1-2008

Transportation Security Framework for a Medium-Sized City

Ryan Fries
Clemson University

Mashrur Chowdhury
Clemson University, mac@clemson.edu

Anne Dunning
Clemson University

Transportation Security Framework for a Medium-Sized City

Ryan Fries*, Mashrur Chowdhury** and Anne Dunning***
* Department of Planning and Landscape Architecture
Clemson University
Clemson, SC 29634
USA
tel: +1 864 656 3329
fax: +1 864 656 7519
e-mail: rfries@clemson.edu

** Department of Civil Engineering
Clemson University
Clemson, SC 29634
USA
tel: +1 864 656 3313
fax: +1 864 656 2670
e-mail: mac@clemson.edu

*** Department of Planning and Landscape Architecture
Clemson University
Clemson, SC 29634
USA
tel: +1 864 656 0151
fax: +1 864 656 7519
e-mail: anned@clemson.edu

EJTIR, **8**, no. 1 (2008), pp. 1-16

Received: June 2007
Accepted: January 2008

Terrorist attacks have made security preparedness unquestionably necessary in all cities. While major metropolitan areas have long recognized that their global visibility has required strong security operations, many medium-sized cities, specifically those of the U.S. and European Union, now face the need to establish transportation security frameworks for the first time. This paper assesses the resources available to help medium-sized cities begin the task of creating such systems. This assessment presents infrastructure risk assessment tools, identifies infrastructure and funding resources, and creates a process for developing a security framework to connect agencies responsible for transportation security in these

metropolitan areas. Descriptions of transportation security framework practices at the national level had led to the preparation of a transportation security framework for Greenville, South Carolina, USA, to serve as a prototype that other medium-sized cities can emulate. This security framework can serve as either a checklist to ensure security coverage in existing asset management systems and intelligent transportation systems architectures such as those frequently used in the U.S., Europe, and Japan, or it can provide baseline structure for developing a new transportation security framework for cities in developing countries.

Keywords: Transportation security frameworks, medium-sized cities, urban security, emergency planning

1. Introduction

Worldwide, terrorist attacks on transportation systems since 2000 have more than doubled compared to the 1990s. The attacks have further spread to smaller targets and smaller cities. In 2006, several terrorist attacks focused on medium-sized cities (considered here to have a population between 50,000 and 1,000,000) and included Chapel Hill, North Carolina; Kufa, Iraq; Dortmund and Koblenz, Germany; Kandar, Afghanistan; and Tiraspol, Moldova. All of these attacks focused on smaller targets using cars and car-bombs, suitcase-bombs, suicide bombers, and grenades, as weapons (U.S. Department of State, 2003).

The United States (U.S.) and other global leaders must adapt to the changing security environment involving medium-sized cities. Developing a security framework for existing and proposed transportation systems can aid in the development and coordination of security plans between many stakeholders and maintain the vitality of the transportation industry and therefore global commerce. Since the terrorist attacks of September 11th, 2001, the Transportation Security Administration in the U.S., has formed and allocated large amounts of money for shoring transportation infrastructure and systems against human threats, but this funding has not resulted in noticeable security improvements in all modes of transportation and for all areas of America. Although costly in delay and capital, airport security is receiving much attention to balance risks and costs. Because there is currently no other transportation mode that offers the same travel speeds, increased security procedures will not quickly compromise the airline industry's market share of the general population for long-distance routes. Public transit systems, however, do not have this luxury and must continue to offer easy access to maintain passenger ridership. Road infrastructure is similarly difficult to secure due to its massive network size. Unique security challenges also exist in rail and maritime shipping. Regardless of mode, transportation system designers and operators must broaden their focus from mobility and speed to include more security and safety (Okasaki, 2003).

Major metropolitan areas, such as New York City and Paris, have long recognized that global prominence makes them targets for terrorist attacks, but the threats of the War on Terror reach into the depths of countries. The September 11th terrorist attacks primarily targeted average citizens, and average cities also need to be prepared. Just as increased security on airlines preceded a shift of terrorism to surface modes, increased security in and around large cities since September 11th could shift some terrorist focus toward medium-sized cities. With the demonstrated targeting of transportation systems, agencies responsible for these systems

in populated areas of all sizes need to implement security measures and prepare for previously unimaginable events.

Although medium-sized cities have more limited resources to fight terrorism, they also have a smaller number of targets to protect and a relatively smaller number of stakeholders to coordinate. Establishing transportation security frameworks in these cities could save lives if universally adopted by all transportation-related agencies. Although local leaders in medium-sized cities might now approach the concept of transportation security frameworks for the first time, a number of resources already exist to launch such systems. Cities with asset management systems or intelligent transportation systems (ITS) architectures might turn to these resources to enhance security and expand coverage.

This paper assumes that significant risks to medium-sized cities justify security planning and adequate resources exist to develop security frameworks to mitigate these risks. The objectives of this paper are to:

1. present infrastructure risk assessment tools available for medium-sized cities,
2. identify infrastructure and funding resources available to medium-sized cities for addressing the risks, and
3. create a process for developing a security framework that applies available resources for mitigating risks.

The last objective, perhaps the most significant one, will be met by both discussion and the presentation of a case study of Greenville, South Carolina, U.S.

1.1 Infrastructure Risk Assessment Tools

Asset management programs are used in 75 percent of medium-sized U.S. cities (Wittwer et al., 2003) to maintain and best-manage their public infrastructure. Such programs will aid in the development and maintenance of a security framework because key public locations are already identified and monitored in some manner. Because security requires the proper selection of areas to protect, choosing high-risk locations for protection requires a careful selection process.

One strategy for the best allocation of funding in the protection of vital transportation facilities from terrorism considers the likelihood of the hazard occurring, the socio-economic importance of the facility, and the consequences of hazards (King et al., 2003). While this method was founded on intrinsic principles of natural hazard risk assessment, specifically earthquakes, the identification of key infrastructure is the same for human-made disasters as they share the same need for an objective assessment of risk.

Similarly, Hood et al. (2003) suggest identifying vulnerability through an integrated transportation analysis approach, considering vehicle, user, infrastructure, social setting, and environment as elements. While this approach seemingly requires a large amount of data, it provides exercises that stakeholders can use to identify these elements and their associated vulnerabilities or threats. This integrated transportation analysis approach was applied at the state level to New Mexico, but appears to readily apply to medium-sized cities.

Another framework for risk assessment focusing on highway sections uses both static and dynamic data. The static data can include infrastructure characteristics and the dynamic data can include traffic volumes and weather conditions. These factors are important because high-volume freeway links pose high risks for attacks and because weather, such as wind direction, might play a significant role during attacks using biological weapons or fire. The framework produces a risk score for each highway element based on the static data, dynamic

data, and terrorist attack potential. This risk score allows a systematic ranking of the highway elements or sections (Xia et al., 2005). Due to a heavy reliance on highways in medium-sized cities, this method is particularly applicable, but the technologies associated with modern transportation coordination require attention as well.

Another favoured risk assessment methodology focuses on traffic management centres (TMC) involved in real-time traffic monitoring. This risk assessment methodology includes asset identification, vulnerability assessment, threat assessment, consequence assessment, and countermeasure development (Rowshan et al., 2005). Many medium-sized cities operate TMCs to manage and control traffic in real-time to mitigate traffic congestion and to improve safety. As intelligent transportation systems (ITS) continue to gain momentum, the use of TMCs is likely to become more important for medium-sized cities.

The American Association of State Highway Transportation Officials' (AASHTO) *Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* (SAIC, 2002) also provides methods of risk assessment, weighing vulnerability against criticality, and suggests possible countermeasures, such as motion-activated video systems. This source also provides a quantitative method for ranking the importance of security needs.

Because each security situation is unique in scope and focus, all available methods should be examined to determine the best tool for a given job. Medium-sized cities with massive amounts of transportation infrastructure will likely encounter difficulty ranking their security needs and should review the methods presented by SAIC (2002) and Hood et al. (2003). Cities with less transportation infrastructure will not likely need such data-intensive procedures and might use a hybrid of several methods, for example, referring to Rowshan et al. (2005) when focusing on a traffic management centre and Hood et al. (2003) to guide table top exercises to identify and rank other security needs.

1.2 Infrastructure and Funding Resources

Currently, funding from the U.S. Department of Homeland Security (DHS) is distributed by state. Most states with only medium-sized cities receive no funding from the DHS Urban Areas Security Initiative (DHS, 2005). Many other grants in the U.S. are based on a formulas developed by the DHS. One formula weighs critical infrastructure, threat intelligence, and population density to distribute funding between states and/or cities. The formula aims at protecting the most people and the largest amount of vital infrastructure (DHS, 2005). Unfortunately, this formula favours larger metropolitan areas, leaving populations of medium-sized cities to fall another step behind larger metropolitan areas in protection. Non-traditional sources of funding that require further investigation, might include local gas taxes, city sales taxes or dedicated state revenue sources.

In the U.S., one contact person in each state receives funding from the DHS and bears responsibility for distributing that funding as equitably as possible to the variety of small, medium, and large cities unique to that state (DHS, 2007). While communication differences exist between states, perhaps a greater challenge exists in that the one contact person for each state must recognize and manage the security needs of cities of various sizes. Large cities typically receive focused attention; however, each city within a state should benefit from the needed communication with the DHS regardless of city size. The current organizational structure theoretically provides medium-sized cities with similar opportunities for communication with DHS as small and large cities have. Despite the equivalent communication possibilities, the practice of interaction reveals an important difference:

communication and coordination are more easily accomplished within medium cities than in large cities; however, funding and infrastructure assessment are less likely.

Since funding for large-scale security systems is not as likely for medium-sized cities as for larger ones, solidifying communication protocols is a more realistic outcome. Best practices in transportation recognize the importance of communication and coordination, and state-of-the-practice transportation systems have appeared throughout the U.S. and Europe with multimodal facilities and systems for passengers and freight. The coordination of systems creates efficiency and benefits for commerce, society, and the environment; however, as transportation system users share transportation links, security failures on any given link can have ramifications on a larger number of system users. Given that providing an interconnected system requires multiple agencies, these agencies must communicate and coordinate to ensure transportation security preparedness.

For example, current freight transportation systems are highly interconnected and cargo often travels on several different modes to reach its destination. The use of multiple trip segments can cause both mode transfers and security breeches, which can take two forms. First, if security is increased on one mode while another mode makes no changes, freight operators might change modes to avoid security delays. Conversely, a lack of security on one mode can threaten several others because the cargo might not be inspected upon mode change. Because medium-sized cities have less redundancy and mode choice, security incidents occurring on one mode might cause extensive disruptions, not only on other modes, but potentially on neighbouring cities that depend on the same transportation infrastructure. To prevent security breaches, a consistent quality of security between various modes and stakeholders must be maintained (Guerroro and Rabkin, 2004). This consistency is difficult to achieve because stakeholders have varying security interests, standards, and goals.

A transportation security framework can establish responsibility designations among stakeholders to help maintain consistent security preparations and divide security needs into smaller, more manageable projects. Development of a transportation security framework will also address conflicts between safety and security plans. For example, placing a label on the side of a tanker truck indicating flammable freight can improve safety for incident response personnel, but it degrades security by labelling a potential target (Guerroro and Rabkin, 2004). A transportation security framework emerges from agencies achieving agreement on policies such as whether or how to display a label for flammable freight.

As previously discussed, medium-sized cities have fewer responsible agencies than large cities which simplifies the amounts and types of communication and coordination that need to take place during and after security incidents. A simpler communication network requires less planning and fewer resources and results in a simpler, more adaptable, security framework. Because the security industry must constantly evolve to maintain its effectiveness, security plans and sometimes frameworks must adapt as well. Therefore; medium-sized cities have an adaptability advantage over large cities due to their less-complex frameworks.

2. Process for Developing a Security Framework

A security framework identifies the types of information that needs to be communicated between agencies before, during, and after an emergency. These agencies could include local and state police, fire departments, emergency management centres, traffic management

centres, and the media. This section first reviews previous security framework endeavours and then creates a simple process for developing a security framework. The latter will be presented in two parts, first explaining the process and then presenting a case study as an example.

2.1 State of Knowledge of Security Frameworks

Across the U.S., several agencies at varying levels of geography have formed a base of experience from which medium-sized cities can draw lessons. Although much of this experience has occurred at the state level, the principles demonstrated at this level can transfer to the regions around medium-sized cities. Key themes include the need for strong inter-organizational leadership, even partial security planning provides benefits, designating responsibilities and procedures is key, and sharing security information can provide multiple benefits.

In an effort to depict state security interdependencies, New Mexico's Security Task Force developed the Interdependent Systems Framework. This framework development showed the need for dynamic planning and inter-organizational leadership and action. Developing an effective security framework requires the cooperation of many organizations, both public and private, at many levels (Sobel et al., 2005). Since each organization might have unique opinions and objectives, this process is often challenging. While New Mexico's security framework included transportation infrastructure as one of many components, when focusing specifically on surface transportation security, the agencies involved will change, but the need for strong inter-organizational leadership remains.

During the emergency of September 11, 2001, Virginia's State-wide Transportation Emergency Operations Centre showed that a security framework, even with limited scope, can facilitate efficient coordinated responses. Although no complete security framework existed on that day, prior preparations for lesser emergencies included in the agency's integrated infrastructure security plan, albeit incremental, aided the agency's responses (Pearce, 2003). This case shows promise for developing such a framework in a medium-sized city. While a well-integrated security framework in medium-sized cities might require a phased approach to create due to the limited funding available, it could provide benefits prior to its completion.

California's standardized emergency management system (SEMS) brings to focus the importance of standardization in security frameworks. All state agencies in California are required to use this system, as it provides a standard of operation for any agency, event, or government level. SEMS development began to coordinate earthquake response and has evolved to meet current security needs. Transportation agencies in the San Francisco Bay area created their own transportation response plans that coordinated closely with the SEMS framework and designates responsibilities and procedures for reacting to emergencies in a coordinated manner (Okasaki, 2003). SEMS is akin to a security framework because it provides a communication coordination framework for any incident.

Major metropolitan areas have also demonstrated positive outcomes from the coordination and sharing of security information. Particularly, Boston, Massachusetts, began an aggressive surveillance coordination project in 2004, in reaction to security concerns for the upcoming Democratic National Convention. The project created the Massachusetts Interagency Video Information System, which manages video feeds from six different transportation agencies. While connecting these various agencies was a goal of the existing regional ITS architecture,

these security concerns reduced the completion time of this coordination to only three months with a cost of less than one million dollars. The system remains today to aid in the traffic monitoring, safety, and security of Boston (Bond et al., 2005).
Learning from these examples, several other U.S. states and metropolitan areas have developed security plans. Detroit, Michigan's, city security plan identifies ways to use existing technology to improve information coordination. Massachusetts' state-wide anti-terrorism response network was the first of its kind, proceeded by Arizona's state-wide security strategy (Beaconfire, 2005). The underlying theme in all of these plans is efficient and comprehensive communication; also the goal of a security framework.

2.2 Developing a Transportation Security Framework

Security plans must enable fast and coordinated reactions to prevent or limit the severity of future terrorist attacks and natural disasters. The individual security plans of various agencies must follow a city or regional framework to ensure the proper coordination and continuing interoperability. Such agency interaction is often difficult due to the varying interests and goals of public and private agencies in the transportation industry. Cities of all sizes present many potential transportation infrastructure targets to terrorists. Similarly, developing security plans to help protect cities brings many challenges. Creating a transportation security framework can simplify the process by focusing on responsible agencies, information communications between these agencies, and infrastructure components, such as tunnel ventilation systems and dynamic message signs. Providing the right information to the proper authorities and infrastructure elements can make the difference between repeating the mistakes of the past and preventing or managing disasters in the future.
In the U.S., a regional transportation security framework can coordinate with the "National Strategy for Homeland Security" in several areas. Transportation is listed as one of the thirteen critical infrastructure sectors in the Strategy, and allocating responsibility through a framework, meets the objective of assigning accountability in transportation security (Office of Homeland Security, 2005). Creating a transportation security framework will also promote initiatives of this strategy, including emergency preparedness and response, science and technology, and information sharing and systems (Office of Homeland Security, 2005).
This paper presents a process for creating a transportation security framework without an existing regional ITS architecture, but using the U.S. National ITS Architecture for guidance. A similar process can be followed in Europe by referencing both an applicable regional or national framework and the European ITS Framework. The transportation security framework can contribute to a regional ITS architecture by adding security subsystems, parts of larger ITS systems, not already included; and the regional architecture can contribute already implemented security subsystems to the new framework. Since the U.S. Department of Transportation mandates that any transportation project that includes a federally funded technology component, must follow or develop a regional ITS architecture, these architectures are becoming more common in medium-sized cities. While this mandate ensures interoperability with other technologies, it provides an important tool for building a transportation security framework.
As shown in figure 1, a security framework can be developed in the following steps: 1) identifying security risks, 2) selecting security services to mitigate risks, 3) developing a concept of operations, 4) developing an implementation plan, and 5) evaluating the security framework. This security framework can highlight the security-related subsystems and

interfaces from either the local, regional, or national ITS architecture. The U.S. National ITS Architecture addresses transportation security in the following areas: disaster response and evacuation, freight and commercial vehicle security, hazardous material security, wide-area alert, rail security, transit security, transportation infrastructure security, and traveller security (National ITS Architecture, Version 5.1). It also addresses how ITS needs to be secured from unauthorized use. Leveraging an ITS architecture provides useful information for developing the security framework. Standards related to communications or interfaces between security architecture entities must be identified to ensure interoperability between diverse agencies involved in security preparedness and response. Another important element of the security architecture is to identify the requirements for securing interconnects and information flows to prevent unauthorized use, so that the system that provides security is secured itself.

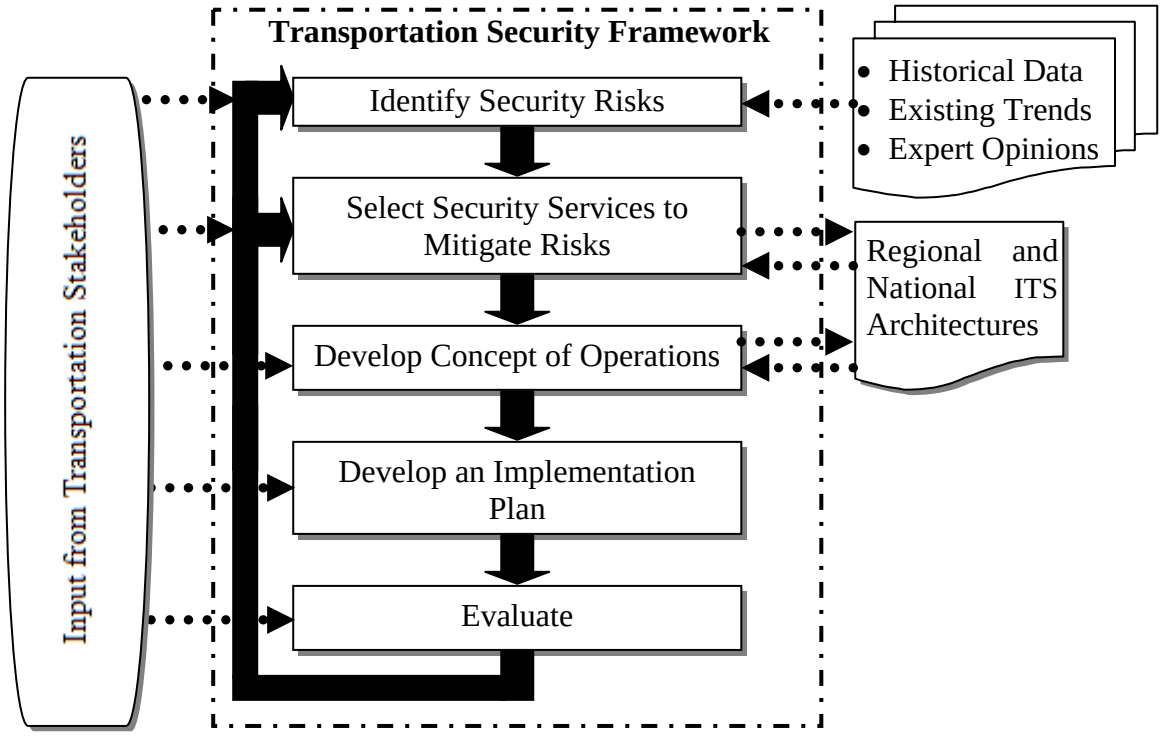

Figure 1. Process for developing a transportation security framework

Step 1: Identify Security Risks: This step includes an analysis of security risks to the regional transportation infrastructure and includes three parts. First, identify areas in the surface transportation network that are widely used by the public and are vulnerable to terrorist threats, such as transit services, tunnels, and bridges. Second, identify different threat scenarios that could lead to the failure of the selected. Last, rank the risks scenarios from most probable to least probable in terms of their likelihood to occur. Historical data, existing threats and expert opinions will be input to this step.

Step 2: Select Security Services to Mitigate Risks: This step will identify alternative security measures that will mitigate the security threats under each scenario. These security services can be selected from the market packages in the National ITS Architecture based on the services that are likely to improve transportation security, such as Transit Security and Evacuation and Re-entry Management. Some of the security related services already in a regional ITS architecture, if it exists, will provide input in selecting the security services. If a

regional ITS architecture does not exist at the time of selection the services, then the selected services could be used during its future development.
Step 3: Develop a Concept Operations: This step will identify the roles and responsibilities of each stakeholder in operating the security services. This includes identifying data requirements of each stakeholder (who will send what data) and communication mediums for security threat identification and response once an event has taken place. It is of particular importance to ensure the security of communication mediums for incident response as terrorists might also try to disrupt these actions.
Step 4: Develop Implementation Plan: This step includes developing a schedule and budget for deploying the selected services based on priority for regional security. This task should also include identifying possible funding sources for deploying the security services. Periodic deployment tracking should be conducted to evaluate the progress according the implementation plan and revise the implementation plan accordingly.
Step 5: Evaluation: Periodic evaluation will be performed to ensure that the system is keeping up with changing security risks, stakeholders, and technology. This task will influence the modification of the selection of security services.

2.3 Case Study of Greenville, South Carolina

This section of the paper uses Greenville, South Carolina, to illustrate how the process for building a regional security framework indicated in figure 1, can be used for developing a surface transportation security framework for any city. Greenville was chosen due to its proximity along a rail and freeway corridor between two larger cities, Charlotte, North Carolina, and Atlanta, Georgia, and the lack of security architecture. Therefore, a security incident in Greenville has the possibility to significantly disrupt the transportation systems in both Charlotte and Atlanta.
Greenville is a quickly growing medium-sized city with an international airport; a smaller, local airport; but lacks any port for shipping. Greenville provides an excellent role model for other medium-sized cities due to its reliance on trucking and rail, allowing the procedure presented here to be rather directly applied to other medium-sized cities with no access to large waterways.
Regional surface transportation security frameworks should coordinate externally with state and federal strategies for security. As discussed previously, many states have developed their own security plans. South Carolina does not have a state-wide emergency management system used by all agencies. Instead, each county develops its own including an office of emergency management, therefore; security plans are consistent within each county.

2.3.1 Framework Development

Step one, identifying security risks, was accomplished by an author interviewing personnel from several key agencies in Greenville including the district coordinator of the traffic management centre (TMC), the director of the Office of Emergency Management, the chief of a local fire department, and a captain in the city police department. The list of stakeholders was started scientifically by contacting agencies with known transportation security responsibilities, such as the TMC, and was then broadened to include additional stakeholders according to responses from interviewed agencies. For example, the TMC identified the names of railroad agencies operating in the area and they were added to the list of

stakeholders to interview. Each agency had different priorities for the future of transportation security; for example the city police were interested in recording video data to solve crimes, but the TMC was not interested because of the number of copy requests from crash victims they would need to satisfy with an already limited staff. The developed architecture needed to meet as many of these priorities as possible and the disparity found suggested the need for a future workshop involving all applicable stakeholders. While this workshop might identify additional differences, it can more importantly identify solutions, such as recording the data from only certain cameras, which would satisfy all or most stakeholders.

The next step was to select security services to the mitigate risks to Greenville's transportation infrastructure. The interviews with the key participating agencies provided information on the existing transportation security services and infrastructure in Greenville. Presently, the main security tool is closed circuit video. Two separate systems operated by the City Police and the TMC total over 125 cameras. These cameras monitor freeways, arterials, city streets, and parking garages. Other security infrastructure includes variable and dynamic message signs, portable surveillance cameras, and various communication systems.

Current security services include monitoring, detecting, and verifying traffic incidents, providing additional security for special events, and recording video from certain cameras for possible future review. In the future, more services are likely to be added. Realistic services in the next five years could include sharing all video feed to a central security location and expanding monitoring areas.

To aid in this step Turbo Architecture, a program developed for the U.S. Department of Transportation to make architecture development user friendly to transportation professionals (National, 2004), was used. The security services selected in this step are classified into market packages and are described in table 1. While there is great potential for future development in other subsystems beyond this five-year plan, this framework included existing and known-planned communication arrangements.

Step three**,** developing a concept of operations, identified the participating agencies in Greenville, their roles and responsibilities, and the transportation security framework needed to provide an information dissemination and communication mechanisms to facilitate reaction and recovery from emergencies that might impact the Greenville transportation system. The agencies identified and their respective roles and responsibilities, shown in table 2, demonstrate that linking only the transportation agencies in a medium-sized city involves much coordination, providing further justification for security frameworks to coordinate security operations.

Table 1. Market Packages Selected for Greenville, South Carolina

Market Packages Selected	Description
Network Surveillance	Includes surveillance equipment to monitor infrastructure and traffic conditions
Surface Street Control	Controls local and arterial signal systems to meet demands
Freeway Control	Includes ramp metering, dynamic speed limits, and incident detection
HOV Lane Management	Coordinates ramp meters and signals to improve HOV lanes
Traffic Information Dissemination	Provides pertinent travel information to motorists through variable message signs and highway advisory radios
Regional Traffic Control	Coordinates information sharing between traffic management centres
Traffic Incident Management System	Manages the detection and management of traffic incidents such as crashes, construction, and special events, such as sports
Weather Information Processing and Distribution	Used to detect conditions such as icy roads, high winds, and dense fog, to prevent crashes
Transit Vehicle Tracking	Monitors the location of transit vehicles to update arrival schedules
Transit Fixed-Route Operations	Aids operations management in scheduling and operator assignment
Demand Response Transit Operations	Aids operations management in routing, scheduling, and operator assignment for on-demand transit
Transit Security	Provides the physical security for transit passengers and operators
Transit Maintenance	Supports the scheduling of maintenance and service on transit vehicles
Multi-modal Coordination	Communication between different modes to enhance operation
Transit Traveler Information	Provides users with real-time information about timing of stops
Broadcast Traveler Information	Provides motorists with a source for all transportation information
HAZMAT Management	Combines commercial vehicle tracking and incident management
Emergency Call-Taking and Dispatch	Provides basic emergency call-taking, dispatching, and routing of emergency responders
Emergency Routing	Provides updated routing information in real-time
Transportation Infrastructure Protection	Includes the monitoring of transportation infrastructure and the barricading and protecting of infrastructure to prevent incidents
Wide-Area Alert	Uses traveller information systems to alert public about emergencies
Early Warning System	Monitors looming disasters such as approaching hurricanes
Disaster Response and Recovery	Enhances transportation response ability, supports coordination of emergency response, and identifies areas for integration
Evacuation and Reentry Management	Provides support during an evacuation and the subsequent return
Disaster Traveler Information	Uses all available means to provide disaster travel information including damage to transportation infrastructure and route changes

The next step in developing the concept of operations is to map the communications between each agency. Similar groups of participating agencies were grouped for simplicity. For example, all fire and rescue departments were combined as one because geography and type of security incident will determine which departments are contacted. Similar circumstances lead to combining all police, all railroads, and all health and medical services. These communications will most likely evolve according to future input from other organizations because not all agencies were available for input towards this framework development.

Table 2. Public Agencies and Responsibilities for Transportation Emergency Response in Greenville, South Carolina

Emergency Management	**Law Enforcement**	**Transportation Agencies**
Office of Emergency Management (OEM) • Receive info from the State Law Enforcement Division • Disseminate info to appropriate fire/rescue department • Disseminate info to appropriate police department • Disseminate info to Emergency Medical Services (EMS) • Serve as Greenville's first point of contact for security incidents • Disseminate info to the S.C. Department of Emergency Management (state-wide impacts)	*State Law Enforcement Division (SLED)* • Serve as South Carolina's first point of contact from the Department of Homeland Security • Disseminate info to regional counterterrorism councils (These are considered with in SLED for framework purposes) • Disseminate info to Greenville OEM (or any county) • Receive info from Greenville OEM (or any county)	*Traffic Management Center (TMC)* • Receive info from police departments • Participate in evacuation plan with incident detection and response • Traffic management • Disseminate traffic video to city traffic engineering department • Disseminate traffic video to web site
Fire and Rescue • Receive info from OEM • Receive incident info from EMS • Disseminate info to OEM • Disseminate info to EMS	*Greenville County Sheriff Dept* • Receive info from OEM • Disseminate info to OEM • Aid in evacuation traffic control • Provide Law enforcement during incidents	*Greenville Transit Authority (GTA)* • Support evacuation through vehicle dedication • Receive traffic info from TMC • Receive threat info from OEM • Disseminate incident info to TMC
Emergency Medical Services (EMS) • Receive emergency calls from citizens • Receive info from OEM • Disseminate info to appropriate Police Department • Disseminate info to appropriate Fire/Rescue • Disseminate info to OEM • Disseminate info to TMC	*State Highway Patrol (SHP)* • Receive info from OEM • Receive info from Transport Police • Disseminate info to OEM • Disseminate info to Transport Police • Aid in evacuation traffic control • Receive state-wide info from the S.C. Emergency Management Division	*Greenville Spartanburg International Airport (GSP)* • Receive threats from Transportation Security Administration (TSA) • Receive info from Greenville OEM • Operate separate police and fire departments • Disseminate info to OEM • Disseminate info to TSA
South Carolina Emergency Management Department • Receive info from OEM Greenville (large disasters)	*Greenville City Police* • Receive info from OEM • Disseminates info to OEM • Receive info from Greenville Fire/Rescue • Disseminate info to Greenville Fire/Rescue • Aid in evacuation traffic control • Provide law enforcement during incidents	*Norfolk Southern (Atlanta, GA and Roanoke, VA)* • Disseminate incident info to OEM *CSX (Jacksonville, Florida)* • Disseminate incident info to OEM *Amtrak* • Disseminate incident info to OEM *Greyhound* • Disseminate incident info to OEM *Carolina Piedmont Railroad* • Disseminate incident info to OEM *Pickens Railway Company* • Disseminate incident info to OEM
Health and Medical Services (all hospitals, clinics, etc) • Receive info from EMS • Receive info from OEM • Disseminate info to OEM • Disseminate info to EMS	*Transport Police* • Receive incident info from SHP • Disseminate info to SHP	*Greenville City Traffic Engineering* • Receive TMC live traffic image feed • Provide signal preemption to emergency vehicles • Provide signal priority to transit vehicles
Spartanburg County Office of Emergency Management • Receive info from Greenville EOC • Disseminate info to Greenville EOC		

Figure 2 shows an example of what information flows can exist between the Greenville Office of Emergency Management and the Greenville Traffic Management Centre. Note that while some information flows between both agencies, other information is being only received or sent, and this is because of the different data needs, capabilities, and resources of each agency. Although all the information flows between the agencies were developed in this project, this information will only be released to the appropriate agencies due to security concerns. Further, properly presenting the information flows requires a large plan-sheet detailing the types of data each stakeholder is responsible for transmitting and receiving. Building from this plan-sheet, transportation stakeholders develop or alter their own security plans to ensure that while their security plans change over time, they continue to provide the needed functionality to the region's transportation security framework.

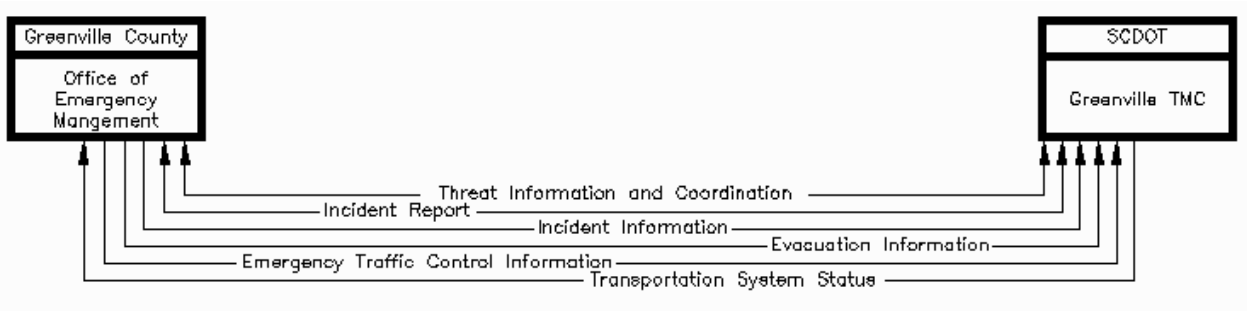

Figure 2. Information flow snapshot

The next step, implementation, outlined the specific projects to materialize the physical flow requirements identified in the earlier tasks. Specific projects based on the previous steps include the following:

- Link the Traffic Management Centre video surveillance systems to the City Police.
- Complete deployment of 800Mhz radios and create dedicated channels for agencies.
- Expand surveillance areas within the city and along the interstate.

These projects and others should be prioritized based on the input of participating agencies. Funding is expected to play a large role in the deployment schedule. South Carolina, a state containing no major metropolitan areas with population greater than 1,000,000, currently receives $26 million in annual funding from the Department of Homeland Security, which is approximately half of the national average for state funding. Further, South Carolina receives no funding under the Urban Area Security Initiative (Department, 2005). Greenville must actively pursue both traditional and non-traditional funding sources. South Carolina can likely make a more aggressive pursuit of federal funding through various Homeland Security administrations, such as the Office of Domestic Preparedness, the Federal Emergency Management Agency, and the Transportation Security Administration. State and local sources of funding require further investigation. Ideally, South Carolina should dedicate funding to the creation and management of security frameworks for the state's metropolitan areas; however, a line item in the general fund might stand as a required first step. Local funding will likely come through a similar process. In addition, as Greenville develops itself as a convention destination, requirements for event security might provide funding for Greenville's security much like the Democratic National Convention in 2004 did for Boston. Since this security framework has not yet been fully implemented, this example will not include the last step, evaluation.

2.3.2 Anticipated Use

Stakeholders in Greenville should continue this work by holding a stakeholder meeting and conducting tabletop exercises to identify further security needs. This process would need a strong champion to lead and organize this meeting and lead this initiative in the future, and the Greenville Office of Emergency Management would be an appropriate agency. The concept of operations should be reviewed in the meeting to ensure the proper communication and coordination among the stakeholders in the event of a security situation.

Stakeholders can discuss projects to improve transportation security in Greenville. Because the transportation security framework only protects one aspect of Greenville's security (transportation), stakeholders can further meld the framework to coincide with other existing security plans. This coincidence might include refining the information received and transmitted between the TMC and the City Police. The process can produce updated versions of figure 2 and table 2. This paper should serve as a tool for law makers and practitioners in Greenville and similar cities to coordinate transportation security either as a checklist for existing coordination of systems or as a baseline for developing new frameworks. Following the guidance of this paper and frequently refining frameworks with input from relevant agencies will provide an up-to-date information communication map. While maintaining a successful transportation security framework requires input from multiple agencies to update risk assessment models and track the deployment and impacts of projects, it will keep transportation security professionals informed of the precedence of security needs. Even though cost-benefit ratios have traditionally steered the selection of projects, the precedence found from a security framework can help decision makers more effectively order projects, while ensuring that each project continues to promote interoperability and communication.

3. Conclusion

Transportation security is now an important objective of transportation stakeholders, perhaps equivalent to safety and mobility. The increasing prevalence of terrorist attacks on less secured transportation targets now brings the security of medium-sized cities into focus.

This paper has presented infrastructure risk assessment tools, infrastructure and funding resources, and a process for developing a transportation security framework for a medium-sized city. This process was demonstrated through a case study of Greenville, South Carolina, U.S. While various tools exist to identify security risks and rank projects, working with participating agencies to develop this prototype project has demonstrated that the precedence of deployment frequently depends on the priorities and funding available to participating agencies. Furthermore, this process requires time to bring all stakeholders together to develop these priorities. As security is a major concern in cities worldwide, where transportation infrastructures at some point are the means for evacuating the population during disasters, the importance of having a framework for addressing these security issues related to transportation is of critical importance.

Medium sized cities in the U.S. and the European Union face particularly unique security challenges in deploying ultramodern transportation security systems. Though population size and existing infrastructure seemingly places these metropolitan areas at a disadvantage as compared to larger cities in terms of grant allocations (using U.S. federal funding formulas), they have several important advantages. First, their smaller size means that fewer

participating agencies must coordinate activities to protect a smaller transportation system; a smaller number of participants can typically make decisions and reach agreement more quickly than larger groups. Secondly, they can quickly adapt and incorporate a security framework into future updates of organizational security plans, which can ensure proper coordination and communication to prevent or manage transportation-related security incidents. Thirdly, since the vast majority of European cities are similar in scope and population to Greenville, lessons from this work easily transfer.

Future work should investigate the feasibility of non-traditional funding sources for medium-sized cities to implement security projects identified by a framework, which can ensure earlier realization of such projects. Further work should also identify how security frameworks differ for medium-sized cities with access to large multimodal facilities such as ports, making the findings of this work more broadly applicable.

References

Beaconfire Consulting (2005). A Homeland Security Plan. Available at: http://www.dlc.org/ndol_ci.cfm?kaid=139&subid=271&contentid=250723 (assessed July 2005).

Bond, R., Piel, C.-H. and Day, N. (2005). City-Wide Traffic Video Surveillance at the 2004 DNC in Boston: the Massachusetts Interagency Video Information System is a Success. Paper presented at the *84th Annual Meeting of the Transportation Research Board*, January, 2005, Washington, DC.

Department of Homeland Security (2007). State Contacts & Grant Award Information. Available at: http://www.dhs.gov/xgovt/grants/index.shtm (assessed October 2006).

Department of Homeland Security (2005). Press Room Press Releases. Available at: http://www.dhs.gov/dhspublic/display?content=4097 (assessed July 2005).

Department of Homeland Security (2004). Department of Homeland Security Grants FY05. Available at: http://www.dhs.gov/interweb/assetlibrary/Grants_SummaryStLocal.xls (assessed July 2005).

Guerroro, P.F. and Rabkin, N.J. (2004). Rail Security Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. Testimony before the committee on commerce, science, and transportation, U.S. Senate. Publication GAO-04-598T, United States General Accounting Office.

Kim, E. (1997). Optimal Demand for Road Investment. *The Korean J. Regional Science*, vol. 13, no. 2, pp. 75-92.

King, S.A., Adib, H.R., Drobny, J. and Buchanan, J. (2003). Earthquake and Terrorism Risk Assessment: Similarities and Differences. Presented at the *6th U.S. Conference and Workshop on Lifeline Earthquake Engineering*, August 2003, Long Beach, California, USA.

Miller, L. (2005). Report: 3,400 Air Violations Since 2001. Available at: http://homelandsecurity.osu.edu/focusareas/transportation.html (assessed July 2005).

Office of Homeland Security (2005). National Strategy for Homeland Security. Available at: http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf (assessed July 2005).

Okasaki, N.W. (2003). Improving Transportation Response and Security Following a Disaster. *ITE Journal*, vol. 70, no. 8, pp. 30-32.

National ITS Architecture Team (2004). Turbo Architecture Version 3.0. Prepared for the Federal Highway Administration, April 2004.

National ITS Architecture Development Team (2003). National ITS Architecture Security. Prepared for the Federal Highway Administration, October 2003.

Pearce, V.P. (2003). Surface Transportation Security Lessons Learned from 9/11. *ITE Journal*, vol. 72, no. 9, pp. 38-43.

Rowshan, S., Sauntry, W.C., Wood, T.M., Churchill, B. and Levine, S.R. (2005). Reducing Security Risk for Transportation Management Centers. Paper presented at the *84th Annual Meeting of the Transportation Research Board*, National Research Council, January 2005, Washington, DC.

Science Application International Corporation (SAIC) (2002). A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. Prepared for the American Association of State Highway and Transportation Officials Security Task Force.

Sobel, A.L., White, K.R., Hood, J.N. and Albright, D.P. (2005). An Interdependent System Framework: Development and Initial Application in the State of New Mexico. Paper presented at the *84th Annual Meeting of the Transportation Research*, January 2005, Washington, DC.

US Department of State. (2003). Significant Terrorist Incidents, 1961-2003: A Brief Chronology. Office of the Historian, Bureau of Public Affairs, US Department of State. Available at: http://www.state.gov/r/pa/ho/pubs/fs/5902.htm (assessed June 2007).

Wittwer, E., Bitter, J. and Kasprzak C. (2003). Asset Management and City Government. Paper presented at the *2003 Mid-Continent Transportation Research Symposium*, Ames, August 2003, Iowa.

Xia, J., Chen, M. and Liu, R. (2005). A Framework for Risk Assessment of Highway Network. Paper presented at the *84th Annual Meeting of the Transportation Research Board*, National Research Council, January, 2005. Washington, DC.