



SECURITY APPLICATIONS OF INTELLIGENT TRANSPORTATION SYSTEMS

Reflections on September 11 and Implications for New York State



**A Report to the Legislature by the NYU Wagner
Rudin Center for Transportation Policy and
Management, at the request of the NYS
Assembly Legislative Commission on Critical
Transportation Choices**

**Assemblyman Darryl Towns
Former Vice-Chair**

**Assemblyman Ruben Diaz, Jr.
Vice-Chair**

July 2002

Security Applications of Intelligent Transportation Systems

Reflections on September 11 and Implications for New York State

July 2002

Prepared by

Henry Peyrebrune, P.E., Visiting Scholar

Allison L. C. de Cerreño, Ph.D., Co-Director

Rudin Center for Transportation Policy and Management

New York University Robert F. Wagner Graduate School of Public Service

At the request of

Assemblyman Darryl Towns, former Vice Chair

Assemblyman Ruben Diaz, Jr., Vice Chair

NYS Assembly Legislative Commission on Critical Transportation Choices

Given the rapidly changing political and technological contexts within which Intelligent Transportation Systems continue to evolve, every effort was made to provide the most recent and accurate description possible of ITS efforts at the federal, state, and local levels. The Authors regret any errors or omissions.

EXECUTIVE SUMMARY

Prepared at the request of the New York State Assembly Legislative Commission on Critical Transportation Choices, and funded by an appropriation made available from the New York Department of Transportation's budget, the purpose of this report is to provide a review of Intelligent Transportation Systems (ITS) as they relate to New York State transportation programs and policy and to highlight policy concerns for further consideration by the State.

Information for this document was obtained primarily through an extensive literature search, including websites for various ITS-related governmental and private organizations. In addition, interviews were held with New York State Department of Transportation officials directly involved with ITS policy and applications. Finally, information was generated from ITS-NY's annual meeting,¹ and outreach to its individual members through a written survey.

Why Intelligent Transportation Systems are Important for New York

Defined as systems that apply "well-established technologies in communications, control, electronics, and computer hardware and software to improve surface transportation system performance," intelligent transportation systems hold much promise for reducing congestion, improving safety, and mitigating negative environmental impacts related to transportation. In some cases, ITS are already being utilized. For example, E-ZPass is already being used throughout the state and New York City has an Advanced Traveler Information System that allows people to view real-time traffic conditions via the internet.

The national and state-wide response to the attacks of September 11, 2002, was swift. A large number of activities have been launched and many improvements to homeland security have already been made. However, improved homeland security is a long-term process. The initial response can be characterized as one that engages all possible human resources available for homeland protection on a 24/7 basis with no expense spared. The increased presence of armed security forces and military forces at civilian facilities is evidence of this. Many of these personnel are working long hours, on overtime, a situation which cannot be sustained in the long term. While there will continue to be a need for security personnel in the long term, a national search is underway for technologies that can provide increased security with less manpower. Thus, the application of technologies (ITS) for homeland security is just starting, and their development will require monitoring over a long period of time.

¹ ITS-NY is an organization that was created to serve as a voice for New York State's ITS concerns at the local, state, regional and national levels.

Framework for the Report

To understand the role of ITS in transportation security, it is important to recognize the key components of ITS. Thus, Section I begins with some definitions and delineations of how ITS and security dovetail. Section II focuses on several activities related to homeland security and ITS at the federal level, while Section III looks more closely at New York's state and local agencies. Section IV provides a brief overview of a number of other initiatives around the country and by different associations and organizations related to transportation. Finally, Section V outlines some key policy considerations for New York State and makes some recommendations for further research and/or action.

Potential Issues for New York to Address

New York State agencies appear to be at the forefront of dealing with security issues as a result of a long history of planning for and dealing with major incidents, as well as their experience in dealing with the events of September 11, 2001. Nevertheless, there are several issues related to ITS and security that will need to be addressed to varying degrees in the coming months.

- 1. *Improved Communications/Enhanced Wireless 911.*** Communications has been described as the key to managing incidents. However, September 11 demonstrated that New York's systems are plagued by incompatibility and system overloads. Of further concern is the lack of "Enhanced Wireless 911" capability, which would allow automated number and location identification as well as selected routing for calls.
- 2. *Privacy and Availability of Public Information – Where are the Balance Points?*** There are a number of ITS that may be utilized to help identify and prevent threats. However, in some cases, there are concerns about infringement on privacy (e.g., systems that could collect data on a person's travel behavior). Further, there are also concerns about the extent of information that is made public regarding transportation systems. Where to draw the line in each of these cases will be a long-term source of debate, but shorter-term decisions may be required.
- 3. *Appropriate Methods for Monitoring and Gathering Information on Highway Systems.*** There are a variety of ways to gather information on transportation systems and traffic conditions. The use of remote sensing technologies, such as satellites or aerial surveillance, including Uninhabited Aerial Vehicles (UAV), is currently being tested, and some applications are proving feasible as image resolution increases and cost decreases. More study is needed to determine the feasibility and economics of instituting them in New York.
- 4. *Formal Monitoring of ITS Activities and Liaison with Congress.*** The Intelligent Transportation Caucus was recently formed by 22 members of Congress to educate and inform their colleagues

about the benefits of Intelligent Transportation systems. Among other items, the Caucus is focusing on ITS issues in conjunction with the reauthorization of federal transportation funding legislation (TEA-21), which expires in September 2003. Given the geographic size and population of New York State, as well as the complexities of the economic and political framework here, consideration might be given to establishing a similar caucus in the New York State Legislature.

5. ***Taking Advantage of Key Opportunities for Funding.*** Considerable sums of money will be expended at the federal level in developing and deploying ITS technology for homeland security. There are a number of opportunities for New York in these activities. For example, New York State agencies could offer New York sites as test-beds for deployment and New York State firms could aim to be leaders in research and development for new technologies, as well as in deployment of them.

TABLE OF CONTENTS

I. Introduction.....	1
Defining Intelligent Transportation Systems.....	1
Security Applications of Intelligent Transportation Systems.....	1
Some Caveats.....	4
II. Federal Activities Aimed at Utilizing ITS for Security.....	5
United States Department of Transportation (USDOT).....	5
Federal Highway Administration (FHWA).....	6
Federal Transit Administration & Federal Railroad Administration (FTA & FRA).....	6
Federal Motor Carrier Safety Administration (FMCSA).....	7
Research and Special Programs Administration (RSPA).....	7
United States Congress.....	7
III. New York State and Local Agency Responses to September 11, 2001.....	9
Metropolitan Transportation Authority (MTA)/New York City Transit (NYCT).....	9
State Executive Activity.....	11
New York State Department of Transportation (NYSDOT).....	11
Port Authority of New York & New Jersey (PANYNJ).....	12
New York City Department of Transportation (NYC DOT).....	12
IV. Security and ITS Activities Elsewhere Across the Nation.....	14
Organizational and Association Initiatives	15
American Association of State Highway Transportation Officials (AASHTO).....	15
ITS America.....	16
V. Policy Considerations.....	18
Potential Issues for New York to Address.....	18
References.....	22

I. Introduction

This study was prepared at the request of the New York State Assembly Legislative Commission on Critical Transportation Choices, and was funded by an appropriation made available from the New York Department of Transportation's budget. Its purpose is to provide an overview of intelligent transportation systems (ITS) as they relate to security in New York State in the aftermath of the terrorist attacks of September 11, 2001.

Defining Intelligent Transportation Systems

As defined by the United States Department of Transportation, Intelligent Transportation Systems (ITS) apply "well-established technologies in communications, control, electronics and computer hardware and software to improve surface transportation system performance."³ Central to most ITS activities are four categories of technologies:

1. **Sensing** – the ability to note the position and speed of vehicles using the infrastructure (e.g. rail lines, roadways, bridges, tunnels);
2. **Communicating** – the ability to send and receive information, between vehicles, between vehicles and infrastructure, and between infrastructure and centralized transportation operations and management centers;
3. **Computing** – the ability to process large amounts of data collected and communicated so that conclusions can be drawn and assessments made; and,
4. **Algorithms** – computer programs which process information gathered by ITS and develop operating strategies for transportation facilities.

Intelligent transportation systems are utilized to fulfill a number of objectives. They can help reduce congestion, improve personal safety, mitigate the environmental impacts of transportation systems, enhance energy performance, and improve productivity.

Security Applications of ITS

ITS have been implemented to varying degrees around the country for over a decade, but following September 11, there has been heightened interest in the security applications of ITS. How ITS can

³ U.S. Department of Transportation (USDOT), Federal Highway Administration (FHWA), *What We Have Learned from Intelligent Transportation Systems* (Washington, D.C.: December 2000).

contribute to national security objectives lies in the very technologies that are central to such systems. In terms of security applications, for example, sensing helps monitor systems and identify potential threats. Communicating is critical to security, both in terms of preventing incidents and effectively dealing with crises should they occur. Massive amounts of security information can be processed using computing, and algorithms can help detect patterns, and optimize solutions.

Security and transportation professionals who have been addressing the question of exactly how ITS can aid in security have clearly acknowledged the utility of these technologies for national and state efforts dealing with “the new realities following 9/11.” In fact, there are numerous examples of how current ITS systems mitigated the negative effects of the 9/11 attacks. Initial work has identified roles for ITS in: (1) the prevention of terrorist activities; and, (2) dealing with the aftermath of terrorist attacks.

Current thinking within the ITS profession on the use of ITS for security is perhaps best summarized by the following statements drawn from the *National Intelligent Systems Program Plan: A Ten-Year Vision*. With respect to preventing terrorist attacks, the report notes that:

While all terrorist attacks cannot be prevented, the technologies of Intelligent Transportation Systems can offer great promise for preventing attacks.⁴

If an attack should occur, the report points out that:

... many of the technologies and the communications networks being used today to better manage transportation systems can be utilized to assess the extent of damage and facilitate the movement of traffic for recovery, evacuation or quarantine.⁵

Beyond better surveillance on commercial and passenger vehicles (which may in itself help deter or prevent terrorist incidents) several transportation-related technologies, which could be also be utilized to prevent or deter terrorist attacks, are available, and in many cases already deployed. Among these are the following:⁶

- **Smart Card.** The size of a credit card, smart cards have embedded within them either a microprocessor and memory chip or a memory chip alone. While the latter only allows pre-defined operations to occur (e.g. a telephone calling card), the former allows manipulation of the data included on the card.

⁴ ITS America, *National Intelligent Transportation Systems Program Plan: A Ten-Year Vision* (Washington, D.C.: ITS America, January 2002), p. v. The report is online at [http://www.itsa.org/resources.nsf/Files/PPRA_Full_Final/\\$file/PRA_Full_Final.pdf](http://www.itsa.org/resources.nsf/Files/PPRA_Full_Final/$file/PRA_Full_Final.pdf).

⁵ Ibid.

⁶ ITS America, *National Intelligent Transportation Systems Program Plan*, p. v.

- **Biometrics.** This refers to technologies that help identify individuals based upon biological traits, including, for example, retinal/iris scanning, fingerprints, and face recognition.
- **Automatic Vehicle Identification.** Such technology identifies vehicles as they pass specific points without requiring any action by the driver.
- **Map Databases.** These databases may be utilized for a variety of purposes, including traffic and incident analyses.
- **Vehicle Classification Sensors.** As the phrase suggests, these sensors can automatically detect the class of a vehicle moving past them.
- **Weigh-in-Motion Technology.** This technology allows trucks to be weighed while moving at regular highway speeds. When trucks are over the weight limit, authorities are notified.
- **Spatial Geo-Location.** This helps identify specific locations of vehicles.

In addition, technologies exist that enable security personnel to detect the contents of vehicles, including hazardous substances, explosives, and drugs, without opening the vehicles firsthand. Also available are technologies that match a specific vehicle with a specific operator and specific cargo, preventing travel in the absence of a match. Finally, technologies to remotely control the starting and stopping of vehicles and engines are already utilized in many personal vehicles for comfort (e.g. turning on the engine to warm up the car before entering) and could easily be applied for security purposes as well.⁷ Such technologies have obvious applications in terms of preventing theft and hijackings.

Similarly, there are a number of technologies currently available that could aid in the aftermath of an attack by allowing the timely flow of information, increasing the flexibility of systems to accommodate emergency traffic, and decreasing emergency response times. Among these technologies are:⁸

- Automated Signal Systems
- Signal Priority Systems
- Moveable Lane Barriers
- Variable Message Signs
- Automated Incident Detection Systems⁹
- Mayday Systems
- Public Safety Response Systems

In all ITS operations, communication between and among various information systems, (e.g., between road conditions monitoring and traffic management centers or between different agencies responsible for transportation systems) as well as communication with the users of the system is critical to successful deployment. The same types of communication have been cited as critical components of improved homeland security systems. Thus, there is synergy between ITS and homeland security.

⁷ ITS America, *National Intelligent Transportation Systems Program Plan*, p. v.

⁸ Ibid. ITS America and USDOT are assembling resources to address the ITS' role in maintaining and ensuring surface transportation aspects of homeland security.

⁹ This technology is available, but not widely used, partly because false alarm rates are typically higher than with other methods.

Some Caveats

There are several important caveats that bear mentioning prior to continuing. First, while the national interest in transportation security is currently dominated by concerns over aviation, efforts to improve security utilizing ITS are underway in all modes of transportation. However, since ITS refer to surface transportation, this report will only deal with highways, transit, and motor carrier ITS and security activities.

Second, when dealing with national and state security, the question of how much information should be available in the public domain is always difficult to address. Indeed, at the January 2002 Transportation Research Board (TRB) Annual Meeting, John Magaw, who formerly led the Transportation Security Administration, stated that the United States must stop making public its intelligence and security measures. He cited the arrest of the infamous "shoe bomber" and the subsequent release of information on what security personnel are now being trained to recognize as suspicious behavior, including paying cash for tickets, no baggage, and multiple trips also paid in cash.

By making this information public, those whom the government is trying to deter also become aware of what to avoid. Mindful of these considerations, the information presented in this report comes from sources already made public, such as news reports, periodicals, websites, and publications, as well as from presentations made at the January TRB Annual Meeting in Washington, D.C. No attempt was made to interview officials involved in security matters. Obviously, some agencies are taking additional actions that are not being reported. State legislative committees and similar institutions might consider developing procedures to obtain more detailed information on such processes while not compromising public safety.

II. Federal Activities Aimed at Utilizing ITS for Security

There are a number of efforts currently underway at the federal, state, and local levels to improve transportation security. Many of these make use of ITS either directly or indirectly. For example, in a recent survey of bus transit security systems around the country, the following features were identified as already deployed or planned in several technologically advanced transit systems:

- Two-way radios with panic buttons
- Cell phones on board
- Onboard video surveillance
- Computer Aided Dispatch (CAD) with Automated Vehicle Locator (AVL)
- Cab enclosures (to isolate bus drivers)
- Destination signs with messages activated by panic buttons
- Police and security on board¹⁰

To a large degree, transportation security activities have been undertaken in response to the events of September 11, and in some cases they remain uncoordinated. Thus, before providing any assessment and recommendations on how best to utilize ITS for security in transportation, it is important to have an understanding of the breadth of initiatives already in place.

United States Department of Transportation (USDOT)¹¹

USDOT is involved in several ongoing initiatives at the Secretary and agency levels. Immediately following September 11, for example, Secretary Norman Y. Mineta created the National Infrastructure Security Committee (NISC) to “focus on intermodal transportation security issues in the “new” threat environment.”¹² The Committee brings together representatives from USDOT agencies and members of the business, industry, and labor communities to discuss maritime, pipeline, and hazardous materials concerns. The Committee coordinates with the Office of Homeland Security.

Also new at USDOT is the Transportation Security Administration (TSA), which was created within USDOT as a result of the Aviation & Transportation Security Act, which was signed into law on November 19, 2001. Its mission is to “protect the Nation's transportation systems to ensure freedom of movement for people and commerce.” Admiral James M. Loy has led the TSA since John Magaw's resignation on July 18, 2002.¹³ While the initial emphasis has been on improving security in the aviation industry, the TSA is responsible for all transportation modes.¹⁴

¹⁰ Darin Allan, “Cops, Cameras, and “Cages:” A Synthesis of Transit Bus Operator Security Methods and their Effectiveness,” Presentation made at the Transportation Research Board Annual Meeting, P02-5975 (Washington, DC: January 2001).

¹¹ Unless otherwise noted, the information presented throughout this section is drawn largely from individual agency presentations made at the January 2002 TRB Annual Meeting.

¹² U.S. Department of Transportation, “Remarks for the Honorable Norman Y. Mineta, Secretary of Transportation,” provided at the National Transportation Security Summit, (Washington, D.C., October 30, 2001), p. 3.

¹³ For more on the Transportation Security Administration, see their website at <http://www.tsa.dot.gov/>.

¹⁴ <http://www.tsa.dot.gov/>.

Complementing the Secretary's initiatives are a number of efforts being carried out by the various agencies within USDOT. Not surprisingly, several common themes have emerged:

- Support recovery efforts
- Undertake vulnerability assessments
- Gather intelligence
- Extend Public-private outreach
- Document best practices
- Strengthen incident management
- Determine how technology can strengthen security

Following is a brief description, by agency, of several key activities currently being pursued at USDOT.

Federal Highway Administration (FHWA). In conjunction with state departments of transportation, and in some cases the American Association of State Highway & Transportation Officials' (AASHTO) Task Force, FHWA is working on several strategies to increase transportation system redundancy and resilience. Among the planned goals and strategies are to:

- *Develop emergency plans, tools, and resources*, including documentation of alternative routes and procedures in case of an attack;
- *Perform vulnerability assessments* in multiple states;
- *Compile case studies on attacks*, including documentation of best practices and lessons learned from non-transportation agencies;
- *Conduct freight technology security demonstrations*;
- *Solicit ITS technology projects* intended to improve security; and
- *Host workshops* to discuss these and other related issues.

More importantly for the purposes of this report, FHWA proposed a list of homeland security-focused ITS projects under the Intelligent Transportation Systems Deployment Program as a means to generate some project specifically linking ITS and Homeland Security initiatives. Expecting to disburse approximately \$90M, USDOT issued the request for proposals in January 2002 and completed its reviews in April 2002, with recommendations for appropriations made thereafter.¹⁵ Whether or not the recommendations are adhered to remains to be seen.

Federal Transit Administration and Federal Railroad Administration (FTA and FRA). The FTA is conducting security assessments of commuter railroads along with the Federal Railroad Administration (FRA). For other transit systems, the FTA security program has 5 elements:

- *Security assessments.* A team has been assembled to assess the top 30 transit systems across the country.

¹⁵ U.S. Department of Transportation, Federal Highway Administration, "Memorandum" (January 2002). Also, personal communication with FHWA personnel on July 3, 2002.

- *Emergency plan refinement based on the assessments.*
- *Assistance and funding of emergency drills.*
- *Regional workshops/training.*
- *Technology development.* \$2M has been earmarked for technology research under The Transit Cooperative Research Program (TCRP).

Federal Motor Carrier Safety Administration (FMCSA). The FMCSA is working with relevant states on upgrading truck inspections at points of entry along the Mexican and Canadian borders, and on the handling of hazardous materials (hazmat). (The latter area is of great concern and there are requirements for background checks on drivers and placarding of contents.) With the help of the states, the FMCSA is also conducting security sensitive/vulnerability visits/checks of all carriers; assessing how technology can be used in security checks/background checks; and evaluating technology which can track the route of hazardous materials trucks and intervene if they stray from their intended course or come too close to a nuclear plant or military base.

Research and Special Programs Administration (RSPA). The Research and Special Programs Administration is responsible for several offices, including the Office of Emergency Transportation (which was activated on 9/11), the Office of Hazardous Materials Safety, the Office of Pipeline Safety, and the Volpe National Transportation Systems Center. The RSPA solicited ideas/white papers on how technology can help security. At the close of the solicitation period in November 2001, RSPA received over 600 responses.

United States Congress

The Executive and Legislative branches of the Federal government have also taken steps to improve homeland security, several of which are directly related to transportation security. As part of Public Law No. 107-38, signed by the President on September 18, 2001, Congress provided the first \$20B installment on a \$40B anti-terrorism supplemental package. The bill included \$3.5B for the Defense Department, \$8.2B for state recovery, and \$8.3B for Homeland Security. Included in the Homeland Security program were:

- \$100M for ferry operations between NY and NJ;
- \$100M to improve Amtrak owned tunnels under the East and Hudson rivers;
- \$100M to repair Port Authority transit facilities; and,
- \$75M for New York highways emergency relief for facilities damaged in the attack.¹⁶

¹⁶ The bill was initially sponsored by Representative C.W. Bill Young (R-Largo) from the 10th District of Florida. It was introduced in the House on September 14, 2001, as HR-2888, "2001 Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States," and became Public Law No. 107-38 with the President's signing four days later. For details, see www.house.gov/apps/list/pres/tx04_hall/patriot.html.

Congress and the White House also directed \$49M to the Washington, D.C. Metro system earlier this year. This funding will be used to purchase and install an array of high-tech security equipment to make it the most protected transit system in the country. Among the measures to be implemented are:

- *Bomb-sniffing dogs*
- *Intrusion detection alarms* for track beds, rail yards and bus garages
- *Computerized identification cards* that track employee movement around Metro facilities
- *Digital cameras* on all Metrobuses
- *Chemical sensors* in stations
- *GPS* for all buses
- *Development of a backup command center* in the event that the primary control center is inoperable

III. New York State and Local Agency Responses to September 11, 2001¹⁷

Prior to September 11, several state and local agencies around New York already had in place measures which proved efficient and effective for responding to the crisis on that day. For example, TRANSCOM,¹⁸ a consortium of 16 transportation and enforcement agencies in the New York/New Jersey/Connecticut Tri-State region, used ITS, including previously deployed variable message signs, to re-route traffic around Manhattan during the crisis. The resources of the I-95 Coalition membership,¹⁹ including variable message signs and highway advisory radio systems throughout the northeast, were also used to keep travelers away from New York City. Cars equipped with electronic toll tags were used as anonymous traffic probes, providing real-time information on traffic flows outside affected areas.

Similarly, geographic information systems (GIS) already in place, with information easily accessible via the Internet, allowed for real-time decision-making on the day of the attacks. GIS technologies also helped in the immediate recovery efforts as officials gathered all the available information in a central GIS database so they could quickly create critical maps (e.g. modeling the collapse, plumes of contaminants, traffic patterns, utilities, power grids, telephone coverage). In fact, over 5,000 maps were produced in this process. Among the lessons learned:

- Map production capability must be quickly established;
- Storage of data should be centralized;
- Standardized map products should be selected;
- Map request processes need to be automated; and,
- Products can be shared quickly and efficiently via email/Internet.

Specific state and local agency responses to the terrorist attacks are summarized in the following paragraphs.

Metropolitan Transportation Authority (MTA)/ MTA New York City Transit (NYCT). The MTA was able to act quickly on September 11 because of its decentralized decision-making process. Initially, NYCT shut down the entire system, and then selectively started portions as possible or as needed. Sixty thousand passengers were in the subways at the time of the attack, along with 300 NYCT personnel, but there were no fatalities among them. Three thousand five hundred transit personnel and multiple pieces of equipment, including 300 buses, were quickly dispatched to transport victims and firefighters, and to deliver emergency generators, creating a two-mile convoy at one point. After

¹⁷ Unless otherwise noted, the information presented throughout this section is drawn largely from individual agency presentations made at the January 2002 TRB Annual Meeting.

¹⁸ TRANSCOM acts as an information clearinghouse, alerting public and private organizations of traffic incidents, coordinating construction schedules, and undertaking research and demonstration projects for the benefit of the region.

¹⁹ Begun informally by a group of transportation professionals who were interested in overcoming barriers to institutional cooperation, the I-95 Coalition became a formal entity in 1993, after the USDOT labeled the area of I-95 between Virginia and Maine a priority corridor. The Coalition today is a regional partnership of major public and private transportation agencies, toll authorities and industry associations.

the initial crisis, the MTA used automated scheduling and created a new subway map daily on the Internet. Their website received over 7 million hits each day.

MTA officials credited annual drills with other emergency agencies for the quick and decisive reaction to the emergency. Among the lessons that MTA officials cited as having learned from their agency's involvement in the 9/11 attacks:

- Continually updating emergency plans is critical.
- Inter-agency drills are crucial and should be performed at least 4 times each year.
- Effective communications are essential, both internally and externally.

Since 9/11, the MTA has outlined a number of steps that the agency is taking to improve security, including direct measures that will help on a daily basis as well as broader measures for thinking about the best ways to maintain and improve security in the long-term. These measures, many of which directly incorporate ITS, include the following:

- *Increased vigilance in terms of who has access to MTA properties.* This will be accomplished through a variety of methods, such as the introduction of photo identification; inspection of vehicles/trucks entering property; inspection of bags and packages; the installation of Jersey barriers around facilities; utilization of X-ray equipment for deliveries; the blocking of vehicle entrances; locked non-public areas; installation of intrusion and access controls; and the development of strategies for dealing with trash receptacles. More rigorous background checks will also be performed on contractor employees.
- *Improved sharing of information.* This measure has two components: (1) sharing best practices to expand the knowledge base of how to deal with security and develop or refine evacuation plans; and, (2) sharing actual information specific to a crisis or intelligence gathering. There are many means for improving the knowledge base related to security measures. Among the methods being discussed are symposia with other transportation properties (MTA officials visited Paris and London, which they found to be helpful). In terms of sharing information, mechanisms are being explored to provide information to employees in real time on what is happening during a crisis; and to gather and share intelligence with other agencies.
- *Improved training.* Foremost among the methods here are drills and simulations, which were credited for the ability of different agencies to communicate during the 9/11 crisis. This practice will be continued and expanded as necessary. There is discussion of training employees to act as the "eyes and ears" of the institution, and training is also expected on more specific topics, including dealing with nuclear, chemical, or biological attacks. Finally,

there is an interest in extending the “training” in a more informal way to the public so as to encourage them to report suspicious or unusual activities.

- *Utilization of new/improved technologies.* The technologies being discussed include chemical sensors and various types of protective equipment. Also, there is discussion of scanning the Internet on a regular basis for information (in one case, someone was found selling drawings and uniforms).

State Executive Activity. In response to the attacks on September 11, Governor George Pataki created the Office of Public Security on October 10, 2001. Directed by John Scanlon and James Kallstrom, “the Office is charged with coordinating and enhancing anti-terrorist efforts in the State of New York, specifically with developing a comprehensive statewide strategy to detect, protect against, respond to, and prevent cowardly and murderous acts of violence.”²⁰ The Office is the primary contact point with the federal Office of Homeland Security

New York State Department of Transportation (NYSDOT). In the days immediately following September 11, NYSDOT provided a daily New York City Metro Area transportation report which provided emergency closures and traffic updates on all modes of transportation for affected areas. Their initial response was described as a multifaceted campaign aimed at helping safeguard transportation system assets and the public. According to a November 2001 report, “a system-wide vulnerability assessment is underway as well as an extensive internal audit of information technology security. On the roadways the number of truck inspections being done per day has nearly doubled and special attention is being given to inspections conducted near the border crossings.”²¹

Ongoing is NYSDOT’s Integrated Incident Management System (IIMS) project, a real time incident management system that will enhance the communication of incident data among incident managers at operations centers and incident response personnel at incident scenes. Veridian, a New York State firm, is the key system supplier. The project was begun in New York City and involves the following agencies: New York City Department of Transportation, New York State Department of Transportation, NYC Police Department, NYC Fire Department/EMS, the Mayor’s Office of Emergency Management, NYC Department of Environmental Protection, NYC Department of Sanitation, and the MTA NYC Transit. Current deployment involves nine NYC Police Department and three NYC DOT Emergency Response vehicles.²² (A total of 25 vehicles are planned.) Each vehicle collects digital information (text/image) and shares the information with multiple centers

²⁰ <http://www.state.ny.us/security/>.

²¹ See USDOT, FHWA, *Focus* (Washington, D.C., Nov 2001), <http://www.tfhr.gov/focus/nov01/nineoneone.htm>.

²² NYS DOT, “New York MOVES: ITS Program Status Report,” June 2002, p. 12.

(transportation, police, fire/EMS, environmental protection, public works, emergency management) and the corresponding agencies that respond to and manage incidents.

Port Authority of New York and New Jersey (PANYNJ). At the headquarters level, the Port Authority has also been dealing with a variety of issues with respect to developing new strategies and implementing increased security procedures. Officials have noted that they see a role for technology in vehicle and cargo inspection, and in the expansion of E-ZPASS and chemical detection measures, especially. Highlights of their overall security efforts to date include the following:

- For the past 10 months PANYNJ personnel have been heavily involved in dealing with security, leading to a great deal of overtime. They continue to investigate how technology can help substitute for personnel over the long term.
- PANYNJ has implemented enforced commercial vehicle inspection on all facilities.
- Commercial vehicles remain restricted on the upper deck of George Washington Bridge; ITS helps with message signs and other communications devices.
- There is increased deployment of PANYNJ police supported by State, National Guard and local law enforcement.
- An Office of Operations and Emergency Management has been created.
- By reallocating internal funds, priority has been reassigned to security issues in the PANYNJ capital plan.

Within the Tunnels, Bridges and Terminals Division (TB&T), PANYNJ created a Manager of TB&T Security; developed facility security plans after conducting facility threat assessments; and added private security forces.

New York City Department of Transportation (NYCDOT). NYCDOT has a Transportation Management Center (TMC) in Long Island City with an active Incident Management Program, in coordination with the City Police and New York State DOT, which are co-located in the same building. NYCDOT is concerned with some of the longer-term implications of policies enacted in response to the emergency. While the control of transportation systems and restorations is currently with the City Office of Emergency Management, some of the long-term policy issues with which they are grappling include:

- Single occupancy vehicle (SOV) bans
- The role of waterborne travel
- Plans for rebuilding Lower Manhattan
- Maintenance of inter-agency coordination

As various transportation agencies around New York State seek to implement programs and projects to meet their identified objectives, there will be a number of challenges. For example, the TB&T at the Port Authority believes the agency faces the following challenges to further improve security:

- Establishing a real and perceived safe network
- Restoring customer confidence
- Maximizing mobility
- Building on inter-agency cooperation/relationships
- Dealing with uncertainty

These challenges, of course, exist within a framework of additional obstacles related to politics and economics. For example, there is concern across agencies as to how to best apply security measures in an open society. What will be the trade-offs involved, and will the public be willing to accept them? Also, increased security often has a negative effect in terms of restricting mobility, which has societal and economic implications. Finally, there are costs associated with increasing security. How will that be paid for, and by whom?

IV. Security and ITS Activities Elsewhere Across the Nation

In the wake of September 11, several state departments of transportation raised some key questions which warrant further discussion. Among these are:

- ***How should agencies design for a terrorist attack?*** States have modified bridge and road designs for natural disasters such as earthquakes. Are there design modifications that can minimize the impact of a terrorist attack? Some RFP's are out from states dealing with this issue.
- ***How much security of existing infrastructure is enough?*** Added security brings with it added costs. It is important to determine the appropriate balance.
- ***How can the partnering and coordination that is critical for homeland security be improved and expanded?*** In addition to existing cooperative efforts that already exist, there is need for connections among agencies whose interagency dealings previously were limited, such as between state DOTs and federal law-enforcers.
- ***When multiple agencies or locations are involved, who should be responsible for key decisions in times of crisis?*** It is important, for example, to have a clear delineation of which agencies have the authority to close roads and redirect traffic, especially when emergencies affect more than one locale.
- ***What is the best way to train maintenance workers and other agency employees so they can be the first line of security "eyes" in the field?***

Many state and local agencies are not waiting for these questions to be formally addressed. Like the initiatives in New York that were described in the previous section, state and local measures are being implemented across the country. For example, Texas, Virginia, and California are each conducting vulnerability assessments of critical bridges. The general process involves:

- Identification of all bridges, along with application of criteria to determine vulnerability/criticality, and selection of a limited number of bridges for vulnerability analysis;
- Performance of vulnerability analyses;
- Limitation of facility access;
- Implementation of measures for deterrence and surveillance (technology includes motion sensors and surveillance cameras); and,

- Creation of response plans in case of an incident.

The cost estimate in California was \$1-\$4M per facility for the 16 most vulnerable and important bridges.

Organizational and Association Initiatives

Many organizations and associations representing transportation interests have initiated research and/or information sharing activities. The following is a list of these organizations and a brief description of their activities. (Additional information and periodic updating of activities can be found on each organization's website.)

American Association for State & Highway Transportation Officials (AASHTO). AASHTO has created a Task Force on Transportation Security to review security and emergency preparedness related to bridges, tunnels and other facilities critical to the transportation system and national defense. The Task Force will address three areas: (1) Physical features of highways; (2) Information systems that are used to manage traffic systems; and, (3) Commercial vehicle operations on the highway system. Short term, top priority items include development of a federal legislative agenda; the creation of a vulnerability assessment handbook; development of a set of state DOT case studies related to September 11; and the creation of a secure website and clearinghouse for information.

In addition, AASHTO surveyed all state DOTs to determine their research and contract support needs. The responses from 49 states identified the following possible focus topics:

- Development of guidelines for maintenance workers;
- Use of training courses and regional forums for emergency response and vulnerability assessment;
- Creation/Identification of website linkups for assorted association and agency efforts on security;
- Distribution/Creation of communications guidelines for public safety and systems to aid in transportation interoperability;
- Design guidelines for rehabilitation of existing or construction of new infrastructure, taking security into account;
- Development of model state laws on privacy of security related data; and,²³
- National assessment of infrastructure and operating costs needed for the security of the nation's roadways, tunnels and bridges.

²³ For more information see AASHTO's website at www.AASHTO.org.

ITS America has formed an ITS Homeland Security Task Force, with the purpose of assessing the role of current and future intelligent transportation system technologies. The organization identifies the following current technologies as having security and disaster response applications:²⁴

- *Automated Vehicle Location Systems (AVL)* that track vehicle/freight movement and delivery. The transportation of hazardous material, for example, can be closely monitored. Many transit agencies also utilize AVL in conjunction with on-board cameras;
- *Advanced Traffic Management Systems* to monitor, control, and speed the flow of traffic;
- *Universal Transponders on Commercial Vehicles* that track vehicles as they pass through electronic weigh stations;
- *License Plate-reading Technologies*, which are already deployed at borders, parking facilities and certain domestic checkpoints;
- *Wireless Enhanced 911* which can provide automatic location information; and,
- *Real-time Interoperable Communications Links* between transportation and public safety agencies.

ITS identifies the tracking of hazardous materials as an important area for action. A national system for hazardous materials tracking would involve advance filing of shipping plans, tracking of materials, and coordination with law enforcement for interdiction if a shipment is hijacked. ITS America also submitted a White Paper which outlines the ITS industry's long-term vision for an Integrated Network of Transportation Information which will provide for seamless travel for people and goods; critical infrastructure protection and crises management; seamless freight movement; and road weather information.

A number of other organizations have also created security-related task forces or committees. Among them, **The National Association of Counties (NACO)** has created a task force on homeland security which will provide a direct link between counties and federal agencies, especially the Office of Homeland Security in the White House. The mission of the task force is to determine how counties and the association can help the federal government and how NACO can assist counties with security issues.²⁵

The Transportation Research Board (TRB) has a Committee on Critical Transportation Infrastructure Protection which is also sponsoring a website on security resources.²⁶ Similarly, **The New York Public Transit Association (NYPTA)**²⁷ formed a Safety and Security Committee to discuss steps taken by public transit systems to improve and ensure the safety and security of passengers and drivers. The Committee will investigate new technologies and systems available; serve as a mechanism to share

²⁴ ITS America, *Press Release* (Washington, D.C., 19 October 2001).

²⁵ *Emergency Preparedness News* 26, 1 (1 January 2002): pages?

²⁶ See <http://san-antonio.tamu.edu/trba5021/Members/members.html> for information about the Committee. Also see the website they maintain for information on security at <http://www4.trb.org/trb/homepage.nsf/web/security>.

²⁷ Formed in 1983 by representatives of the transit industry, NYPTA is a nonprofit association of public and private transportation service providers, private sector manufacturers and consultants, and state government agencies. See <http://www.nytransit.org>.

information among transit agencies; and make recommendations to NYPTA and NYSDOT on safety and security issues.

Some organizations have created websites, including **The American Public Transportation Association (APTA)**, which offers a site with current information on transit security issues. Research efforts and/or workshops are being conducted by various institutions, including the Norman Y. Mineta International Institute for Surface Transportation Policy Studies (MTI),²⁸ and **The Association of American Geographers**, which has initiated a two-part research effort. The first part involves an assessment of the utility of geographic dimensions in emergency planning. The second part of the effort will be a pilot study on the use of geographic technology in dealing with terrorism and post terrorist disaster rescue relief efforts. The **Palisades Group USA** has been holding a monthly National Teleconference Series on Counter-Terrorism in Public Transit.²⁹ After September 11, a group of leading design and construction industry leaders and several federal agencies came together to create **The Infrastructure Security Partnership (TISP)** which is focusing on security in design and construction.³⁰ Finally, the **Intelligent Transportation Society-NY (ITSNY)** is surveying their membership on ideas for using ITS to improve security. Several member firms are already working at the national level. ITSNY co-sponsored two Conferences on ITS and Public Safety in Syracuse on March 13 and 14.

Though this list is by no means exhaustive, it does provide a sample of the many activities that exist around the nation.

²⁸ MTI was created by Congress through the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA) and established in the California State University system at the San José State University College of Business. Its homepage is <http://transweb.sjsu.edu/index.asp>. Also see <http://www.transweb.sjsu.edu/rpd9805a.htm> for information on one of the projects.

²⁹ See <http://www.palisadesgroup.com/PGUSA/NationalTeleconferences.htm> for a list of sessions.

³⁰ <http://www.tisp.org/>.

V. Policy Considerations

The national and State-wide response to the attacks of September 11, 2002 was swift. A large number of activities have been launched and many improvements to homeland security have already been made. However, improved homeland security is a long-term process. The initial response can be characterized as one that engages all possible human resources available for homeland protection on an around-the-clock basis with no expense spared. The increased presence of armed security forces and military forces at civilian facilities is evidence of this. Many of these personnel are working long hours, on overtime, a situation which cannot be sustained in the long term. While there will continue to be a need for security personnel, a national search is underway for technologies that can provide increased security with less manpower. Thus, the application of technologies (ITS) for homeland security is just beginning, and their development will require monitoring over a long period of time.

Potential Issues for New York to Address

New York State agencies appear to be at the forefront of dealing with security issues as a result of a long history of planning for and dealing with major incidents, as well as their experience in dealing with the events of September 11, 2001. Nevertheless, there are several issues related to ITS and security that will need to be addressed to varying degrees in the coming months.

1. Improved Communications/Enhanced Wireless 911. Communications has been described as the key to managing incidents. There are stories of failures in the communications systems in New York during the terrorist attacks due to incompatibility and system overloads. Some specific issues cited were:

- The use of different technologies by wireless message carriers, requiring different frequency bands, which restricts customers' ability to easily transmit text messages or attachments to a person whose phone is serviced by a different carrier;
- Insufficient wireless network capacity; and,
- The lack of interoperability, including, for example, the existence of frequency incompatibilities with two-way radios.

These difficulties are not unique to the New York metropolitan region. Indeed, a recent assessment by the Public Safety Wireless Network program (PSWN) found that only Michigan and Delaware have what would be considered mature integrated public safety systems.³¹

Of further concern is the lack of "Enhanced Wireless 911" capability. Most wire line phones in the United States now have enhanced service, which means they have automated number identification, automated location identification, and selective routing when dialing 911. Though more than 50% of

³¹ Jim McKay, "Reconciling the Differences," *Government Technology* (October 2001). An

911 calls are now made from wireless phones, enhanced service is not available. Recognizing the importance of establishing the same level of emergency service for wireless phones that exists for wire lines, the FCC is requiring wireless providers to make enhanced wireless 911 service available in phases. The process was to begin October 1, 2001, but implementation of this system has been delayed for technical and institutional reasons.

At this point, the State of Rhode Island will be the first state to have enhanced wireless 911. There is activity in New York State to implement enhanced wireless 911. Indeed, the process for implementing enhanced wireless 911 has a long history with the Executive and the Legislature. Ongoing issues include funding responsibility, surcharge revenues, routing, technology, training, caller rights, and education. What is new in recent years is the inclusion of the ITS community, the tie-in to incident management and also the direct involvement of the medical community which sees enhanced communications as a benefit to earlier and more informed treatment.

The Emergency Call Locator Partnership, a partnership between the Department of Emergency Medicine at Upstate Medical University in Syracuse, and the National Highway Traffic Safety Administration, has developed an implementation template for enhanced wireless 911 for New York to, "develop and deploy the infrastructure needed to maximize the effectiveness of wireless 911 emergency communications across New York."³² Numerous stakeholders have been involved, including: fire, police and EMS administrators; telecommunications and traffic safety engineers; elected officials; emergency care providers; Public Safety Answering Point (PSAP) administrators; and telephone and wireless communications providers.³³ On March 14, the Partnership's stakeholders convened a conference in Syracuse. After two years of discussion, the Partnership is planning to make available a New York State Wireless Enhanced 911 Implementation Guide. Participating organizations will sign on to the document to demonstrate solidarity in implementing an enhanced wireless 911 system in New York as soon as possible.

Also discussed on March 14 was the proposed implementation of a statewide wireless radio network (SWN) by the NYS Office for Technology (OFT). According to their website:

OFT intends to develop and deploy an integrated public safety, public service land mobile radio communications network for use by state, federal and local governmental entities which operate within the State's borders. The digital network will use trunking technology to provide a spectrum-efficient, statewide mobile radio communications network that will allow interoperability between all participants and interface with other legacy systems as necessary.³⁴

³² <http://www.upstate.edu/cellular911/>

³³ In particular, the Fire Association of the State of NY, the Department of Criminal Justice Services, the NYS Wireless Carriers Coalition, the NYS Department of Health EMS Bureau, and various legislative and technology experts were involved from the beginning of the process. For more information on this partnership, see <http://www.upstate.edu/cellular911/about.shtml>.

³⁴ <http://www.oft.state.ny.us/index.htm>.

There was a consensus on the need for such a network, and many participants voiced their concerns that existing radio communications systems are out-of date and need replacing.

It is important to keep in mind that with respect to identifying location, the current FCC requirement for enhanced wireless 911 is an ability to gauge position based solely on longitude and latitude. However, following September 11, there has also been pressure on the Federal Communications Commission to require police and telecommunications carriers to implement technologies that will aid in locating wireless transmissions inside large structures, including subway stations, office buildings and schools. Further, the Federal government is speeding up a priority cellular network for emergency and national security personnel. (There is already a priority system for landline communications called the Government Emergency Telecommunications Service which was used on 9/11 and performed well.)

2. ***Privacy and the Availability of Public Information – Where are the Balance Points?*** A recent article by Peter Huber and Mark Mills in *City Journal* on how technology can be used to prevent terrorism discusses the various methods of threat recognition including, for example, imaging systems, transponders, and pattern-recognition software. According to the authors, the issue of collecting information about people to prevent terrorist activities versus public privacy will be a public policy issue over the long term. Similarly, where to draw the line in terms of public access to information regarding the nation's transportation and security systems. Providing too much information publicly may make them more vulnerable, but how one prevents this in an open society is not a question that is easily answered.
3. ***Appropriate Methods for Monitoring and Gathering Information on Highway Systems.*** There are a variety of ways to gather information on transportation systems and traffic conditions. One method commonly used is visual reconnaissance, e.g. traffic helicopters. However, these were not allowed to fly following 9/11 and have only been selectively allowed to resume service. Wiring the transportation system with sensors, video surveillance, fiber optics etc. is effective but very costly. Only 5% of the nation's major highways have such systems in place. The use of remote sensing technologies, such as satellites or aerial surveillance, including Uninhabited Aerial vehicles (UAV), is currently being tested, and some applications are proving feasible as photo resolution increases and cost decreases. More study is needed to determine the feasibility and economics of instituting them in New York.
4. ***Formal Monitoring of ITS Activities and Liaison with Congress.*** The Intelligent Transportation Caucus was recently formed by 22 members of Congress to educate and inform their colleagues

about the benefits of Intelligent Transportation systems. There is one member from New York on the Caucus: Anthony Weiner (D-NY9).³⁵

One of the early meetings of the Caucus focused on the use of ITS in response to the events of 9/11. Among other items, the Caucus is focusing on ITS issues in conjunction with the reauthorization of federal transportation funding legislation (TEA-21), which expires in September 2003. The Caucus held a hearing on the ITS aspects of the reauthorization of TEA-21. (ITS America hosted the ITS Caucus kick-off reception and technology demonstration on March 6, 2002.)

Given the geographic size and population of New York State, as well as the complexities of the economic and political framework here, it might be worthwhile to establish a similar caucus in the New York State Legislature. The Caucus could monitor state activities; liaise with Congress and New York Congressional Caucus members; monitor and provide input for federal legislation (there are a number of bills before Congress that deal with Homeland Security and provide federal funding to states and local governments); and liaise with New York State industries involved in ITS.

5. ***Taking Advantage of Key Opportunities for Funding.*** As a result of decreased federal gasoline and other transportation user fees, federal funds for transportation are projected to decline significantly during the next round of reauthorization (up to 25% is possible). Nevertheless, it is clear from reviewing the activities at the national level that considerable sums of money will be expended in developing and deploying ITS technology for homeland security, which will present a number of opportunities for New York. For example, New York academic research institutions could aim to be leaders in research and development for new technologies; firms throughout the State could bring to market new technologies as well as existing technologies for which use has shifted; and State agencies could offer New York sites as test-beds for deployment.

³⁵ Prior to his 2002 electoral defeat, Felix Grucci, Jr. (R-NY1) was also on the Caucus.

References

- Allan, Darin. "Cops, Cameras and Cages; Synthesis of Transit Bus Operator Security Methods and Their Effectiveness. Presentation at the Transportation Research Board Annual Meeting, Washington, D.C.: January 2001.
- Apogee Associates. *ITS National Investment and Market Analysis*. Report prepared for ITS America and the United States Department of Transportation. Washington. D.C.: ITS America, 1997.
- Briggs, Valerie, and Keith Jasper. *Organizing for Regional Transportation Operations: Houston TranStar Case Study*. McLean, VA: Booz-Allen & Hamilton, August 2001.
- _____. *Organizing for Regional Transportation Operations: San Francisco Bay Area Case Study*. McLean, VA: Booz-Allen & Hamilton, August 2001.
- _____. *Organizing for Regional Transportation Operations: Vancouver TransLink*. McLean, VA: Booz-Allen & Hamilton, August 2001.
- Emergency Preparedness News* 26, 1 (January 1, 2002).
- Huber, Peter, and Mark P. Mills. "How Technology Will Defeat Terrorism." *City Journal* 12, 1 (Winter 2002): 24-33.
- Intelligent Transportation Society of America. *National Intelligent Transportation Systems Program Plan: A Ten-Year Vision*. Washington D.C.: ITS, January 2002.
- _____. "News from the TRB Annual Meeting." *News*. (15 January 2002). www.itsa.org.
- _____. *Press Release*. (19 October 2001).
- Konheim, Carolyn S. "Intelligent Transportation Systems in the New York Region: An Overview." *ITS-NY Newsletter* (Winter 1998/99).
- McKay, Jim. "Reconciling the Differences" *Government Technology* (October 2001).
- Peyrebrune, Henry. *Technology: A Bridge to the States*. Washington, D.C.: Public Technology Incorporated, 1996.
- New York State Department of Transportation. *Brochure on ITS in New York*. Albany: NYSDOT, Summer 2001.
- Public Technology Incorporated. *How Can We Work Together? A Guidebook to Smart Response through Coordinating Local Public Safety and Transportation Information and Technology*. Washington D.C.: PTI, February 2001.
- Rudin Center for Transportation Policy and Management, New York University. *Large City Technical Exchange and Assistance Program: Final Report on Inter-jurisdictional Coordination for Traffic Management, Interagency Fiber Optic Sharing, Planning for Pedestrians in Large Urban Centers*. New York City: Rudin Center, November 2000.
- United States Department of Transportation. Federal Highway Administration. "September 11 and Beyond: Highway Agencies Respond to Keep America Mobile and Secure." *Focus Newsletter*. Washington, D.C.: USDOT, Nov 2001.
- _____. *ITS Resource Guide*. Washington, D.C.: 2001.

_____. *What Have We Learned From Intelligent Transportation Systems*. Washington D.C.:
December 2000.

_____. United States Senate. *Statement before the Committee on Environment and Public Works,
Subcommittee on Transportation, Infrastructure and Nuclear Safety*, by Christine Johnson.
Washington, D.C. (September 10, 2001).