



America's Travel Information Number

Deployment Assistance Report #3: 511 and Homeland Security



June 2002



Published by the 511 Deployment Coalition

Table of Contents

- I. Introduction1
- II. Context for Homeland Security4
- III. Customer Issues8
- IV. Institutional/Organizational Issues 10
- V. System Performance Issues 12
- VI. Conclusions..... 15
- VII. Acknowledgements..... 17

I. Introduction

Purpose of White Paper

Prior to September 11, the U.S. homeland had been mostly spared from terrorist attacks. Today, transportation agencies are beginning to address the need for threat and vulnerability assessments, and re-examine how existing emergency management plans will be implemented during a homeland security emergency or alert. Travel information is an important component of emergency management, and the telephone is one of many delivery mechanisms. As 511 systems become more widely deployed, it is reasonable to ask—what role should 511 systems play during homeland security emergencies and alerts, and what are the organizational, technical, cost, and other impacts of doing so?

This White Paper discusses the challenges and opportunities for 511 systems, their designers, and their operators, arising from the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon. Neither location had a 511 system, but relevant lessons were learned. While it does not provide the solutions, this White Paper highlights the issues and suggests related guidelines, for consideration by the 511 Deployment Coalition Policy Group at its meeting on February 26, 2002.

The 511 Deployment Coalition Working Group established the 511 and Homeland Security Task Force at its December 2001 meeting, with the purpose of developing a White Paper to examine both the role 511 can play in assisting in homeland security efforts and the impact that homeland security preparedness could have on 511 services. This White Paper is the result of that initiative. The volunteer Task Force members are listed in section 7.

Linkage between 511 and Homeland Security

It is important to acknowledge the existing relationships between the transportation and emergency management communities with regard to major incident response. These relationships formed the basis for the responses to the September 11 attacks. Among the many stories of human tragedy and heroism on September 11, transportation agency staff guided hundreds of thousands of travelers to safety in the minutes and hours following the attacks. Given the disruption caused by the attacks, this effort continued for days and weeks. Providing accurate, timely information to travelers was critical to safety and mobility, not just in the New York and Washington D.C. regions but also throughout the eastern seaboard.

How can 511 support emergency management?

Under ‘normal’ conditions there are multiple media for dissemination of information to travelers. However, on September 11, the need for a rapid exodus on foot from the affected areas precluded the options to use the Internet, television, or even radio. For many, cell phones became the primary means of communication in the hours following the attacks. Just as transportation agencies responded to that need, it is apparent that had a 511 system been available it too would have contributed to support emergency management and evacuation.

Today there are a handful of 511 systems across the nation. As the number of systems multiplies in the years ahead, familiarity with 511 as the telephone number for travel information may become as commonplace as 911 is today for emergencies. People from a city, region, or state with 511 systems may not hesitate to dial 511 for travel information when traveling on business or visiting unfamiliar locations, including for homeland security emergencies.

Are there homeland security considerations for 511 systems?

While a homeland security emergency has many parallels to a major incident in terms of detection, response, and recovery, there are differences as well. Perhaps the most troubling is the combination of:

- The potential for large numbers of people to be the target of an attack, or to be impacted by its immediate aftermath, creating a spike in demand for travel information, or related news;
- Transportation infrastructure may be the target of an attack, e.g. bridges or railway stations, or be indirectly impacted, e.g. closure of surface streets due to exclusion zones around sensitive buildings or facilities, highlighting the need for accurate travel information in a dynamically changing environment;
- Communications infrastructure may be the target of an attack, e.g. communications hubs, or be indirectly impacted, e.g. collateral damage to fiber optic cables, highlighting the need for communications network redundancy;
- An attack could occur at any time, with or without warning, when available response resources are insufficient;
- The nature of an attack could be outside the envelope of knowledge and experience of transportation operations staff, e.g. weapons of mass destruction, delaying an accurate assessment of need and appropriate response; and,
- An attack could comprise multiple primary and secondary events over a short period of time, designed to create confusion and lure emergency responders and civilians into a 'trap', and again highlighting the need for accurate travel information in a dynamically changing environment.

This combination of circumstances leads to challenges for a broad spectrum of emergency responders, law enforcement, and transportation agencies. This in turn will impact how travel information is gathered and disseminated. Where 511 systems exist or are planned, it appears prudent that their designers and operators take account of such challenges.

A recurring theme throughout the White Paper is that many issues apply to traveler information systems in general, of which 511 systems are but one delivery medium.

Overview of White Paper content

This White Paper continues with a more detailed description of the context for homeland security, and how agencies and organizations are responding. Issues are identified and addressed in three sections—customers, institutional/organizational, and system performance. The White Paper discusses each issue and proposes guidelines and actions.

- A proposed guideline represents specific advice to 511 system designers and operators, to be incorporated into the next version of the 511 Implementation Guidelines.

- A proposed action represents an area for further discussion or research by the 511 community at large that needs to be undertaken prior to the development of proposed guidelines for 511 system designers and operators.

The White Paper concludes with a summary of the challenges and opportunities, and recommendations for moving forward.

II. Context for Homeland Security

Trends in Terrorism

The U.S. Department of State reports nearly 140 significant terrorist attacks worldwide since 1961. While many of these attacks have been against U.S. interests, prior to September 11 just three of these attacks were on the homeland: World Trade Center (1993), Oklahoma City (1995), and Empire State Building sniper attack (1997). Research by the Mineta Transportation Institute on terrorist attacks and serious crime involving public surface transportation systems indicates that worldwide there have been an average of 5 significant attacks per month during the 1990s. None of these were on the U.S. homeland. Research by the Federal Transit Administration (FTA) indicates that 58% of international terrorist attacks in 1998 were on transportation targets, and of these 92% were on surface transportation.

While there are many lessons that transportation agencies may learn from these attacks, the relatively small number of attacks on the U.S. homeland leaves 511 system designers and operators with a dilemma. On the one hand, there is a heightened sense of awareness of threats and vulnerabilities. On the other hand, there is little in the way of hard data to influence 511 system design and operation. This is perhaps understandable, given the relatively short period of time since September 11, 2001 and the immediate concern for critical infrastructure protection and emergency preparedness. Nonetheless, it is appropriate for the 511 Deployment Coalition to provide some initial guidance to designers and operators, and to continue to review the emerging homeland security situation.

It is not the intent of this White Paper to conduct a detailed review of the events of September 11 or to address the potential for, or nature of, any future terrorist attacks on the U.S. homeland. Of relevance to this paper, and the subject of the remainder of this section, are how transportation system operators responded on September 11, initiatives and actions of various national organizations, and the missions and actions of new federal players.

Overview of transportation system operators' responses

The Federal Highway Administration (FHWA) has commissioned case studies to document the actions taken by transportation agencies in response to the terrorist attacks on the World Trade Center and the Pentagon. Two additional case studies will document the actions taken by transportation agencies in response to a rail tunnel fire on July 18, 2001 in Baltimore, and the Northridge earthquake on January 17, 1994. These case studies were not available at the time of publication of this report. In addition to FHWA's case studies, AASHTO has commissioned its own case studies for the terrorist attacks on the World Trade Center and the Pentagon.

While none of the above case studies explicitly addressed traveler information, all touched on it to varying extents given their general focus on transportation agency response. To the extent possible, draft products have been reviewed, and relevant findings have been incorporated into this White Paper.

FHWA, in conjunction with AASHTO, is currently undertaking a series of emergency transportation operations preparedness and response workshops. FTA, in conjunction with the Federal Railroad Administration and American of Public Transportation Association, is developing a series of emergency preparedness and security forums.

Initiatives and activities of national organizations

Transportation system security is not a new issue, although there is no doubt it has come into sharper focus since September 11. In 1998 TRB established a Task Force on Critical Infrastructure Protection in Transportation, with a mission to raise awareness among all TRB committees of the importance of critical infrastructure protection and to promote the inclusion of critical infrastructure protection in the mission of TRB committees. At TRB's 81st Annual Meeting in Washington D.C. in January 2002, there were more than 30 sessions that addressed critical infrastructure protection or transportation security.

Several national organizations have developed a focus on homeland security. AASHTO has established a transportation security task force, which has initiated the case studies referred to above, as well as vulnerability assessment guidelines and an emergency response handbook. AASHTO has undertaken a joint survey (with TRB) to assess the transportation security concerns of state DOTs, and their research needs in the field of emergency preparedness and transportation security.

In addition, both ITS America and the Institute of Transportation Engineers have taken homeland security initiatives.

New Federal players

President Bush's budget for fiscal year 2003 proposes substantial increases in areas that require immediate attention to secure the U.S. homeland: enhancing first responder programs, securing America's borders, combating bio-terrorism, strengthening intelligence sharing, improving transportation security and supporting other national defense related initiatives. While it is too early to determine whether this budget will result in any new funding for travel information initiatives, it is likely that the roles of two new federal 'players' will impact the linkage between 511 and homeland security.

Office of Homeland Security

The mission of the Office of Homeland Security will be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The Office will coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. The Office is expected to play a role in developing a National Threat Alert System, which will provide a consistent process with which federal, state, and local agencies, and private sector entities will be able to prepare for and respond to the threat of terrorist attacks. When in place, such a system may be of potential importance to 511 systems.

Transportation Security Administration

The Aviation and Transportation Security Act created the Transportation Security Administration (TSA). The TSA is charged with security for all the modes of transportation. Currently, the TSA has a focus on aviation mandates but recognizes the security needs of other transportation modes. Across every mode, the TSA will develop measures to increase the protection of critical transportation assets, addressing freight as well as passenger transportation. The TSA plans to maintain a commitment to relentlessly measure performance, building a security regime that provides both world-class security, and world-class customer service, to the American people.

United States Secret Service

While not a new agency, the United States Secret Service, under the U.S. Department of the Treasury, is the lead agency for designing, planning and implementing security for National Special Security Events (NSSE). The Secret Service has had that role since August 1999, when the 2002 Salt Lake City Winter Olympics were named a NSSE, the first Olympics so designated. Previously, the U.S. Secret Service performed the lead security role at the 2000 U.N. Millennium Summit in New York City, the 2001 Presidential Inaugural in Washington, D.C., and the 2002 Superbowl. Given the importance of transportation to security, and the potential impact of security measures on transportation, the Secret Service can be considered not just as a new player in the transportation community, but one with formidable authority.

Potential demand patterns for travel information during emergencies

Any spike in demand for travel information will likely be a function of many factors, including the type of homeland security emergency or alert, location, time of day and day of week, maturity of local traveler information systems (including 511 systems), and maturity of traveler information systems in general (including 511 systems). Perhaps one of the most immediate lessons that can be learned from September 11 is how the demand for travel information changed during the attacks and in the following days and weeks. As 511 systems do not currently exist in either the New York or Washington D.C. regions, existing telephone and web site usage provide the best proxy.

New Jersey Transit's transit information center, which normally receives approximately 8,400 calls per day, received over 16,000 calls on September 12. The Metropolitan Transportation Authority's website, which normally gets 200,000 hits per day, received 10 million hits per day in the week following the attacks.

The SmarTraveler service in the Washington D.C. region publishes calls taken and website hits on a monthly basis, making meaningful comparisons difficult at this time. However, calls taken for the month of September are considered to be somewhat low, possibly indicative of overload issues. Website hits were up by approximately 100,000 to slightly in excess of 500,000. As a general observation, SmarTraveler operated with high levels of demand on its system, requiring staff to work longer hours and additional staff to be added on September 11.

TRANSCOM, which collects and disseminates real time incident information to over 100 member agencies and affiliates in the NY, NJ, and CT region, does not provide travel information to the public. However, on September 11 staff took calls requesting travel information, an indication both of the heightened need for travel information and the difficulty obtaining such information.

Clearly, evidence is mixed as to the true pattern of demand for travel information on September 11. An alternate proxy that has been explored is the demand for travel information related to extreme weather events in North Carolina. In September 1999, Hurricane Floyd closed over 1500 roads in the eastern third of the state. This generated 160,000 phone calls to the toll free DOT Customer Service line over a 2 week period. Normal call volume is 1,500 calls per week. Call volume dropped significantly when the DOT posted this information on its website. In January 2002, 94 of the state's 100 counties received significant snow (more than 12 inches in the Raleigh area). This generated nearly 400,000 website hits in 2 days where normal volume is 2,000 hits per day.

Understanding the likely demand for travel information during a homeland security emergency is a fundamental input to system design and operation.

III. Customer Issues

Message content

Issue: Travel conditions may be so disrupted by the emergency that other menu options will lead to information that is not accurate, timely, nor reliable. In addition, the 511 system may be experiencing huge spikes in demand.

Proposed Guideline: The Implementation Guidelines (version 1.1) suggest that during major emergencies, an emergency interrupt message may be provided prior to, or in place of, the normal initial greeting. Under these circumstances, callers will be provided with immediate information related to the emergency without having to navigate any menus. In order to meet unusual levels of demand, this may be the only message that callers hear before the call is automatically terminated. Depending on the details of the proposed National Threat Alert System, it may be appropriate, e.g. at intermediate levels of threat alert, to implement a combination of an emergency interrupt message with limited navigation of menus.

Accuracy, timeliness, and reliability of travel information

Issue: Travel conditions during the early stages of a homeland security emergency may be very dynamic, and it may be difficult to continuously collect data that will result in accurate, timely, and reliable travel information. Following the attack on the Pentagon, there were numerous instances of media dissemination of false information regarding threats, impending attacks, or actual attacks on sites across the Washington D.C. region. It is not known whether these were malicious hoaxes or misunderstandings, but they highlighted the challenge of collecting accurate, timely, and reliable information. The likely involvement of law enforcement and security services may lead to actions, e.g. exclusion zones, with no warning or advice, that may blindside 511 system operators.

Proposed Guideline: 511 system operators must consider what additional sources of information they may need to access, how they will validate the information they receive, and the frequency of posting updates.

Issue: While there was no evidence of this on September 11, there have been numerous examples of “hacked” computer systems and web sites. “Cyber-terrorism” may be an emerging form of homeland security emergency, either as a primary attack, or as part of a secondary attack designed to compromise response. In either case, this may lead to the collection and/or dissemination of inaccurate travel information.

Proposed Guideline: 511 system designers and operators should take all possible precautions to protect data and telephony systems from cyber-terrorism, and develop recovery plans in the event that data is corrupted.

Focus of travel information

Issue: Travel conditions during the early stages of a homeland security emergency may be very dynamic, and it may be necessary to provide travel information with content that is more regional or multi-modal in nature than is normally the case. During the emergency, normal travel options may be unavailable, meaning people may need very basic and specific information on alternative travel options.

Proposed Guideline: 511 system operators must consider the broader impacts of the emergency on travel options. This may require wider coordination with other agencies to determine “safe” escape routes to locations where travel options are less disrupted, and a thorough interpretation of available options including alternative means, e.g. ferry, walking. This, in turn, may require 511 system operators to have a regional and multi-modal knowledge of transportation systems in their area.

IV. Institutional/Organizational Issues

Public and private sector roles and responsibilities

Issue: While many traveler information systems are entirely public service operations, some are partnerships between the public and private sectors, and others are purely private sector enterprises. While public agencies may provide some data, the private sector partners generally undertake the processing and dissemination functions. If the private sector partners are responsible for operating a system, they may become the primary source of travel information during a homeland security emergency. However the private sector partners may not be best positioned to provide accurate, timely, and reliable travel information if they do not have immediate access to data specific to the emergency that is collected by the public sector. Conversely, private sector partners normally have some capability to gather their own data. If the public sector is responsible for operating 511 systems in their areas, they may not have access to data specific to the emergency that is collected by the private sector.

Proposed Guideline: Public and private sectors should develop coordinated responses to homeland security emergencies, with regard to collection, processing, and dissemination of travel information. For example, this may include standard operating procedures for sharing what might normally be considered proprietary or privileged data.

Additional resources required

Issue: As homeland security emergencies will typically occur without specific warning, it is likely that operations staff will become intensely busy “working the issue” for as long as it takes. Traveler information, while important, may be regarded as a low-level concern during the initial phases of emergency response. This situation may be compounded by the evacuation of non-essential staff, and/or self-dismissal of staff concerned for family members. Insufficient qualified staff may be available to operate 511 systems; particularly posting and updating of emergency interrupt messages.

Proposed Guideline: Agencies responsible for providing content to 511 systems should designate as essential those staff qualified to operate such systems. Those staff individuals would be dedicated to the function of operating the 511 systems, and would likely be in addition to operators responsible for ensuring the other transportation functions of the agency. Appropriate management processes, such as preparation of emergency rosters, training, supervision, and overall coordination of staff functions and responsibilities may need to be addressed as appropriate to individual agency circumstances. Most importantly, standard operating procedures would be needed to ensure that 511 system operators would have immediate access to travel information and the means to update their 511 systems.

Inter-Agency Coordination

Issue: While most, if not all, transportation agencies have developed and refined emergency plans tailored to local circumstances, many of these may be predicated on past emergencies, such as natural disasters, extreme weather events, hazardous material spills, street riots, major events,

and attractions. A few states or large jurisdictions may have developed specific terrorism plans, including bio-terrorism. For the most part, these may be less developed and rehearsed than traditional emergency plans. Primary responders for such emergencies include FBI, FEMA, DOD, Secret Service, National Guard, as well as law enforcement. With the exception of FEMA and law enforcement, transportation agencies may have limited experience working with security and military authorities, and vice versa. In an emergency, the transportation function may be subject to the direction of the appropriate Office of Emergency Management, or other designated authority. The non-transportation community may not understand what types of information, and information granularity, are helpful to transportation system operators. The non-transportation community may not appreciate the role of traveler information in general, and 511 systems in particular, for emergency response.

Proposed Action: Transportation agencies must develop new relationships, including operational planning and rehearsals, with security and military authorities to ensure that the importance of 511 systems are understood and factored into emergency response processes. In addition, transportation agencies should recognize the likelihood that some information will need to be regarded as “secure”, and factor this and the possible need for staff with security clearances into their emergency planning activities, to ensure that the integrity of secure information is preserved and not posted onto 511 systems.

V. System Performance Issues

511 System capacity considerations, including cost

Issue: What assumptions about demand during a homeland security emergency should 511 system designers make when determining system capacity, i.e. what volume of calls should the 511 system be designed to accommodate? Providing adequate capacity is somewhat analogous to traditional design conventions, such as designing a facility for a pre-determined life or for a 100-year event. As with any design that enhances capacity or functionality, 511 system designers will have to make trade-offs between the benefits of such features and the cost of providing them. Designers are faced with four primary approaches:

- Design to a locally determined spike demand, such that the 511 system can be expected to maintain normal or near normal service during the emergency;
- Design to normal levels of demand, but with the feature to activate additional capacity when needed. This was the case for Salt Lake City during the 2002 Winter Olympics, where the regular capacity had been increased from 96 to 360 lines for the duration of the games, with a guaranteed overflow protection of 110% in the event that the 511 system detects a spike in demand;
- Design to normal levels of demand, and plan to address any spike in demand on an as-needed basis, e.g. by replacing the normal menus with an automatically terminated emergency interrupt message to constrain call length, adding more call takers, and adding more phone lines on an as-needed, as-available basis; and,
- Design to normal levels of demand and not attempt to address any spike in demand related to a homeland security emergency, on the basis that the 511 service is locally determined to be an inappropriate means to address such situations relative to other options, e.g. local media or law enforcement.

Proposed Action: Undertake further research into the functionality/cost trade-offs represented by the preceding design principles, and use this as a basis for proposed guidelines to 511 system designers and operators. One important avenue to explore in the coming months is the linkage between 511 system design and the proposed National Threat Alert System, in particular whether the declaration of certain levels of threat alert may trigger specific travel information responses that are eligible for federal funding.

Issue: Some estimates of spikes in demand are provided earlier in this report. Their significance and relevance to other locations or circumstances in determining adequate and appropriate capacity are matters of interpretation and judgment, and should be considered alongside other factors, such as local evidence of demand spikes for non-homeland security emergencies.

Proposed Action: Undertake further research into spike demand for travel information during emergencies, including non-homeland security emergencies, and use this as a basis for enhanced guidelines to 511 system designers and operators.

Issue: The foregoing discussion assumes sufficient capacity exists on the telephone providers' networks to handle calls from users to the 511 service. While this may be a reasonable assumption for landline service, it may not apply for cellular service.

Proposed Action: Work with landline and cellular providers, and their industry associations, to ensure adequate capacity exists to meet the locally determined needs of potential callers to 511 systems during a homeland security emergency.

Response times/quality of service

Issue: The Implementation Guidelines (version 1.1) suggest that 511 systems should be sized to accept all calls for the 90th percentile peak hour load. If live operators are utilized or connected to as part of a 511 service, 90th percentile wait time should not exceed 90 seconds, and callers should receive indications that they are on hold. 511 services should have availability to callers of 99.8% (out of service less than 18 hours a year). System performance against these parameters should be measured and monitored. During a homeland security emergency it is likely that the quality of the 511 service may deteriorate, depending on which design principle (of the four listed above) is adopted.

Proposed Guideline: Experience from New York and Washington D.C. indicates that callers experienced delays and dropped calls on September 11. Unless a 511 system has been designed to maintain normal or near normal service during the emergency or with a feature to activate additional capacity when needed, relax or suspend the quality guideline for wait time and availability.

System redundancy

Issue: Immediately following the September 11 attacks, landline and cellular telephone services became unreliable, apparently as a result of overload. In Lower Manhattan, the situation on September 11 with regard to using telephone service was compounded by damage to a Verizon central hub, resulting in the loss of 200,000 phone lines, cellular sites knocked out, local telephone switching office damaged, fiber optic transport equipment crushed, and high-speed internet service down for many companies because of power failures. Not only did this make it difficult for callers to get access to travel information, it also impacted the ability of agencies to communicate between office and field staff, and to share information with other agencies.

Proposed Action: Work with landline and cellular service providers, their industry associations, emergency management agencies, and others to address the need for communication network and system redundancy.

Critical Systems Assessment

Issue: Communications capacity and redundancy are not the only systems of concern during a homeland security emergency. Power supply and the 511 systems themselves may be the target of an attack, or be impacted by an attack.

Proposed Action: Undertake vulnerability assessments of critical systems to assess the risk of primary or backup system failures, and as a basis for the development (and costing) of mitigation plans.

VI. Conclusions

Summary

511 systems offer the potential to become a valuable medium through which to provide travel information in support of homeland security emergency management. This potential is likely to increase in the coming years as more systems are deployed and familiarity with such systems continues to grow across the nation. Put simply, 511 has the potential to be a national asset in the event of homeland security emergencies.

It is therefore appropriate for 511 system designers to take homeland security considerations into account at this time. While the September 11 attacks were tragic, it is perhaps fortunate that most 511 systems are at a formative stage of development and are thus able to embrace homeland security needs. Perhaps, it is possible that they will even offer higher levels of public service than was ever envisioned.

This White Paper draws attention to a number of issues related to customers, institutions / organizations, and system performance that must be addressed. It is fair to say that a number of the issues apply to traveler information systems in general, of which 511 systems are but one medium. Closely related to this is the recognition that there are new federal players, with their respective missions, who will likely influence the future role of 511 systems in ways that have yet to be determined. These players signify that there is a “new order” in terms of authority, control, and lines of responsibility. Transportation agencies will likely find that their detailed knowledge of transportation networks, human resources, geographical dispersion, and technology systems bring a utility to the security community that has been previously undervalued or even recognized. What is less clear is the extent to which transportation agencies retain the same level of control over their resources (including travel information systems such as 511) during a homeland security emergency, compared to a pre-September 11 situation.

Recommendations

This White Paper has addressed the challenges and opportunities for 511 systems, their designers, and their operators, arising from the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon. However, the homeland security environment is evolving, meaning this White Paper cannot be the last statement on the subject from a 511 perspective. Recognizing that there needs to be wider debate as to what role, if any, 511 systems will play during homeland security emergencies, we recommend that the 511 Deployment Coalition take the following actions:

- Recognize that while 511 system design will be primarily driven by local considerations, the potential for diverse approaches to homeland security may result in a loss of the desired national consistency, e.g. 511 could be a pillar of one region’s response to an event, while it could be non-existent in another region’s response to a similar event.
- Incorporate the proposed guidelines in this White Paper into the 511 Implementation Guidelines.
- Undertake the proposed actions in this White Paper.

- Open a dialogue with representatives from the homeland security environment, especially the new federal players (Office of Homeland Security, Transportation Security Administration, and the United States Secret Service) to better understand their perspectives towards homeland security emergency management, including the proposed National Threat Alert System, and to apprise them of the challenges and opportunities for 511 systems.
- Work closely with FHWA, FTA, and the emergency management community, and with national associations (TRB, AASHTO, APTA, ITS America, and ITE) to pool knowledge and resources regarding challenges and opportunities for 511 systems related to homeland security.
- Conduct a post-games case study of the operation of the Salt Lake City 511 system during the 2002 Winter Olympics, to document any additional homeland security related lessons learned.

VII. Acknowledgements

Task Force Members

The task force was comprised of the following members:

- Kelly Hutchinson, NCDOT, lead
- Ron Boenau, Federal Transit Administration
- Pete Costello, ITS America
- Sandra Check, New Jersey Transit
- Les Jacobson, PB Farradyne
- Keith Jasper, PBS&J
- Mac Lister, Federal Highway Administration
- Steven McDonald, Missouri DOT
- Bob Rupert, Federal Highway Administration
- Mike Sobolewski, Minnesota DOT
- Alice Wiggins, Metropolitan Atlanta Rapid Transit Authority
- Jim Wright, Minnesota DOT

Additional Insights

The task force acknowledges the assistance and insights of the following:

- Malaika Abernathy, Metropolitan Washington Council of Governments
- Karen Cavallo Miller, Battelle
- Judy Chen, California DOT
- Allan DeBlasio, Volpe National Transportation Systems Center
- Dave Ekern, AASHTO
- Arthur Hamilton, Federal Highway Administration
- Tom Hicks, Maryland State Highway Administration
- Chris Hill, NET
- Tony Kane, AASHTO
- David Lively, California DOT
- Steve Mondul, Virginia DOT
- Vince Pearce, Federal Highway Administration
- Joe Peters, Federal Highway Administration
- Frank Quon, California DOT
- Ray Ruggieri, TRANSCOM
- Rick Schuman, PBS&J