resources and agency coordination.

Given these circumstances, it is apparent that decision-makers need to employ a new paradigm for transportation risk management. In particular, this paradigm must: 1) more explicitly consider security threat and vulnerability, and 2) integrate security considerations into the overall framework for addressing natural and man-made disasters, be they accidental or planned.

It is important to recognize that transportation security and traditional risk management share a common objective:
To reduce the likelihood and consequences of disasters so as to protect human health, quality of life and the environment.
As a result, an opportunity exists for security considerations to be folded into an overall decision-making framework that guides how risks are assessed and where resources are allocated so as to generate the best "return on investment". The process can then be governed by addressing a fundamental set of risk management questions (see Figure 1).

The purpose of this white paper is to: 1) review traditional transportation risk management methods and practices, 2) introduce security issues into this framework and 3) recommend actions that enable security considerations to become an integral part of transportation risk management. This "big picture" conceptual view could serve as a catalyst in the development of an agenda that will enable transportation risk managers to devote resources where the overall impact is most beneficial, be it through enhanced security or other risk management control strategies.

The Risk Management Spectrum

Traditionally, risk management has focused on two primary causes of concern, natural and man-made disasters. Natural disasters include a wide range of events, such as floods, earthquakes, tornados, hurricanes, and avalanches. The prevailing attitude is that these events are "acts of God" and there are limited things one can do to prevent incident occurrence. Consequently, the majority of risk management attention in these circumstances has been focused on mitigating the consequences of these incidents when they do occur.

Man-made disasters pose a different problem, both in terms of risk tolerance and the focus of risk management attention. Whether due to human error, poor design or faulty technology, man-made disasters are associated with the failure on the part of an individual or organization to make the appropriate decisions that adequately protect human health and the environment. Hence, society's risk tolerance for man-made events is much lower than for natural disasters and there is greater public scrutiny applied to how these risks are managed. Moreover, if the event is man-made, risk management attention and resources are devoted to both incident prevention and mitigating the consequences of the incident, should it occur.

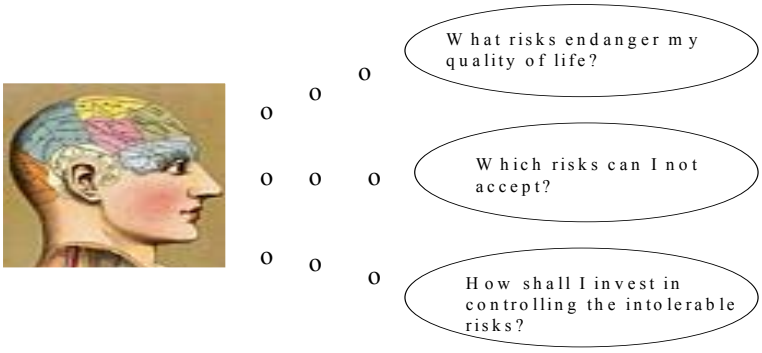


Figure 1. Fundamental Risk Management Questions

Whereas, traditionally man-made disasters have been considered largely accidental in nature, the events of September 11, 2001 underscore the significance of intentional acts of terrorism as both a leading cause of incidents as well as creating the potential for more significant consequences. As shown in Figure 2, the new transportation risk management paradigm needs to explicitly accommodate this additional source of causation and wider range of potential consequence.

In addition, this paradigm should recognize that acts of terrorism can target new pathways. Historically, attention has been focused on chemical/nuclear incidents, leading to fire/explosion and/or toxic release. New scenarios will now require formal recognition, such as bio-terrorism

and cyber-terrorism, as well as physical attack where large groups are congregating (e.g., congested traffic areas, parade routes). Moreover, many believe that the use of biological agents and computer viruses threatens a larger population in ways that our science and technology cannot fully comprehend, raising the level of public anxiety that much more.

Risk Assessment

Risk assessment focuses on the ability to measure the likelihood of a potential event and its associated consequences. The introduction of man-made disasters caused by malicious intent into the risk management spectrum suggests a need to re-visit traditional approaches to determining likelihood and consequence. In the discussion below, consequence measurement is addressed first.

When an incident takes place, the consequences can range from no impact to what is typically referred to as a "worst-case scenario". A worst-case scenario, although considered an extremely unlikely event, characterizes what is believed to be the most catastrophic result imaginable given the incident circumstances. Traditionally, most worst-case scenarios have involved predictions of multiple fatalities and injuries, but rarely, if ever, have they considered consequences of the scale witnessed at the World Trade Center, simply because it was beyond what risk managers considered plausible. Under the new paradigm, a broader set of consequences with more far-reaching effects must be actively considered. This, in effect, extends the consequence scenario spectrum, as shown in Figure 3.

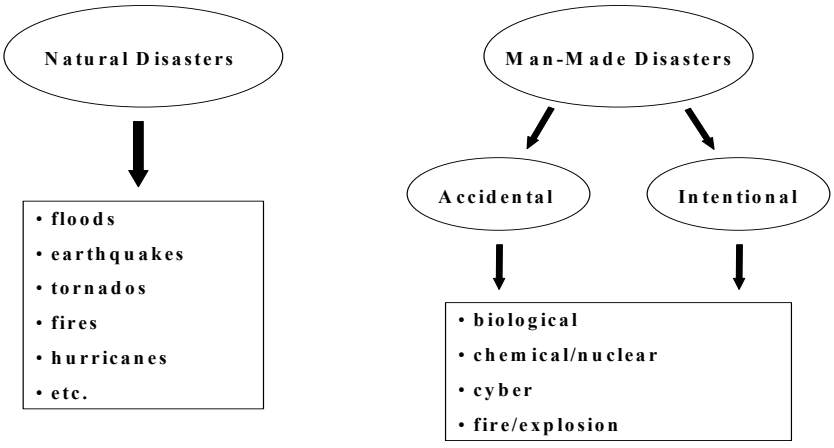


FIGURE 2. THE RISK MANAGEMENT SPECTRUM

To more effectively measure overall impact, a new approach to evaluating consequences is also recommended, one that takes into consideration a more comprehensive account of contingent and societal effects. Among the recommended measures are:

- Fatalities & injuries (acute and long-term)
- Cleanup & disposal costs
- Property & product damage
- Loss due to business interruption
- Environmental degradation & ecosystem damage
- Traffic & community disruption
- Public anxiety
- Diminished agency/company value and image

The obvious benefit of a more accurate measure of consequence is the ability of transportation risk managers to make more informed decisions.

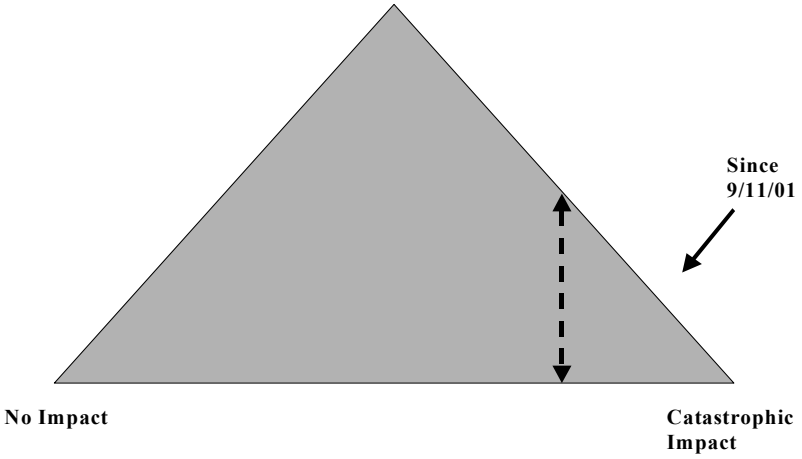


FIGURE 3. RE-VISITING THE CONSEQUENCE SCENARIO SPECTRUM

Paradigm changes are also needed in determining incident likelihood. The altering effects of September 11, 2001 on event likelihood are shown in Figure 4. With a new catalyst for incident occurrence and the potential for far greater consequences than previously imagined, one can expect that incident likelihood will increase somewhat across the entire range of potential consequences, with the consequence range having been extended to include more catastrophic scenarios.

Putting these risk assessment concepts into practice poses a challenge because there is a limited history of terrorist acts from which to estimate event probabilities and predict consequences. Overcoming this impediment will therefore require extensive use of what can be inferred from empirical data combined with the development of predictive models based on the theory of scenario structuring and logical inference (Garrick, 2001).

Prioritizing Transportation Risk

Despite public outcry for a completely safe world, resource constraints (people, time, money) will always exist that preclude such a lofty goal from being fully achievable. Hence, the risk management process must be oriented towards the prioritization of risks, prompting those of greatest concern to become the focus of improved control.

Risk prioritization and follow-through is a process-oriented activity, involving the following steps: 1) identify critical transportation facilities, 2) perform risk assessments, 3) develop risk management control strategies (prevention & deterrence; preparedness; response; recovery), 4) implement control strategies and 5) monitor performance (Chin et. al., 2002).

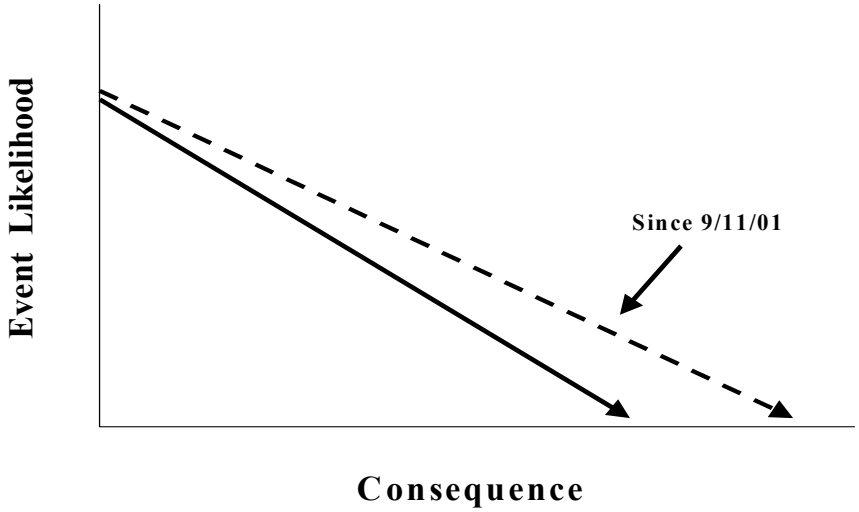


Figure 4. Re-Visiting Event Likelihood

While perhaps simple in concept, successful implementation of this process within the transportation sector is an ambitious task. Our nation's transportation infrastructure is large and diverse, representing a variety of potential terrorist targets. This infrastructure, supporting both passenger and freight transportation, contains:

- Highways (including bridges & tunnels)
- Pipelines
- Railroads
- Navigable waterways
- Air transport networks
- Fixed facilities (traffic management centers, terminals, transfer and storage sites, rest areas)
- "Vehicles" that use these facilities

Whether conducted on a local, state or national scale, it will be important for the risk prioritization process to be inclusive by involving all transportation risk managers in the region of interest. This will help ensure that all potential transportation vulnerability points have been identified and evaluated at the front end of the process, allowing risk management priorities and control strategies to be determined with the confidence of knowing that a systematic process in making these decisions.

INSTITUTIONAL COORDINATION AND DECISION-SUPPORT

Risk management embodies risk communication (sharing information) in addition to risk assessment (generating information). Within the transportation industry, there are a variety of influential parties who, in effect, operate as risk managers (see Figure 5). In the public sector, this can include a multitude of federal, state and local agencies (AASHTO, 2002):

Federal Government

- Department of Transportation
- Environmental Protection Agency
- Federal Emergency Management Agency
- Department of Defense
- Department of Energy
- Department of Justice

STATE AGENCIES

- Emergency Management
- Transportation
- Environmental Management
- Law Enforcement
- Public Safety
- Health Departments

LOCAL GOVERNMENT

- Emergency Operations Centers
- Local Emergency Planning Commissions
- Port, Bridge and Tunnel Authorities
- Fire Departments
- Local Police
- Water Departments
- City Planners

Because there are multiple stakeholders involved, it has always been important to understand the circumstances under which different parties have jurisdiction, the need for mutual agreements and the upward compatibility (i.e., local to state to federal) of disaster preparedness.

The introduction of security risk exacerbates this situation, however. First, the need for timely and accurate, yet secure, information is even more compelling. Secondly, a greater number of

risk managers are likely to be involved, resulting in an increase in the number and type of communication interfaces that must be established and maintained. Finally, the scale of the potential consequences requires these parties to prepare for managing and deploying greater response resources to more victims over a larger geographical area.

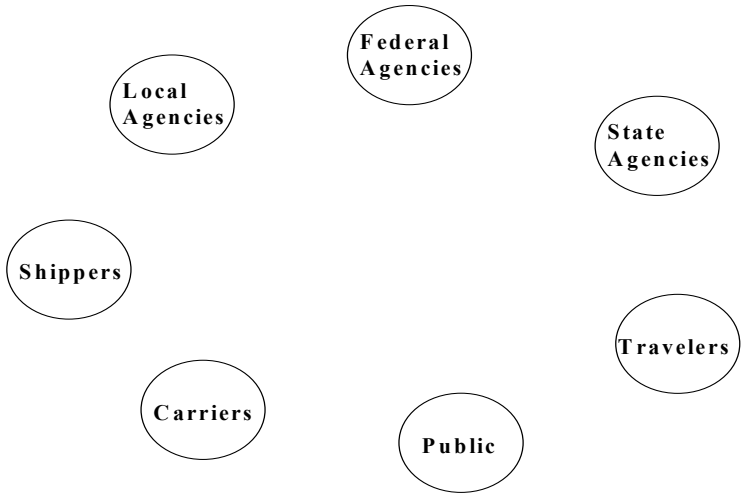


Figure 5. The Population of Transportation Risk Managers

Enabling Tools

To meet these expectations, transportation risk managers will be asked to handle a variety of responsibilities, such as being able to:

- Plan & track before/during/after a major event
- Assess & prioritize locations in need of risk management attention
- Identify at-risk populations & sensitive environments
- Communicate risks to affected parties
- Locate & deploy response resources
- Estimate damage
- Identify & evaluate mitigation strategies
- Maintain a centralized risk management information system

The availability and use of a variety of enabling tools will be critical in supporting these needs. Several of these are discussed below.

Knowledge and Awareness Building. An important part of the transition into a new paradigm is to be able to share the vision and concept with transportation risk managers in a nurturing environment. This provides the opportunity to introduce new ideas as well as to invite feedback. Through channels such as conferences, workshops, training courses, guidebooks and web sites,

knowledge and awareness building can be provided in a manner consistent with a transportation risk manager's ability to absorb information and adapt to change.

Process Development. A systematic approach to identifying critical transportation facilities, performing risk assessments, implementing risk management control strategies and monitoring performance requires the development of policies and procedures to guide the process. Activity flow diagrams should be created that identify all possible transportation infrastructure that could be subject to natural and man-made (accidental and intentional) risks. Credible methods and practices should be established for assessing and prioritizing these risks as well as evaluating and selecting management control strategies. Finally, meaningful measures of risk performance should be defined along with appropriate data collection mechanisms. Within each of these process steps, key stakeholders should be identified and tasks assigned, so that accountability can be established and managed.

Intelligence Gathering. The effectiveness of the transportation risk management process will be strongly influenced by the quality of the information used in its execution. Determining threat and vulnerability requires access to information that enables the transportation risk manager to define the range of consequence scenarios and assign corresponding likelihood. Although some of this information may be available either in the public domain or reside within the organization, liaison with the intelligence community will likely improve data quality in terms of information breadth, depth and quality.

Emergency Response Planning. With an expanded set of consequences to consider and the potential for more severe impact, the preparedness community should re-consider its approach to emergency response planning. At the outset, it may be desirable for the region of interest to identify: 1) all the transportation risk managers that might be involved in an emergency response, 2) the coordination & communication links that presently exist between respective organizations, 3) how well these links are performing and 4) other communication & coordination links that need to be established. Based on these findings, a regional response plan can emerge in which any anticipated transportation risk with significant potential for harm will have been pre-screened, with the deployment and management of the response activity carefully laid out. With this structure in place, preparedness exercises (e.g., simulated emergencies) can be devised that may offer greater benefit to the region because the focus can be placed on the most appropriate concerns and involve the appropriate risk managers**.**

Information Management. At the crux of any transportation risk management activity is the need to obtain, store, analyze and share information. Because transportation involves both static (e.g., location of fixed facility) and dynamic (e.g., location of rolling stock) operations, a variety of technologies offer the potential to support transportation risk management information needs. These include:

- Surveillance and detection technologies (e.g., remote sensing, electronic tags)
- Geographic information systems (GIS)
- Global positioning systems (GPS)
- Communications devices and networks

For example, we are beginning to see the proliferation of software applications that utilize GIS to provide visual maps of risk scenarios that show the location of exposed population as well as proximity to emergency response resources. These images and underlying data can be updated by GPS field devices and accessed via the Internet to communicate information to both internal and external audiences. The key, as we move forward in this arena is to harness only those aspects of available technology that result in practical, easy-to-use tools that enable transportation risk managers to perform their duties with a high degree of confidence.

A WORD OF CAUTION

Considerable attention and resources are currently being allocated to security initiatives in response to the events of September 11, 2001. While it became painfully evident that enhancing security is an immediate risk management priority, it is nonetheless important to understand the long-term ramifications of devoting a disproportionate amount of resources to enhanced security, particularly if the resources are drawn from a general pool of funds allocated for risk management activities. The ultimate concern is that while there is likely to be a high return on investment by flowing resources into controlling security risk in the short-term, eventually a point of diminishing return will be reached, where the next increment of security risk investment will not produce an attractive risk benefit.

A disproportionate allocation of funds directed at security risk also implies a shift of resources away from managing accidental man-made and natural disaster risks. Deferring investment in new and ongoing control strategies in these areas for an extended period time could leave society overall more vulnerable to the risk.

Figure 6 illustrates this tradeoff by showing the potential impact of investing in managing security risk versus other risk management strategies. Investment in security initiatives may be strongly advisable now because of the risk benefits that can be achieved (point A). As diminishing returns are realized over time, reaching a point where new investment in managing these other risks will produce greater societal benefit than continued investment in security risk (point B), the value in shifting resources to other risk management initiatives will become apparent. Ultimately, a balance of investment in security risk and other transportation risks (point C) will represent the most effective use of transportation risk management resources. Knowing when point B has been reached and being agile in adjusting risk management resource investment to reach point C would be exceedingly difficult if security risks were to be managed as a separate "silo" from traditional risk management activities. If security and traditional risk management activities were evaluated, controlled and monitored as part of a single, integrated function, then undesirable risk management results could be avoided.

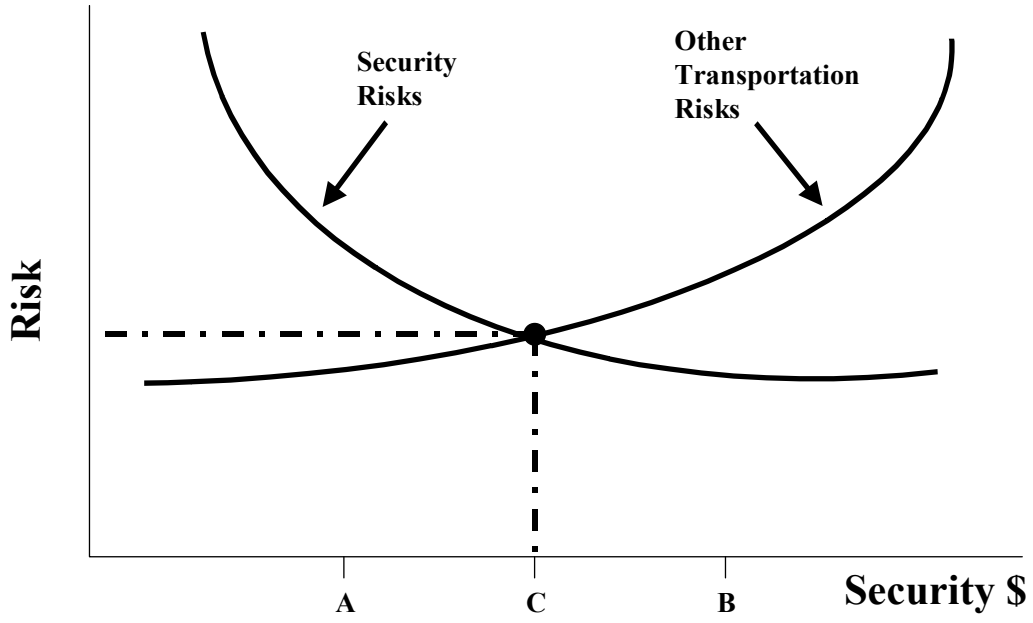


Figure 6. Effect of Shifting Resources From Traditional Risk Management to Security Initiatives

This argument also applies to issues related to risk communication; an example is how to manage the delicate balancing act between the public's right-to-know and making potential targets less transparent to terrorists. A case in point is EPA's Clean Air Act, Risk Management Plan (RMP) rule. This rule requires thousands of industrial facilities, mostly chemical plants, to prepare and submit documentation describing the worst-case scenario incident that could occur at the facility. Were this information to be made publicly available, as initially planned, a terrorist contemplating an act of malicious intent could easily assemble a prioritized list of potential targets (Willis Environmental, 2001). While a decision not to make RMP submittals accessible to the public could be an effective short-term deterrence strategy, continued restrictions on the availability of this information could eventually create greater societal risk, because the communities in proximity to these facilities would lack valuable information from which to improve emergency preparedness in the event of an industrial accident.

SUMMARY

The visibility of terrorist activities has prompted us to re-think how to effectively manage the risks associated with our nation's transportation infrastructure. This paper makes the case that a new transportation risk management paradigm is needed to accommodate considerations associated with assessing and communicating the risks of man-made disasters caused by intentional acts.

Because of the added complexities associated with managing security risks, institutional coordination and decision-support becomes even more critical. As transportation risk managers will be expected to handle a variety of responsibilities, the availability and use of enabling tools will be essential. These tools include knowledge and awareness building, process development, intelligence gathering, emergency response planning and information management. Information technology will play an important role in this regard, provided that technology is utilized to develop practical, easy-to-use tools that enable transportation risk managers to perform their duties with a high degree of confidence.

The significance of integrating security risk with other transportation risks should not be underestimated. As opposed to these risks being managed in separate silos, if they are evaluated, controlled and monitored as a single, integrated function, better overall risk management strategies will emerge and the likelihood of producing undesirable risk management results can be avoided.

REFERENCES

1. AASHTO, "Security and Emergency Response Survey of State Transportation Agencies", presented at the Annual Meeting of the Transportation Research Board, Washington, January 2002.

2. Chin, S. M., H. L. Hwang, O. Franzese and L. D. Han, "Security Vulnerability Assessment Resources for U.S. Highway Network", presented at the Annual Meeting of the Transportation Research Board, Washington, January 2002.

3. Flynn, S. E., "Transportation Security Agenda for the 21st Century", TR News, No. 211, November/December 2000, pp. 3-7.

4. Garrick, B. J. "The Conceptual and Philosophical Basis of Quantitative Risk Assessment", presented at the Frank L. Parker Distinguished Lecture Series, Vanderbilt University, Nashville, November 2001.

5. Morgan, D. F. and H. N. Abramson, "Improving Surface Transportation Security Through Research and Development", TR News, No. 211, November/December 2000, pp. 28-30.

6. Willis Environmental, "Evaluation and Prioritization of the Environmental Risks of Terrorist Action", November 2001.

NATIONAL EMPHASIS ON SECURITY: IMPLICATIONS FOR STATE AND LOCAL TRANSPORTATION POLICY

Malcolm E. Baird, Ph.D
Vanderbilt University

INTRODUCTION

Since September 11, 2001, federal, state and local governments and most other institutions in the U.S. have focused their attention on "security"—looking for ways to make our nation and communities safer from terrorism and other threats to public safety, health and welfare. In time, some of that focus will shift to other issues, but security concerns will almost certainly influence public policy for many years to come.

This paper examines the implications of this emphasis on security for state and local transportation policy, using Thomas Dye's very broad definition of public policy:

> Public policy is whatever governments choose to do—or not to do. (1)

The paper is concerned with the implications of the national emphasis on security relative to what state and local governments have done or may choose to do, or not do, in the transportation arena.

The attacks on September 11th were directed against the United States—the entire nation, not just New York City, New York State, the District of Columbia, or the State of Virginia. The terrorists aimed at buildings with national significance and killed people simply because they were Americans or worked in America. Likewise, anthrax spores were sent through the U.S. Postal Service to the offices of national leaders, without regard to state or city boundaries. Appropriately, the federal government has mobilized in response to these horrific acts and other serious threats to our national security.

The federal government has the duty to "provide for the common defense," and the federal government has acted accordingly. Relative to transportation, the U.S. Department of Transportation has taken aggressive action on several fronts, through the Office of the Secretary, the Federal Aviation Administration, the U.S. Coast Guard, the newly created Transportation Security Administration (TSA), and other modal administrations. Congress has passed legislation to enhance security in aviation and other components of the overall transportation system. The President and Congress have identified transportation as part of the nation's "critical infrastructure" that must be protected.

However, state and local government also have significant responsibilities relative to security and transportation. Table 1 is a reminder of the extent of state and local governments in the United States. As shown in the table, the federal government is but one of almost 40,000 "general purpose" governments (including states, counties, municipalities, towns and township),

most with security and transportation responsibilities. Also, of the "special districts" identified by the Bureau of the Census, almost 1,200 had transportation as their primary purpose, 721 districts whose primary purpose was "highways" and another 476 whose purpose was "air transportation." (2)

TABLE 1. GOVERNMENTS IN THE UNITED STATES (2)

National government	1
State governments	50
Counties	3,043
Municipalities	19,372
Towns and townships	16,629
School districts	13,726
Special purpose districts	34,683
Total	**87,504**

An important premise of this paper is that, while transportation security is certainly a national issue, state and local governments are more than spectators. State and local governments have considerable influence over the development of national policies and initiatives. Also, state and local governments are often the implementing agencies for federal programs, such as the federal-aid highway program, and state and local governments have considerable discretion in administrating those programs. Finally, state and local governments have the power and, arguably, the resources to act independently and help ensure the security of their transportation systems and their citizens.

One final introductory note is that the circumstances driving and surrounding federal, state, and local governments relative to transportation security are still very dynamic. Many of the events that will determine the ultimate changes in state and local transportation policy may not have even occurred. The despicable acts on September 11th will influence policy, probably for generations, but our national leaders and security officials tell us that additional acts of terrorism are likely. State and local policies will change over time and will be heavily influenced by whatever subsequent attacks may occur, the consequences in terms of human injury and death, economic costs, and assessments of what we might have done to prevent or mitigate the incident.

Also, more time will have to pass before we will know the levels of risk that are socially, economically, and politically acceptable. Those decisions will also depend on the events yet to occur, on whatever successes we have in preventing further acts, and the characteristics of the strategies or programs that are material in those successes. The levels of acceptable risks may also be influenced by other demands on state and local budgets and other threats to public health, safety, or welfare.

Nonetheless, the emphasis on security does have immediate implications for state and local transportation policy—for what state and local governments are doing, or may or may not do, relative to transportation. The remainder of this paper examines some of those implications, beginning with an overview of the "national transportation system," the framework within which

state and local governments make transportation policy decisions. To some extent this paper examines what state and local governments have already done, and the paper ends with some suggestions for further consideration. However, most of the paper is devoted to examining the context for state and local transportation policy and trying to identify key questions and issues relative to the new emphasis on security.

Components of National Transportation Infrastructure

Just what do we mean by our "national transportation system" or our "national transportation infrastructure"? The "system" is really a set of separate but interrelated components owned, operated, and paid for by a jumble of governments, special purpose authorities, private companies, shippers, and passengers. At the highest policy levels, state and local governments are concerned with the entire system, the security of the entire system, and how transportation security affects the health, safety and welfare of the citizens. However, state and local governments, and various transportation "authorities" created or enabled by state and local governments, play different roles in different components of the system.

To help describe this context for transportation policy, Table 2 lists the major components of the national transportation system and identifies for each component: (1) the typical "owner," (2) primary sources(s) of capital funds, (3) primary source(s) of operating funds, (4) provider of day-to-day security and (5) first responders during crisis.

The listed "owners" in Table 2 reflect the arrangements that are most common throughout the nation, but exceptions can be found in virtually every state. Some transportation authorities own roads, bridges and tunnels as well as transit systems or ports. Some state agencies own air carrier airports, public transit systems, and railroads. The federal government owns roads within national parks and other federal lands. Regardless of the exceptions, the "owners" information highlights two important facts.

First, the federal government owns only a few components of our national transportation infrastructure, specifically the air navigation and traffic control system, the navigable waterway system, most locks and dams, and Amtrak. For all of the components, except Amtrak, the federal government provides only part of the infrastructure, and private sector providers deliver the services. Amtrak is unique in that the federal agency actually delivers the service, using infrastructure provided in part by the private sector.

Second, Table 2 highlights the important role of the private sector. The private sector is typically the owner of one-third of the components shown in the table. Further, for many of the publicly owned components, the private sector is an essential partner, such as with highways, bridges and tunnels as well as Amtrak and the air carrier and general aviation airports. The private sector operates the trucks and the airplanes and provides the track for Amtrak. Further, some communities contract with private companies to help operate public transit systems and traffic management centers and to maintain roadways.

Component of the Transportation Infrastructure	Typical Owner	Primary Source of Capital Funds	Primary Source of Operating Funds	Provider of Day-to-Day Security	First Responders During Crisis
Deep-draft seaports, Great Lakes, inland, and intracostal ports	Authority	Revenue bonds, federal, state, and local governments	Authority**	Authority police, contract security, USCG	Local/state police, local fire services, EMS, USCG
Marine terminals, equipment, and port intermodal facilities	Private	Private	Private	Private	Local/state police, local fire services, EMS, USCG
Marine vessels, containers, barges, and equipment	Private	Private	Private	Private	Local/state police, local fire services, EMS, other local
Inland and intracostal waterways	Federal government	Federal Authority**	Federal	USCG, state and local police	Local/state police, local fire services, EMS, USCG
Waterway locks and dams	Federal government	Federal government	Federal	Corps of Engineers or other federal	Local/state police, local fire services, EMS, other local
Air carrier airports	Authority	Federal, state and local governments	Authority**	Authority police	ARFF, authority/ local/state police, fire services, EMS
Airline passenger terminals	Authority	Revenue bonds, federal, state, and local governments	Authority**	Authority police	ARFF, authority/ local/state police, fire services, EMS
General aviation airports	Local government or authority	Federal, state, and local governments	Authority,** local government	Local police, contract security	Local/state police, local fire services, EMS, other local
AIR NAVIGATION AND TRAFFIC CONTROL SYSTEM	Federal government	Federal government	Federal government	Federal government	Local/state police, local fire services, EMS, other local
Airfreight and package express systems, terminals, and hubs	Private	Private	Private	Private	Local/state police, local fire services, EMS, other local

Component of the Transportation Infrastructure	Typical Owner	Primary Source of Capital Funds	Primary Source of Operating Funds	Provider of Day-to-Day Security	First Responders During Crisis
Deep-draft seaports, Great Lakes, inland, and intracostal ports	Authority	Revenue bonds, federal, state, and local governments	Authority**	Authority police, contract security, USCG	Local/state police, local fire services, EMS, USCG
Marine terminals, equipment, and port intermodal facilities	Private	Private	Private	Private	Local/state police, local fire services, EMS, USCG
Marine vessels, containers, barges, and equipment	Private	Private	Private	Private	Local/state police, local fire services, EMS, other local
Inland and intracostal waterways	Federal government	Federal Authority**	Federal	USCG, state and local police	Local/state police, local fire services, EMS, USCG
Waterway locks and dams	Federal government	Federal government	Federal	Corps of Engineers or other federal	Local/state police, local fire services, EMS, other local
Air carrier airports	Authority	Federal, state and local governments	Authority**	Authority police	ARFF, authority/ local/state police, fire services, EMS
Airline passenger terminals	Authority	Revenue bonds, federal, state, and local governments	Authority**	Authority police	ARFF, authority/ local/state police, fire services, EMS
General aviation airports	Local government or authority	Federal, state, and local governments	Authority,** local government	Local police, contract security	Local/state police, local fire services, EMS, other local
AIR NAVIGATION AND TRAFFIC CONTROL SYSTEM	Federal government	Federal government	Federal government	Federal government	Local/state police, local fire services, EMS, other local
Airfreight and package express systems, terminals, and hubs	Private	Private	Private	Private	Local/state police, local fire services, EMS, other local

Component of the Transportation Infrastructure	Typical Owner	Primary Source of Capital Funds	Primary Source of Operating Funds	Provider of Day-to-Day Security	First Responders During Crisis
Passenger and cargo aircraft	Private	Private	Private	Private	Local/state police, local fire services, EMS, other local
Rail public transit systems (heavy rail, light rail, commuter)	Authority	Federal, state, and local governments	Fares, local and state governments	Authority, state, and local police	Local/state police, local fire services, EMS, other local
Bus public transit systems	Authority or local government	Federal, state, and local governments	Fares, local and state governments	State and local police	Local/state police, local fire services, EMS, other local
Passenger ferries	Authority or state government	Federal or state government	Fares, state or local governments	Local and state police	Local/state police, local fire services, EMS, other local
Transit passenger stations and stops	Authority or local government	Federal government	Authority, local & state governments	Authority, state, and local police	Local/state police, local fire services, EMS, other local
Intercity bus systems, terminals fleet	Private	Private	Private	Private	Local/state police, local fire services, EMS, other local
National Rail Passenger Corporation (Amtrak) system	Federal government	Federal government	Fares, federal government	Amtrak police	Amtrak/local/state police, local fire services, EMS
Intermodal passenger terminals	Authority or local government	Federal, state, and local governments	Authority, local & state governments	Authority, state, and local police	Local/state police, local fire services, EMS, other local

* Largely from dedicated fuel taxes, vehicle registration fees, and other user taxes and fees such as tolls

** Primarily from fees paid by users and lease revenues from tenants

Abbreviations used: EMS—Emergency Medical Services
USCG—U.S Coast Guard
ARFF—Aircraft Rescue and Firefighting (on-airport fire and rescue services)

Relative to funding, Table 2 shows that the federal government, while not a major owner of transportation infrastructure, is an important source of funding especially for capital improvements for highways, airports, and public transit. Obviously, the federal government also pays for expenses related to the components of the system that are federally owned, such as the air traffic control and navigation system, but also for activities such as harbor dredging, training of state and local transportation officials, transportation research, the work of the National Transportation Safety Board (NTSB), the National Motor Carrier Safety Administration (NMCSA), the U.S. Coast Guard, and other federal agencies that serve or support the transportation industry.

Another important consideration is that the majority of the public funds used to build and operate the transportation infrastructure come from direct or indirect user fees. Motor fuel taxes and vehicle registration fees, for instance, are the primary sources of state and federal funding for highways. Public transit operators receive significant portions of their revenues from passenger fares. Ports and airports rely heavily on revenues from leases and various user fees. Some freeways, turnpikes, bridges and tunnels are supported, at least in part, by tolls.

Of course, the railroads, pipeline companies, airlines, air cargo and express operators, trucking companies, steamship companies, barge operators, intercity bus companies, and other privately-owned transportation providers must rely on private financing for their capital improvements and must eventually pay all of their bills with revenues from their customers.

The column headed “Responsibility for Day-to-day Security” shows that the routine security of the transportation infrastructure is provided in a number of different ways Most components of the highway system, from major Interstates down to city streets, rely on state and local police for day-to-day security. The major railroads, rail transit authorities, many deep-water port authorities, and the largest airport authorities have their own police departments. Some transportation providers hire private companies to guard specific locations. Others rely entirely on their non-security personnel and local police patrols. Although not shown in the table, some tunnels and bridges have special security patrols. The Corps of Engineers and the U.S. Coast Guard (USCG) provide some day-to-day security for ports, locks and dams, and waterways.

In the column labeled “First Responders During Crisis,” the answer is virtually the same for every component. Most of the first responders to serious incidents of any kind, even at federally-owned facilities, will always be local or state—law enforcement officers (local and, in some locations, state), local firefighters, local emergency medical personnel, local emergency managers, and local or state transportation, public works and utility workers. Many federal agencies will eventually respond to the incident, but except for incidents on military bases, the most highly secured federal facilities, and the ports patrolled by the U.S. Coast Guard, the first responders will all be from state and local agencies, mostly local. In some rural areas many of the first responders will be volunteers.

This broad overview of the “national transportation system” describes the general framework within which state and local transportation policy is made. Many exceptions can be found, and circumstances and priorities vary in important ways among the states and localities. For instance, the states that are home to the nation’s seaports and the states that border Canada and Mexico

have some unique transportation issues. States with military installations, nuclear power plants, and other sensitive facilities also have special issues, as do cities with major bridges or tunnels, intermodal terminals, and international airports. However, the system is complex in every state and community.

Implications For State And Local Transportation Policy

Recognizing the uncertainty of the situation and the complexity of the transportation system, some of the security implications for state and local transportation policy are discussed below, under the following headings:

- Institutional issues
- Financial issues
- Planning and design issues
- Human resource issues
- Communication and information management
- Building on experience
- Accelerating current initiatives

Institutional Issues

Security issues are now receiving the direct, personal, and sometimes undivided attention of many national leaders as well as the top executives in state and local governments –including governors, state DOT secretaries and commissioners, mayors, city managers, public transit directors, airport managers, and public works directors. Circumstances have demanded high-level attention. However, as we move beyond crisis management, responsibilities for security will be institutionalized and integrated into overall decision-making processes.

The federal government moved quickly in creating new agencies, reassigning responsibilities and resources, and breaking down some traditional boundaries. Two of the most notable actions from a transportation perspective were the creation of the Transportation Security Administration (TSA) within the U.S. Department of Transportation and the subsequent appointment of a career law enforcement officer to head the TSA. (3)

The TSA's initial focus is on screening airline passengers and baggage and performing other security activities at the more than 400 U.S. airports with scheduled airline passenger service. The Federal Aviation Administration (FAA) already had oversight responsibilities for these activities, and the employees in the FAA's Office of Civil Aviation Security are moving to the TSA.

However, the TSA is also hiring thousands of new employees, and TSA employees will soon be conducting security inspections at the 400 plus airports. Each airport will have a Security Director employed by the federal government. Passengers will be screened, not by airline or airport employees, private contractors, airport police officers, or local or state law enforcement officer, but by a federal agent. The situation is not totally unprecedented, since U.S. Customs agents have full responsibility for other activities in many of these same airline terminals, but the scale is certainly different.

Do the TSA activities relative to airports signal a broad change in federal policy? Is this the first step toward direct federal control of security throughout the transportation industry? Will federal agents conduct security checks for other modes of passenger travel? What about security in ports, rail terminals, and air cargo hubs? John Magaw, the Under Secretary of Transportation for Security, made the following statement to a House committee on January 23, 2002:

> The TSA is charged with security for all the modes of transportation, and a focus on aviation mandates must not slow the TSA's pace in addressing the security needs of other transportation modes. Across every mode, we must continue to develop measures to increase the protection of critical transportation assets, addressing freight as well as passenger transportation. We will maintain a commitment to measure performance relentlessly, building a security regime that provides both world-class security, and world-class customer service, to the American people. (4)

In the meantime, will state and local governments make any institutional changes relative to transportation security? In December of last year, the National Emergency Management Association reported that:

> While most states had terrorism task forces or WMD (weapons of mass destruction) working groups in place prior to September 11, many states felt the need to give terrorism preparedness a heightened awareness. At least eighteen states have created new task forces, commissions, advisory panels or similar bodies to further address terrorism preparedness. These are interagency, executive-level bodies that serve a number of purposes including review of: the state's existing emergency operations plans . . . critical infrastructure security and cyber terrorism issues, terrorism preparedness funding and resource needs and state authorities to deal with acts of terrorism. (5)

A more recent scan of state government Web sites indicates that most of these coordinating groups include the heads of cabinet-level agencies responsible for public safety and law enforcement, military (National Guard), public health, agriculture, transportation, and the state's emergency management agency responsible for "all-hazards" planning and response. Many also include representatives of agencies responsible for information technology, environment and natural resources, and other state functions. Also, every Governor has now designated a person as the state's point of contact with the President's Office of Homeland Security, and most of those contacts seem to be either the chair of the coordinating group or the director of the emergency management (all-hazards) agency.

The key point here is that state governments seem to be relying on coordination among existing state agencies and refocusing the resources of those agencies, rather than creating new organizational units. State transportation agencies are integral parts of those coordination efforts in most, if not all, states. New agencies could be created in the future, but for now the success of state efforts to improve transportation security seems dependent on developing new or more effective internal and interagency working relationships.

Especially important will be the working relationships between transportation agencies and the agencies responsible for public safety and security. What will these relationships look like? To

what extent will transportation agencies be responsible for security? To what extent will law enforcement agencies be responsible for transportation? How will decisions be made about: appropriate levels of funding, privatizing security functions, or assignment of security responsibilities? How will state and local agencies work together, work with federal agencies, and work with private transportation providers?

Regardless of what the Transportation Security Administration does, state and local transportation officials will have to develop new relationships with federal, state, and local law enforcement agencies. A unique aspect of this situation is that the federal-state-local transportation relationships are well developed and comprehensive, especially in the highway, public transit and airport programs. In many cases, the state and local agencies are, in effect, the implementing agents for the federal programs. However, federal, state, and local law enforcement agencies generally have completely separate jurisdictions and responsibilities, and seem to work together more on a project basis.

The American Association of State Highway and Transportation Officials (AASHTO) conducted a "Security and Emergency Response Survey" of state transportation agencies in November and December 2001. Some of the survey questions asked about outside agencies that had been consulted by the transportation agencies in preparing emergency response plans. By the end of January 2002, 51 agencies had responded. The results, shown in Table 3, point to some areas where new relationships may be needed. (6)

Of the twenty-nine agencies or categories of agencies listed in Table 3, the majority of the state DOTs consulted only five—FHWA, state emergency management agencies, state law enforcement and public safety agencies, and airports. Almost all of the DOTs consulted FHWA and their respective state emergency management agency. Fewer than a third of the DOTs consulted with any of the private sector organizations. Only nine consulted with a Metropolitan Planning Organization or Council of Governments, and fewer than a dozen consulted FRA, FTA, or the Research and Special Projects Administration (RSPA).

TABLE 3. NUMBER OF STATE DOT'S CONSULTING WITH OTHER FEDERAL, STATE AND PRIVATE SECTOR ORGANIZATIONS ON EMERGENCY RESPONSE PLANS (51 TOTAL RESPONSES) (6)

Number Consulting with Agencies of U.S. DOT	
FHWA	48
FAA	24
FMCSA	18
U.S. Coast Guard	16
FRA	11
FTA	9
RSPA	2

Number Consulting with Other Federal Agencies	
FEMA	18
DOD	16
Security Agencies	12
U.S. Treasury	7
Homeland Security	7
DOE	5
HHS	3
EPA	1

Number Consulting with Other State Agencies	
Emergency Management	45
Law Enforcement	38
Public Safety	37
Airports	26
Health Departments	22
Transit Agency	22
State's Attorney	18
Ports	15
Bridge/Tunnel	11
MPO/COG	9

Number Consulting with Private Sector Organizations	
Railroads	15
Utilities	12
Motor Carrier Associations	13
Oil and Gas Companies	8

The point is not to criticize the DOTs that did not consult with one agency or another. In all likelihood, many of the other agencies also made decisions about emergency management with out consulting with their respective DOT. In some cases the DOT may not have *needed* to consult with all of the listed agencies. The point is that some of the listed agencies and the DOTs have common, overlapping, or mutually dependent responsibilities relative to security, and circumstances seem to call for closer working relationships.

Also, transportation agencies must decide on internal roles and responsibilities for security. As noted earlier, most of the large airport authorities, transit and port authorities, and railroads already have their own police departments, but "security" can involve many different activities. Responsibilities for those activities could be divided among different units, even in organizations with their own police forces. Within a state DOT, should a special unit be organized to promote (or oversee) security considerations throughout the department? Currently, many of the state transportation CEOs seem to be filling that role, but are procedures in place to ensure that information flows downward and throughout the organization as needed? (The AASTHO survey

found that only 28% of the CEOs for state transportation agencies had a federal law enforcement security clearance, although another 20% were "in the process" of obtaining a clearance.) (7)

Financial Issues

No one doubts that increased transportation security will have a financial cost. In some cases, new equipment or facilities will be needed. In other cases, the new concerns about security will increase the costs of otherwise needed capital improvements. In virtually every transportation organization, the greater emphasis on security will add to the costs of operations.

Even setting aside the costs of the damages inflicted on September 11th, all levels of government anticipate significant increases in spending. The President's budget proposal for FY 2003 includes almost $38 billion dollars for "homeland security," not including expenditures to combat terrorism abroad. (8**)** The National Governor's Association estimates that the costs to state governments during the year following September 11th will exceed $4 billion, with about $3 billion devoted to bioterrorism preparedness and emergency communication and $1 billion for guarding critical infrastructure. (9) The U.S. Conference of Mayors estimates that the twelve-month costs for the cities with over 30,000 population will be $2.1 billion. (10)

And where will the money come from? Improvements in security at the state and local levels will require additional revenues or reduced expenditures for other purposes—or both. At the federal level, security spending is being blamed for the return to "deficit spending."

In addition to direct federal expenditures, by the Department of Defense, the Coast Guard, the TSA, and other agencies, the federal government has added significant new dollars to existing security-related grant programs and has proposed new grant programs and even higher levels of funding in upcoming years. Federal grants will be available to help improve public health systems, buy new equipment for first responders, upgrade emergency training, and help pay for other needed improvements. However, with one exception, no new federal funding has been set aside for transportation purposes, and it appears that, at least for the immediate future, state and local transportation agencies will have to rely on their existing revenue sources. The exception is a new Port Security Grants Program, administered by the TSA, to "finance security enhancements at critical national seaports." (11)

State and local transportation agencies are already facing significant budget problems. Travel is growing much faster than the capacity of the transportation system, and the unit costs of adding capacity are growing even faster. Maintenance and operating costs are demanding larger shares of transportation budgets each year. The yields on gasoline and motor fuel taxes, the mainstay of federal and state highway funding, are not keeping pace with travel, because vehicles are more fuel efficient and alternate, untaxed fuels are more widely used.

Further, some of the long-standing support for dedicated funding for transportation seems to be eroding. Maintenance and operating expenditures usually do not attract the same kind of political support as "new projects." Also, the overall strain on state budgets is putting "trust funds" in jeopardy.

Regardless, the most direct way to pay for more security would be to increase transportation user fees—taxes on fuel and vehicle registration, passenger fares, tolls, leases and rentals, and ticket taxes. The federal government has added a $2.50 per segment (boarding) "security fee" on airline tickets, with the revenues dedicate to help pay for more security at airports.

In many cases, however, the benefit to the transportation user may not be so direct or so easy to calculate. Even agreeing on the actual costs of security may be tough. Sometimes transportation improvements will be specifically for security enhancements, and the security costs can easily be separated from other costs. Other times, however, improvements in security will be imbedded in larger programs and projects, and cost allocation will be difficult.

Also, equity issues have to be addressed. Should gasoline taxes be raised to pay for investments in system redundancy, or should general fund tax revenues pay some of those additional costs for economic security? Should transit passengers be charged higher fares to improve security at the downtown transit mall, or should property taxes cover some of the costs? Should specific roadway and bridge tolls be raised to help pay for more troopers assigned throughout the state?

State and local transportation officials, as well as private transportation providers, may also need to consider the costs they would have to absorb from an act of terrorism. Direct federal intervention and federal assistance would be expected, but which parts of the direct and indirect cost would the federal government pay? How much help could the state government provide to the local governments? Obviously, state and local governments have ongoing financial risk management programs that consider all types of emergencies and potential losses, but terrorism presents some new challenges. A group known as the Coalition to Insure Against Terrorism, which includes the American Association of Railroads and the Associated General Contractors, is asking Congress to enact a terrorism insurance plan or "security net" to "ensure that comprehensive terror-related coverage is both available and affordable" for the private sector. (12)

Human Resource Issues

State and local governments will also have to address a range of human resource issues. According to the Bureau of the Census, in March 2000, state and local governments employed more than 13 million full-time employees and almost 5 million part-time (15 million full-time equivalents). (13) All of those employees are concerned about security in their work places and about what new responsibilities they may have in preventing or responding to acts of terrorism.

The people most directly concerned are the police, fire fighters, emergency medical personnel, and other first responders who are most at risk. The Census reports that state and local governments employ approximately 870,000 law enforcement personnel and approximately 270,000 firefighters. (14) The Bureau of Labor Statistics estimates that another 170,000 people worked in 2000 as emergency medical technicians and paramedics. (15) The national Office of Homeland Security estimates that another 750,000 Americans are volunteer firefighters. (16) The above numbers total to 1.3 million full-time emergency responders and another 750,000 volunteers. (For comparison, the total active duty force for the U.S. military—Army, Navy, Marine Corps, and Air Force combined, was approximately 1.4 million people in 2000.) (17)

Many of the state and local first responders have questions about pay and benefits in relation to new job requirements, hazardous duty criteria, policies for overtime work, additional training to deal with weapons of mass destruction, the adequacy of their personal protection equipment, whether or not they have access to complete information about current threats, and other issues specific to their job, community, or personal circumstances. Many hospital and public health employees have similar questions.

Another 800,000 state and local employees work in transportation jobs (highway, airports, water transportation and terminals, and public transit), and some state and local officials have suggested that these workers should be the "eyes and ears" to protect the transportation infrastructure. (18) What will this mean in terms of actual day-to-day responsibilities, working conditions, and pay? What kinds of new training will be offered? What if one of these workers overlooks a threat? What if an overzealous transportation worker causes harm to innocent people?

State and local governments must also contend with human resource issues involving National Guard and Reserve forces. As an employer, state and local governments lose the services of valuable employees when they are called to active duty, and most state and local governments extend special benefits to ensure that the individuals and their families do not suffer financially while serving on military duty. Could long term or frequent use of National Guard and Reserve forces leave some public agencies seriously shorthanded and with unbudgeted expenses?

On the other hand, these reserve forces, especially the National Guard, are integral resources in responding to domestic emergencies of all kinds. National Guard troops have been very visible in U.S. airports since September 11th and have been guarding critical infrastructure throughout the nation.

The National Guard has dual missions, (federal and state), reporting to their respective Governors during normal circumstances, but subject to being "federalized" when needed for national emergencies and may even be used as part of overseas military action. In addressing the new concerns for security, what roles do the state governments see for their Army and Air National Guard units relative to security and how do those expectations match with the expectations of the federal government and the Department of Defense?

Finally, state and local governments will have to deal with issues related to background investigations and identification (ID) cards for people who work in transportation and other sensitive jobs. Some business and government leaders have proposed that a national system be established to issue ID cards for all citizens. Others have proposed national systems for transportation workers. (19)

Rear Admiral James Underwood of the Department of Transportation's Office of Intelligence and Security, made the following statement to a Congressional committee in February, 2001:

> The credentialing of transportation workers is but one part of a security system, and it is likely the most challenging because it raises fundamentally important concerns about individual privacy and interoperability. (20)

Regardless of what happens in Washington, state and local governments may require security checks for their own transportation employees and even for private sector employees working around public infrastructure. Some controversy will be unavoidable, not to mention the difficulties of administering background checks and IDs. Privacy and confidentiality issues will abound. The time and expense for thorough investigations will be substantial. Inevitably, some current employees with years of honorable service will not meet the established criteria because of some previously undisclosed incident in their backgrounds. Policy makers will have to weigh all of the likely controversies and costs against the risks of not performing such checks and not issuing IDs.

Legal Considerations

State governments have been quick to act on the legislative front, beginning with a package approved by the New York state legislature on September 17, 2001. The New York package added six new penal offenses, expanded the scope of the state's death penalty, loosened restrictions on eavesdropping, and authorized New York to join other states in the Emergency Management Assistance Compact (EMAC). (21)

Most, if not all, of the other state governments have also launched reviews of their state statutes and regulations, and bills are being debated in a number of states. The Web page for the "Suggested State Legislation" program sponsored by the Council of State Governments offers seven anti-terrorism bills that were enacted by state legislators prior to September 2001, along with a host of other bills that have been or are now being considered. (22)

In these various bills state legislators have attempted to deal with many different subjects, including cyber terrorism, paid leave for state employees who volunteer for emergency relief work, mutual aid pacts, possession of weapons of mass destruction or biological agents, protection of crops, requirements for drivers licenses and hazardous material endorsements, aerial spraying for agricultural purposes, and organizational changes within state government to facilitate homeland security. Many of these bills specify or clarify that certain acts are illegal and then prescribe minimum or standard penalties for violations of the anti-terrorism statutes. In some cases, the laws also impose penalties for making terrorist *threats.* Also, a number of states are considering bills that would amend Freedom of Information statutes and limit public access to certain records.

Relative to transportation, bills have been introduced or proposed in at least eleven states, including Michigan, Maryland, Virginia, and Florida, requiring background checks for flight training applicants or photo identification cards for aircraft pilots. The Aircraft Pilots and Owners Association (AOPA) has opposed the background checks for U.S. citizens and argued that any government issued ID card with a photograph should be adequate. (23) (Pilots' licenses are issued by the Federal Administration Agency (FAA) through a system of designated examiners. Some states also require a pilot to "register" in that state.)

The Florida legislature passed a bill in May 2001 that is now receiving national attention because the bill sets out standards for security at Florida's 14 deep-water ports. One provision requires that each port conduct background investigations and issue identification cards to all port workers, including truckers who move loads to and from the port. The American Trucking Association, the Teamsters and others are complaining that requiring a separate ID at each port is unreasonable.(24)

Beyond the initial flurry of action, an array of other legislative or regulatory questions may still need to be addressed in many communities. When emergency plans are updated, agencies may need new powers, and new questions may be discovered. Which state or local regulations might need to be suspended or streamlined during emergencies? Who would have the authority? Can the police department tow away suspicious vehicles without waiting the normal time specified in the statute for abandoned vehicles? Can public transit vehicles and school buses be used interchangeably during emergencies? Which agency will have legal responsibility under different scenarios?

More broadly, do transportation workers, volunteers, or others who respond to incidents that are not part of their normal job duties have sufficient protection against liability? Can public funds be used to protect privately owned infrastructure, e.g., railroads, pipelines, and truck or river terminals? Can state and local governments justify such actions on the basis of public *interest*? What if the security of the private infrastructure is breached anyway?

Communication and Information Management

Transportation officials also must grapple with some thorny communication and information management issues. The overarching policy challenge is to ensure that secrecy for the sake of security does no more harm than good. Many of the basic issues related to secrecy and public information will be debated and eventually resolved at the national level. At every level of government the media and various public interest groups will be alert to abuses, and the courts may have the final say on some of the issues.

In the meantime, after decades of striving for more extensive public involvement in transportation planning and decision-making, circumstances now seem to call for secrecy and suppression of information. State and local governments have moved quickly to ensure that some information is more closely guarded. An article in the Lexington Herald-Leaders noted that, "State legislators from Florida to Washington are debating what should be concealed in the interest of public safety, such as blueprints for bridges, tunnels and airports." The article questions whether state legislators are going too far in restricting information for public safety. (25)

Federal and state officials are in a quandary about the well-developed system for the placement of "placards" on buildings, tank cars, trucks, and other containers to alert emergency responders to the presence of hazardous materials. These placards may also identify the vehicle, containers, or building as an attractive target for malicious or deranged acts. Are the advantages of these placards in emergency situations enough to offset the risks? Can the information be made available to emergency responders in some other, more secure, way?

Public officials are also scrutinizing the information posted on the Internet. An article in the New York Times began with:

> The Pataki administration has quietly ordered state agencies to restrict information available on the Internet and limit its release through New York's Freedom of Information Law to prevent terrorists from using the material, . . . which includes maps of electrical grids and reservoirs as well as building floor plans. The state's new policy guidelines to restrict information and tighten security are occurring in lock step with the national debate over how to balance the need for safety and the public's right to information. (26)

The following message was posted on the Web site for the National Pipeline Mapping System, an initiative led by the Research and Special Projects Administration (RSPA) of the U.S. DOT:

> The Office of Pipeline Safety (OPS) has discontinued providing open access to the National Pipeline Mapping System (NPMS). Recent events have focused additional security concerns on critical infrastructure systems. Due to these concerns, OPS no longer provides unlimited access to the Internet mapping application, **. . .** At this time, OPS is providing pipeline **data** (not access to the Internet mapping application) to pipeline operators and local, state, and Federal government officials **only**. (27)

Also, the Container Working Group, an offshoot of the National Infrastructure Security Committee, created by Transportation Secretary Norman Mineta shortly after the September 11 attacks, has announced that it "will not release the details of its recommendations to help prevent terrorists from launching an attack by using some of the estimated 5.7 million shipping containers that enter the country each year." (28)

In addition to protecting specific items of information, transportation policy makers face some questions about public involvement in sensitive processes. As security becomes an integral part of transportation planning and decision-making, how will we ensure that the interests of all stakeholders are represented without compromising security? Will some participants be asked to "leave the room," figuratively or literally, when certain subjects are discussed, or will those subjects be discussed off line from other transportation decisions?

Also, new standards and protocols seem to be needed for communication of risk information. How should transportation departments and authorities, private transportation providers, shippers, and law enforcement and other emergency response agencies share information among themselves and with the public and the new media? Which items of information will be shared, and how will the information be communicated? How will information be assembled and evaluated to present a comprehensive picture of vulnerabilities, threats, and potential consequences? Who will have access to the "big "picture"?

Perhaps the toughest question: What information does the public need to make informed decisions? How much does the public need to know about vulnerabilities in the transportation system? Should the public be informed about specific threats? Should efforts be made to educate the public on how to interpret risk information?

All other issues aside, the public will have to rely on key public officials—state and local elected officials, department heads, transportation board members, airport authority, transit and port authority board members, transportation labor leaders, and others—to ensure that the public interest is served, even with less public scrutiny of the decision-making processes.

Planning and Design Issues

The emphasis on security also adds yet another factor for transportation planners and designers to consider. We now want our transportation systems to be "safe, effective, efficient, and *secure*." New criteria may be needed for the planning and design processes, and efforts may have to be redoubled to involve law enforcement, fire services, and other emergency workers in the planning and design process. In many cases, the railroads, pipelines, trucking companies, airlines and other private transportation providers may need to be consulted sooner and more often.

Many of the questions about planning and design are technical, but many also have important policy implications. Planners, for instance, may need to consider whether additional capacity should be added, not on the existing route, but on a nearby but separate location to ensure redundant access during emergencies. Tradeoffs will have to be made between construction and the costs of more secure operations, between user costs and user security, and possibly even between an alternate that is easier to secure and one that provides a higher level of service.

Nuclear plants, other power generation and transmission facilities, fuel storage areas, chemical plants, intermodal terminals, military installations all need good access to the various components of the transportation system for daily operation and for emergency response. Designers will be challenged to provide that level of service but also a high level of security against unauthorized access.

The concern for security also calls for designers to be more mindful of the demands placed on transportation facilities during emergencies. How will emergency responders reach the scene? How will injured persons be evacuated from the scene? How will traffic be diverted, short term and for extended periods? Should areas be designed specifically for staging of emergency workers and equipment or storage of debris? How would firefighters get water to the scene? Could normal highway configurations (lane and ramp directions, traffic signals, signing) and transit routes be altered systematically to facilitate large-scale evacuations?

To ensure that security concerns are fully addressed in the planning and design processes, the agencies responsible for security and emergency response along with private sector transportation providers need to be involved in those planning and design processes. However, most law enforcement officers, fire service officials, and other emergency workers, as well as private sector transportation providers, can become frustrated with the slow and often laborious processes involved in transportation planning. Transportation planners and designers sometimes may not understand the need for immediate decisions and operational expedience. These communication issues are not new, but the need for solutions seems more urgent.

Influence of Federal Actions

In what ways will the federal government influence state and local policies relative to transportation security? How will the federal government use its authority and financial

resources to encourage state and local government to carry out national priorities relative to security and transportation? Probably in all of the following ways:

- Laws or regulations that apply to all individuals and corporations
- Mandates directed specifically at state or local governments or the transportation industry
- Categorical funding programs specifically for transportation security
- Security requirements for use of federal funds under broad program categories
- Funding incentives or disincentives for specific actions
- Earmarked funds
- Training and other technical assistance delivered by federal agencies

Until now, the federal government has focused more on direct federal action, and the impacts on state and local government have been limited. In addition to the actions of the Transportation Security Administration, the FAA has closed three Washington, D.C. area airports for extended periods and established "no-fly" zones in numerous states. (29) Increased federal funding for specific programs has required increased state and local matching funds to help first responders buy equipment and to upgrade public health systems. FEMA, the Department of Justice, and the U.S. DOT are sponsoring new training programs and seminars.

However, major federal decisions with long-term implications for transportation are just ahead. The legislation that authorizes the federal surface transportation programs will expire on September 30, 2003, and the "reauthorization" process is underway. This is occurring at a time when the Administration and Congress have responded to the immediate security crises and are now able to consider using some or all of the powers listed above (e.g., laws and regulations, mandates, categorical funding) to advance transportation security.

Many of the current federal programs were initiated under the Intermodal Surface Transportation Efficiency Act, known as ISTEA, or the subsequent bill, known as TEA-21 (Transportation Equity Act for the 21st Century). With the new emphasis on security, might the next authorization be known as "SecureTEA"?

The new bill will influence state and local transportation policies for several years into the future. Will (or should) security be a driving influence? Should Congress use all of its powers to foster security, or simply add "security" to the list of eligible uses of federal transportation dollars? Should state and local governments have to prepare Security Impact Statements (SISs) for major projects in the future? Should law enforcement officials be designated participants in the Metropolitan Planning Organizations? Should new types of plans or planning processes be mandated? Should federal agencies have a "security veto" over state or local transportation decisions?

The money, of course, will get the most attention during the reauthorization process. State and local agencies and various interest groups will lobby to ensure that their respective jurisdictions and programs receive a fair (or better) share of the authorized federal dollars, that the funds can be used for purposes that are consistent with state, local, and interest group priorities, and that the federal "strings" will be tolerable. The process will not always be orderly, but most state and local officials and interest group representatives know how to participate.

However, two ingredients of this mix seem especially unclear. First, many state and local governments may not yet have a clear vision of what their role *should* be in transportation security and, therefore, may not be sure of their best interests in the new authorization. Second, no interest group exists to promote "security" in the same ways as other groups promote environmental protection, traffic safety, sustainable transportation, or economic growth. For both of these reasons, organizations that represent the governors, mayors, and legislative officials, as well as AASHTO, the American Public Transit Association (APTA), and other transportation interest groups, will be especially important to the process. Hopefully, these groups can come to agreement on some basic priorities relative to security and ensure that the security provisions of the new bill will influence state and local transportation policy in constructive ways.

Building on Experience

All of the above notwithstanding, state and local governments have considerable experience that can be applied or adapted to deal with the increased emphasis on transportation security. State and local governments have know-how from planning and executing hurricane evacuations, preparing and executing plans for earthquakes, nuclear evacuation planning and drills, managing special events that stress the transportation system, all-hazards emergency management planning, including responses to inclement weather, floods and other natural disasters, and, of course, law enforcement.

The Coastal states that are in the path of hurricanes have significant experience in planning and executing emergency responses on a large scale. In these situations, critical components of the transportation system may be damaged or destroyed over a wide area at a time when the system is needed to evacuate people and to move emergency personnel and equipment. Concurrently, other critical or sensitive infrastructure, including power generation facilities, chemical plants, military installations, and hospitals, may also have been severely damaged or in danger. State and local governments in these states have experiences that seem almost directly transferable to dealing with security threats or attacks.

Other states, especially California, have experience in preparing for and dealing with earthquakes, both the associated damage to the transportation system and the exceptional demands placed on the system. The pictures of the collapsed upper deck of the Cypress Freeway (I-880) and the failed section of the San Francisco-Oakland Bay Bridge were probably the most widely seen images of the Loma Prieta Earthquake in 1989. The Northridge earthquake in 1994 caused bridge failures on freeways in the Los Angeles area. These and other earthquakes caused severe damage to the transportation system, placed exceptional demands on the system for emergency response, required accelerated work to repair the damages, and required the system to function for extended periods without full capacity. States and local governments would face the same challenges following a widespread, deliberate attack.

Since 1980, every nuclear power plant in the United States has been required by federal law to prepare emergency response plans and to ensure that "off-site" plans exist to protect public health and safety. The off-site plans, approved by the Nuclear Regulatory Commission (NRC) and the Federal Emergency Management Agency (FEMA), must provide for protective responses for the community in 10-mile and 50-mile "emergency planning zones." Each site must test its plan biennially in an emergency exercise. State and local governments, including

transportation officials, participate in the biennial exercise. The Nuclear Energy Institute reports that several nuclear emergency plans have been used successfully to cope with other types of local emergencies, such as chemical spills and fires. (30)

Most states and local governments have experience in preparing for and managing special events that stress the transportation system. State and local officials, with help from federal agencies and the private sector, have provided effective and secure transportation services for events as large as the Olympics, most recently in Atlanta and Salt Lake City, the Millennium celebrations, political conventions, Super Bowls, and other recurring events such as Mardi Gras, New Year's Eve at Times Square, athletic and sporting events, and a wide range of national and international conferences and local events. Large numbers of people and vehicles are moved to and from these events, often in very short periods of time, requiring extensive planning and precise execution.

On a more comprehensive basis, the Federal Emergency Management Agency (FEMA) and counterpart agencies in each state, large city, and many counties conduct ongoing "all-hazards" planning. These emergency management agencies also coordinate the use of resources needed in response to hurricanes, earthquakes, industrial or transport accidents involving hazardous materials, floods, snow and ice storms, and other emergencies. In May of 2001, FEMA announced the availability of new terrorism preparedness planning guidance for state and local governments. The purpose according to FEMA was to give state and local emergency planners:

- Information and a framework for developing supplemental emergency operations plans to address the consequences of terrorist acts involving weapons of mass destruction; and
- A consistent planning approach to help foster efficient integration of state, local, and federal terrorism consequences management activities.

The new guidance was published as a supplement to a publication entitled *Guide for All-Hazard Emergency Operations Planning.* (31)

Of course, law enforcement agencies at all levels of government and in the private sector were concerned about transportation security issues long before September 2001. Federal, state and local law enforcement agencies have extensive experience with transportation of drugs, stolen goods, and other contraband; hijacking; human trafficking; evading fares and tolls; evading inspections; and the safety and security of passengers and cargo. The railroads, steamship companies, warehouse operators, major shippers, insurance companies, and other private sector organizations have developed procedures and technologies to avoid, detect and respond to the theft of cargo. Railroad and transportation authority police forces work constantly to prevent unauthorized access and to apprehend violators. The report of the Interagency Commission on Crime and Security in U.S. Seaports (Fall, 2000) considered the possible threat of terrorist acts, but focused on theft of cargo and other crimes. (32)

Also, state agencies inspect all commercial vehicles trucks and license all motor vehicle operators. Federal, state and local agencies enforce environmental laws and regulations. State and local law enforcement agencies observe vehicles on the roadways, enforce state and local

traffic laws, and deal with a wide range of "ordinary crimes" that involve transportation directly or indirectly.

Further, many state and local transportation agencies had incorporated terrorism preparedness in their security planning long before September 2001. Most large pubic transit agencies, for instance, have formal safety and security plans based on joint efforts by the transit industry, the Federal Transit Administration, and the Transit Cooperative Research Program.

State and local transportation officials can draw on all of the experiences described above in responding to the new emphasis on security. Of course, state and local governments in Oklahoma, New York, Virginia and other states also have direct experience with major acts of terrorism.

Accelerating Current Transportation Initiatives

The increased emphasis on security should give new impetus to a number of transportation initiatives that were underway before September 11th and have the potential to make our transportation system more secure as well as more effective, efficient, and reliable. The tendency, of course, will be for advocates of every transportation initiative to argue that their program or project will "also improve security." In fact, most improvements in the transportation system will have some security advantages, if only by making the system more resilient to attack. However, a few major initiatives, as described below, seem to have distinct promise.

The set of initiatives, usually described as Intelligent Transportations Systems (ITS), can contribute to security in a number of ways. For all components of surface transportation, video cameras and electronic sensors that monitor key components of the system can improve security for those components. System-wide monitoring allows for more informed responses when problems do occur, alerting transportation officials to problems and allowing quick and effective responses.

For highways, the information collected via cameras and other sensors are usually monitored in a "traffic management center." These centers often house law enforcement agencies as well as transportation agencies, and virtually every center has direct communications, using multiple technologies, with law enforcement agencies, fire services, emergency medical services, other emergency responders, public transit operators, and public works agencies. Virtually all of the centers have backup power sources and many are designed to continue operations under adverse conditions, ensuring effective communication during emergencies.

Using the information gathered from the field, transportation and law enforcement officials in the traffic management can adjust traffic signals, ramp meters, and dynamic message signs along the roadway, or send travel information to the news media or directly to motorists. The center can also notify or dispatch emergency responders as needed.

An initiative often related to the deployment of ITS is "traffic incident management," focusing on the prompt and effective response to crashes and other incidents (e.g., disabled vehicles, debris in the roadway) as well as special events. Such initiatives are usually built on coordination among transportation agencies, police, fire services, emergency medical services, and towing and recovery operators. Often, the transportation agency will establish a " freeway service patrol" to

augment the resources already provided by the emergency response agencies. The programs usually target day-to-day incidents that create congestion on high-volume urban freeways, but the working relationships and resources developed as part of such programs have proven useful in responding to incidents that impact entire corridors over long periods of time

The potential security benefits of ITS are not limited to highways or to dealing with traffic congestion. For instance, the use of Geographic Positioning System (GPS) and other technology for tracking vehicles and cargo can enhance security and emergency response for trucking as well as rail and water transport. Advances in radio communications, enhanced commercial vehicle operations and driver credentialing technologies, access control, and other technologies offer multiple benefits for security. Further the integration of GPS with Geographic Information Systems (GIS), databases, and the Internet can allow delivery of powerful information for tracking and for responding to any incidents that might occur.

Other initiatives that seem to have important secondary benefits for transportation security include:

- Increasing the focus on, and commitment of resources to, highway "operations and management," including regional efforts to facilitate communication and joint response to system disruptions

- Improving freight security and developing more effective working relationships between the public and private transportation sectors
- Developing technology, software, and operating procedures to facilitate effective on-scene communication between police, fire, emergency responders, other emergency responders, transportation officials and others who respond to transportation emergencies

- Enhancing public safety and security against *all* crimes at passenger terminals, bus and train stations, other passenger waiting areas, cargo terminals, and intermodal facilities

- Implementing projects that will help reduce traffic congestion as well as make the system more resilient or better able to respond to attacks

Finally, state and local governments may choose to accelerate projects or programs that have multi-state significance. Projects to assess or improve physical connections between states (especially major highway and rail bridges, ferries, or commuter rail services) may warrant special attention.

Suggestions For Additional Consideration

The information presented in this paper is too general and the circumstances too unsettled to warrant sweeping recommendations. However, some ideas for further attention, discussion, and research are offered below in six broad categories, expressed as goals for state and local transportation agencies:

- Ensure clarity of institutional responsibilities

- Conduct comprehensive risk assessments and establish risk management procedures for state and local transportation
- Enhance working relationships with private sector transportation providers
- Enhance response capabilities for events that might target or stress the transportation system
- Incorporate security in transportation planning, design and operations
- Accelerate initiatives with comprehensive benefits

Ensure Clarity of Institutional Responsibilities

As noted above, most state and local governments seem to be relying on existing organizations and agencies to deal with transportation security issues. That approach has many advantages, but success will require that all of the existing organizations have a clear understanding of their new responsibilities. Change does not come easily in any organization, even when the stakes are very high.

A special issue for state governments is that some of the critical components of the transportation infrastructure from a state (or even national) perspective may be located in a small city or rural community with very limited resources for security or emergency response. Which agencies of state government will provide those resources? Or, will state government help the local governments develop expanded resources?

Also new working relationships are needed between and among federal, state, and local *transportation* agencies and federal, state, and local *law enforcement* agencies. As noted above, state and local transportation officials cannot assume that those relationships will develop automatically, and state and local transportation officials may need to take the initiative.

Best practices will emerge as state and local governments gain institutional experience with these new priorities, organizational structures, inter-agency relationships, and the interrelated related human resource, legal and funding implications. Research will be needed to identify those best practices and to learn from unsuccessful approaches.

Establish Comprehensive Risk Management Procedures for State And Local Transportation

Much work has been done and more is being done to assess the vulnerabilities of our national transportation system, develop means of protecting the system, and prepare effective responses for threats or attacks that impact the system. However, unique state and local needs and circumstances also need attention.

New tools will be needed to help state and local transportation officials understand their unique problems and develop appropriate responses. Which components of the state or local transportation infrastructure are the most important from a distinct state and local perspective? Which are the most vulnerable? What are the critical interrelationships between components of the transportation infrastructure and between transportation and other infrastructure, e.g. power, communications? What protection and response strategies would be the most effective for state

and local governments? What proportion of state and local resources should be devoted to hardening versus improving response capabilities?

Enhance Working Relationships with Private Sector Transportation Providers

The emphasis on security is one more reason for state and local governments to have effective working relationships with the railroads, trucking companies, terminal operators, pipeline companies, airlines, and other private sector transportation providers that serve or traverse their respective communities. The public and private sectors have obvious common interests at locations where the public and private infrastructure connect, intersect, or are in close proximity, e.g., intermodal facilities, highway-railroad crossings, pipeline crossings, fuel storage areas, and intercity bus terminals. Of course, the private sector transportation providers are critical to the overall transportation system in the state and community.

The emphasis on security also calls for a particular level of coordination with local representatives of the railroads, trucking companies, pipeline companies, intercity bus companies, and other providers. In many cases the local fire services have pre-planned responses to emergencies at private sector terminals and other sites, and the local police have worked with the railroad police, private security, or company officials on crime and law enforcement issues. However, comprehensive security and emergency response plans may not have been prepared, and state and local *transportation* officials may not have been participants.

Finally, state and local officials should recognize that private transportation providers, like other businesses, rely on public utilities and communication systems for essential services. Plans for protection and, when necessary, restoration of utilities and communication should recognize the importance of the private sector transportation providers in the overall transportation system.

Improve Response Capabilities for Events that Might Target or Stress the Transportation System

Whatever is done or not done by the federal government, state and local governments will still be the first responders to terrorist attacks, natural disasters, and other emergencies. The first calls for help will be answered by city police, airport police, port police, county sheriffs, state police, local fire services, emergency medical services, emergency managers, hazardous material workers, highway and transit workers, other employees of local government, and local representatives of railroads, trucking companies, pipeline operators, airlines and other private transportation providers.

However, a National League of Cities (NLC) survey of 465 cites following September 11th found that only 55 percent had terrorism readiness plans. (33) Undoubtedly, many new plans have been prepared in subsequent months and many old plans have been reviewed and updated. However, how many cities, counties, or states have effective, on-going planning processes that address transportation issues in depth and include meaningful involvement by transportation officials, public and private?

For events that target or stress the transportation system, once the first responders have the scene under control, the focus will shift to state and local transportation officials. Are workable plans in place? Can the needed resources, including people and equipment, be marshaled in a reasonable period of time? Are responsibilities clear?

As noted above, state and local governments have a wide range of experiences in responding to emergencies of all types. A 1999 report entitled "Improving Surface Transportation Security Through Research and Development," by the National Research Council (NRC) committee, recommended the following:

> (Security should be considered) as part of a broader picture, not a wholly new and different problem but one that is similar and closely connected to the transportation community's previous experience in responding to accidents, natural disasters, and hazardous materials. (34)

What may be lacking, however, is a "unified assessment" of all these experiences, and the related tools and techniques, to identify the collective best practices. (35) Which approaches are most likely to work in response to which circumstances? How can all of the transportation lessons from past disasters and emergencies be assimilated to advance the state-of the-art and the state-of-the practice for all major disasters, natural and manmade?

Incorporate Security in Transportation Planning, Design and Operations

State and local governments and private businesses are attempting to harden the existing transportation systems in a variety of ways. When the existing infrastructure was designed and built, security was not a primary concern. When existing operating procedures were developed, security was not a primary concern. Physical and procedural retrofits and adaptations have been necessary.

For the future, security should be a primary consideration in the planning and design of facilities and services and in the development and implementation of operating procedures. Transportation planners and engineers will need new planning and design guidelines and procedures. The modal administrations within the U.S. DOT and the various trade and professional organizations in the transportation industry will all have roles in developing the new guidelines and procedures.

State and local transportation officials will also have a role in developing the guidelines and procedures, but, more important, state and local transportation officials will make almost all of the decisions about whether security is actually incorporated in planning, design, and operations. Further, the success of the new guidelines and decisions-making processes will depend largely on whether state and local law enforcement, local fire services, emergency medical services, and other emergency responders have participated in the processes. In developing new guidelines and procedures, equal attention should be given to the processes for involving law enforcement and emergency response agencies in transportation planning, design and operations.

Accelerate Initiatives with Multiple Benefits

The National Research Council (NRC) committee report, cited above, advocated "the value of taking a *dual-use* approach, in which security objectives are furthered at the same time as other transportation goals." (36) The new emphasis on security seems to reinforce that notion.

Transportation projects that have a security benefit, even if the security benefits are secondary, should receive priority over projects without security benefits. Likewise, security projects that have other transportation benefits should receive priority over projects solely for security purpose. Of course, the choices may not be so obvious, but the new emphasis on security should move certain projects higher on the priority list, such as:

- ITS projects that enhance security as well as safety and help reduce traffic congestion
- Traffic incident management programs that improve the capabilities for dealing with major disruptions
- Law enforcement actions that would improve transportation security against terrorism as well as assaults, theft and other criminal activities directed against passengers and cargo
- Physical and operational improvements that would improve security and help reduce congestion, for highways, airports, railroads, seaports and other components of the transportation system

Also, efforts to combat cyber terrorism have to be mentioned. The potential for a cyber attack should not be overlooked in every aspect of the transportation system. FAA is certainly aware of the threats to the air traffic control system, and the IT professionals in every transportation business and public agency are aware of the damages that can be caused by viruses and hackers. ITS technologies are being deployed at a rapid rate by state and local transportation agencies, and protection of the ITS systems should be recognized as a particular vulnerability.

CLOSING

This paper raises far more questions than it answers. Hopefully, the questions are relevant and will contribute to constructive discussion of the emphasis on security and the implications for state and local transportation policy.

In the end, state and local transportation officials will sometimes have to choose between projects or programs that will improve security and those that will improve highway safety, reduce congestion, or accomplish other important goals. Few would argue that security warrants a higher priority than in the past, but more that more than 40,000 people are killed in highway crashes in the U.S. each year, including more than 5,000 pedestrians. (37) Congestion on the nations highways is costing billions of dollars each year, $78 billion just in the urban areas with over 100,000 population**.** (38) Congestion is also a growing problem for our airports, seaports, and railroads. Environmental protection, accessibility, and sustainability are still important. State and local transportation officials will have to sort through all of the competing priorities, considering all of the implications.

REFERENCES

(1) Thomas R. Dye, American Federalism: Cooperation Among Governments. *Lexington Books, D.C. Heath and Company: Lexington, Massachusetts/Toronto, 1990, 38*

(2) U.S. Department of Commerce, Economics and Statistics Administration, Bureau of the Census, *Government Organization*, *1997 Census of Governments, Volume 1*. GC97 (1)-1, August 1999, xiii
http://www.census.gov/prod/gc97/gc971-1.pdf

(3) John Magaw, named on January 28, 2002, as Under Secretary of Transportation for Security, served previously as a state trooper, Secret Service agent, Director of the Secret Service, and Director of the Bureau of Alcohol, Tobacco and Firearms *http://www.tsa.dot.gov/*

(4) John Magaw, "Statement before the Aviation Subcommittee, Committee on Transportation and Infrastructure, United States House of Representatives," January 23, 2002
http://www.house.gov/transportation/

(5) National Emergency Management Association, *Trends in State Terrorism Preparedness, Executive Summary,* December 2001
http://www.nemaweb.org/Trends_in_Terrorism_Preparedness/index.htm

(6) American Association of State Highway and Transportation Officials, Security and Emergency Response Survey of State Transportation Agencies *January 25, 2002, 5-8*
http://transportation.org/download/Security_Emergency.pdf

(7) Ibid.19-20

(8) President George W. Bush, "Securing the Homeland, Strengthening the Nation," 2002
http://www.whitehouse.gov/homeland/homeland_security_book.html

(9) National Governors Association, *Homeland Security: The Cost to States for Ensuring Public Health and Safety*, December 5, 2001, 1
http://www.nga.org/common/issueBriefDetailPrint/1,1434,2915,00.html

(10) U.S. Conference of Mayors**,** "Security Costs Climb for U.S. Citizens: Survey Finds Over $2.6 Billion in Additional Costs," February 4, 2002
http://www.usmayors.org/uscm/us_mayor_newspaper/documents/02_04_02/security_costs.asp

(11) U.S. Department of Transportation, "U.S. Department of Transportation Establishes Port Security Grants For Critical National Seaports," press release, DOT 17-02, February 28, 2002
http://www.tsa.dot.gov/

(12) Coalition to Insure Against Terrorism, Letter to Honorable Tom Daschle and Honorable Trent Lott, February 26 2002

http://www.nareit.com/governmentrelations/ciatsenateletter.pdf

(13) U.S. Census Bureau, Government Employment, March 2002, 1
http://www.census.gov/govs/apes/00emppub.pdf

(14) Ibid.

(15) Bureau of Labor Statistics, "Occupational Outlook Handbook, Emergency Medical Technicians and Paramedics," 2002
http://stats.bls.gov/oco/ocos101.htm

(16) Office of Homeland Security, Local Responders Facts 2002, undated
http://www.whitehouse.gov/homeland/

(17) Annual report to the President and Congress, Secretary of Defense William S. Cohen, 2001, Appendix C, Personnel Table C-1
www.defenselink.mil/execsec/adr2001/

(18) Jonathan D. Salant, Associated Press Writer, "Highway Workers Enlist in Terror War," Intelligent Transportation Society of America, December 20, 2001
http://www.itsa.org/ITSNEWS.NSF/a619bd3fc912d6f38525658d00073cd1/29a84ea1b595855f85256b28004b6bc6?OpenDocument

(19) Robert O'Harrow Jr. and Jonathan Krim, "National ID Card Gaining Support," *Washington Post*, December 17, 2001
http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A52300-2001Dec16&notFound=true

(20) U.S. House Committee on Transportation and Infrastructure,
U.S. Rep. Don Young, Chairman, "Transportation Official Outlines Plans For Secure Identification System For Transportation Workers," February 13, 2002
http://www.house.gov/transportation/press/press2002/release185.html

(21) John Caher, "New York Legislature Approves Sweeping Anti-Terrorism Package," *New York Law Journal*, September 18, 2001
http://www.law.com/cgibin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZGDPEYQRC&live=true&cst=1&pc=0&pa=0

(22) Council of State Governments, "Suggested State Legislation," 2002
http://ssl.csg.org/terrorism/masterterror.html

(23) Aircraft Owners and Pilots Association, "States Proposing Onerous Criminal Background Checks and Pilot IDs," February 26, 2002 http://www.aopa.org/whatsnew/newsitems/2002/02-1-096x.html

(24) Susy Phillips, The Trucker, "Teamsters and ATA Spar Over Background Checks, Transportation ID," *March 5, 2002*
http://www.thetrucker.com/stories/03_02/0305_id.html

Section 311.12, Florida Statutes

(25) By John Cheves, Lexington Herald-Leader, "Legislators Jump on Secrecy Bandwagon," Feb. 11, 2002
http://www.kentucky.com/mld/kentucky/news/2647141.htm

(26) James C. McKinley, "State Restricts Data from Internet in Attempt to Thwart Terrorists," *New York Times*, Feb. 25, 2002
http://query.nytimes.com/search/abstract?res=F50A10F93D550C758EDDAB0894DA404482

(27) U.S. Department of Transportation, National Pipeline Mapping System, "NPMS Access - Online Mapping and Data Download Changes,"
http://www.npms.rspa.dot.gov/data/npms_data_down.htm

(28) Mike Ahlers, "Container Security Proposals Kept Secret," CNN.Com/US, February 4, 2002
http://www.cnn.com/2002/US/02/04/gen.us.security.containers/index.html

(29) Aircraft Owners and Pilots Association, "Closed Maryland Airports Reopen Tomorrow Night," February 21, 2002
http://www.aopa.org/whatsnew/newsitems/2002/02-1-090x.html

(30) Nuclear Energy Institute, "Key Facts," September 1999
http://www.nei.org/doc.asp?Print=true&DocID=&CatNum2&CatID=58

(31) Federal Emergency Management Agency, "Terrorist Incident Planning Guidelines Published," May 21, 2001 *http://www.fema.gov/pte/pte052101.htm*

(32 Interagency Commission on Crime and Security in U.S. Seaports, *Report of the Interagency Commission on Crime and Security in U.S. Seaports*, Fall 2000
http://www.seaportcommission.gov/reports/icssrpt.pdf

(33) Scott Mayben, "On Alert," *Planning*, Vol. 67, No. 12, December, 2001, 13
(34) Committee on R&D Strategies to Improve Surface Transportation Security, National Materials Advisory Board, National Research Council, *Improving Surface Transportation Security: A Research and Development Strategy,* Washington, D.C.: National Academy Press, 1999, 44

(35) Ibid. 23

(36) Ibid. 1

(37) U.S. Department of Transportation, Bureau of Transportation Statistics, National Transportation Statistics 2000*, BTS01-01, Washington, D.C.: U.S. Government Printing Office, April 2001, Table 2-1*
http://www.bts.gov/btsprod/nts/Ch2_web/2-1.htm

(38) Texas Transportation Institute, "2001 Urban Mobility Study, The Short Report" http://mobility.tamu.edu/ums/study/short_report.stm