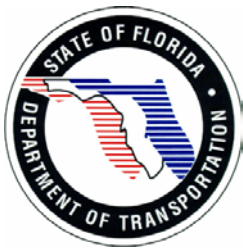


Technical Memorandum No. 3.1

Florida's 2003 Intelligent Transportation System Strategic Plan Update

Homeland Security

January 31, 2005
Version 3



Prepared for:

Florida Department of Transportation
Traffic Engineering and Operations Office
Intelligent Transportation Systems (ITS) Section
605 Suwannee Street, M.S. 90
Tallahassee, Florida 32399-0450
(850) 410-5600

Technical Memorandum No. 3.1
Florida's 2003 ITS Strategic Plan Update – Homeland Security

DOCUMENT CONTROL PANEL		
File Name:	<i>Technical Memorandum No. 3.1 – Florida's 2003 ITS Strategic Plan Update – Homeland Security</i>	
File Location:	W:\ITS Program\ITS GC\TWO25-StrategicPlanUpdate\TM3 - Issue Papers\TM3-1 - Homeland Security\041117 Homeland Security V3.doc	
Deliverable Number:		
Version Number:	3	
	Name	Date
Created By:	Keith Jasper	February 3, 2004
Reviewed By:	Diane Quigley	February 6, 2004
	Diane Quigley	April 26, 2004
Modified By:	Keith Jasper	March 19, 2004
	Dave Hodges	March 30, 2004
	Pamela L. Hoke	April 22, 2004
	Pamela L. Hoke	May 29, 2004
	Dave Hodges, PBS&J	November 17, 2004
	Pamela L. Hoke	January 28, 2005
Completed By:	Pamela L. Hoke	January 31, 2005

Table of Contents

List of Acronyms	iii
1. Purpose	1
2. Background	3
3. Potential Issues	6
3.1 Legal and Budgetary Context	6
3.2 Institutional Coordination	7
3.3 Public - Private Cooperation	5
3.4 Intermodal Transportation	8
3.5 Critical Infrastructure	9
3.6 Information Systems	10
3.7 Other National Initiatives	10
4. Recommendations	11

List of Acronyms

DHS.....	Department of Homeland Security
DOT	Department of Transportation
FDLE.....	Florida Department of Law Enforcement
FDOT	Florida Department of Transportation
FHWA.....	Federal Highway Administration
<i>FTP</i>	<i>Florida Transportation Plan</i>
FY	Fiscal Year
HAZMAT	Hazardous Materials
ITS.....	Intelligent Transportation System
ITSA.....	Intelligent Transportation Systems of America
MI5.....	Military Intelligence, Section 5
RTMC	Regional Transportation Management Center
<i>SAFETEA</i>	<i>Safe, Accountable, Flexible and Efficient Transportation Equity Act of 2003</i>
TOC.....	Traffic Operations Center
TWIC	Transportation Worker Identification Card
UK.....	United Kingdom
USDOD.....	United States Department of Defense
USDOT	United States Department of Transportation

1. Purpose

The purpose of this *Technical Memorandum* is to explore and identify new intelligent transportation system (ITS) trends, technologies, and initiatives that implement and fulfill the vision, goals, and objectives identified in *Florida's Intelligent Transportation Systems (ITS) Strategic Plan*, referred to herein as the *Plan*.

The primary purpose of the *Plan* was to present a 20-year vision for ITS in Florida and to recommend strategies to achieve this vision. The *Plan* included four main ITS goals, which were consistent with the mission and goals of the *2020 Florida Transportation Plan (FTP)*.¹ These goals included:

- Safe transportation for residents, visitors, and commerce;
- Protection of the public's investment in transportation;
- A statewide, interconnected transportation system that enhances Florida's economic competitiveness; and
- Travel choices to ensure mobility, sustain the quality of the environment, preserve community values, and reduce energy consumption.

This *Technical Memorandum* presents research on national and statewide efforts in homeland security, and determines the feasibility of pursuing or implementing these efforts over the next three years as part of Florida's ITS Program.

With the establishment of the United States Department of Homeland Security (DHS) and the signing of the *Homeland Security Act of 2002*² into law, one emphasis of national transportation programs is to secure America's critical infrastructures. This document addresses national and state homeland security policies and guidance; identifies ITS applications that may aid in improving the security of Florida's critical infrastructures; reviews legacy ITS-related homeland security efforts in Florida; and discusses funding opportunities that enhance and support homeland security for the planning, deployment, and operation of ITS.

¹ Florida Department of Transportation, *2020 Florida Transportation Plan* (2000). Available online at <http://www.dot.state.fl.us/planning/2020ftp/default.htm>.

² United States Department of Transportation, *Homeland Security Act of 2002*, PUB.L.NO. 107-296, 116 STAT. 2135 (2002).

Technical Memorandum No. 3.1
Florida's 2003 ITS Strategic Plan Update – Homeland Security

The recommendations in this *Technical Memorandum* are consistent with the *National ITS Program Plan's*³ *Homeland Security and ITS Supplement*⁴ and include recommended security guidelines developed as part of the *Regional Traffic Management Center (RTMC) Security White Paper*.⁵

³ Intelligent Transportation Society of America, *National Intelligent Transportation Systems Program Plan: A Ten-Year Vision* (January 2002). Available online at <http://www.itsa.org/research.html>.

⁴ Intelligent Transportation Society of America, *Homeland Security and ITS – Using Intelligent Transportation Systems to Improve and Support Homeland Security – Supplement to the National ITS Program Plan: A Ten-Year Vision* (September 2002). Available online at <http://www.itsa.org/research.html>.

⁵ Jasper, Keith (PBS&J), *White Paper: Regional Transportation Management Center (RTMC) Security, Version 3* (June 2003). FDOT Contract No. C-7772.

2. Background

The September 11, 2001, terror attacks in New York City and Washington, D.C., have caused many organizations to assess the security threats to, and vulnerabilities of, their mission-critical functions. Prevention of terrorism and the disruptions it can bring is now a major preoccupation across many walks of life, e.g. commerce, leisure, education, and public policy. It is sobering to recall that in the past two years, the United States has created the DHS; waged war in Afghanistan and Iraq; implemented security measures that changed the nature of air and sea travel; and established the Homeland Security Advisory System to communicate threat levels to the public. Despite these efforts, recent quotes serve to remind us that homeland security is an issue that is here to stay:

*The ultimate nightmare could bring devastation to our country on a scale we have never experienced. Instead of losing thousands of lives, we might lose tens of thousands or even hundreds of thousands in a single day of war.*⁶

*I see no prospect of a significant reduction in the threat posted to the UK and its interests from Islamist terrorism over the next five years, and I fear for a considerable number of years afterwards.*⁷

Amid these concerns, it is important to keep a sense of balance. The *Homeland Security and ITS Supplement to the National ITS Program Plan* defines the following goal for the transportation system:

A transportation system that is prepared for and well-protected against attacks, that responds rapidly and effectively to natural and human-caused threats and disasters, that supports appropriate transportation, emergency management, and public safety agencies, that ensures the ability to move people and goods even in times of crisis, and that can be quickly and efficiently restored to full capability.

⁶ Quote by Vice President Dick Cheney in a speech on weapons of mass destruction, Portsmouth, New Hampshire (October 10, 2003).

⁷ Quote by Director-General Eliza Manningham-Buller, Directorate of Military Intelligence, Section 5 (MI5), in a speech in London, England (October 16, 2003).

Five broad areas are identified for the application of ITS to homeland security: preparedness, prevention, protection, response, and recovery. In many regards, Florida is leading the nation in its approach to each of these five areas by virtue of the security component of the *iFlorida* model deployment,⁸ including:

- **Preparedness** – For the bridge monitoring project, *iFlorida* has undertaken a vulnerability assessment of selected bridges and is in the process of doing the same for the District 5 RTMC. In addition, the emergency evacuation project with Daytona International Speedway will be investigating various what-if scenarios in conjunction with numerous transportation and emergency management agencies, as well as other local agencies. A separate *iFlorida* project will develop simulation and visualization techniques to model alternative traffic routing around critical infrastructure components that are impacted by emergency situations.
- **Prevention** – For the bridge monitoring project, *iFlorida* will be deploying sensors and software designed to detect suspicious activity. Likewise, on-board surveillance on selected Central Florida Regional Transportation Authority LYNX transit vehicles in the Downtown Orlando-Walt Disney World corridor will provide continuous monitoring and early warning of security threats.
- **Protection** – The above *iFlorida* projects offer the potential for law enforcement and other emergency responders to not just detect incidents, but also to activate coordinated responses. While not a security project, the *iFlorida* hurricane evacuation project will use such techniques to support the decision process for, and implementation of, emergency lane reversals to increase evacuation capacity.
- **Response** – All components of *iFlorida*, not just security, will provide an architectural framework, and the tools and technologies needed to enhance operational response to a variety of recurrent and other situations. In particular, through a network of sensors, data fusion, and dissemination, *iFlorida* will determine and distribute accurate, up-to-date information about the transportation system's status to responders and the traveling public.
- **Recovery** – Again, all components of *iFlorida* contribute to an enhanced capability to execute situation-appropriate emergency response, and offer the potential to maximize the transportation system's available capacity.

⁸ More information regarding the Florida Department of Transportation's *iFlorida* Surface Transportation Security and Reliability Information System Model Deployment Project is available online at <http://www.iflorida.net>.

There are other efforts instituted by the Florida Department of Transportation (FDOT) that have a bearing on an effective response to emergency situations. The FDOT's Traffic Engineering and Operations Office (TEOO) has established a successful traffic incident management program that provides a platform for institutional and operational coordination in the event of any future terrorist attack. This program has its origin in Florida's long and successful history of coordination between emergency managers and the transportation community in responding to major hurricanes. Tools that can be utilized include contraflow plans for evacuations on major highways, suspension of tolls, traffic advisories posted on dynamic message signs, and information delivered using the 511 traveler information system. These and other ITS technologies were successfully applied in the summer of 2004 when four major hurricanes struck the state over a period of seven weeks.

3. Potential Issues

The remainder of this *Technical Memorandum* highlights some areas of potential concern that merit deeper research and status tracking, as well as prioritization for future consideration and possible action. No priority is implied by the order in which these issues are listed, although in general they are listed from a “soft” issue perspective to a “hard” issue perspective. This order was selected for two reasons, the first being simply that this provides a logical flow to the discussion. The second reason reflects the potential degree of difficulty (ranging from most difficult to least difficult) that may be associated with addressing the issues. In short, the more external partners beyond the FDOT that may or will need to be involved, the greater the likely the degree of difficulty will be.

3.1 Legal and Budgetary Context

The Florida Department of Law Enforcement (FDLE) is the lead agency for homeland security in Florida. The FDOT has established lines of communication with the FDLE, and has worked closely with that agency on homeland security matters of common interest. That said, the extent to which the FDOT can participate in security operations might be limited by legal and budgetary considerations (e.g., the involvement of the Governor’s Office if the FDOT seeks funding for security activities). This, and any limiting factors on the FDOT’s ability to preserve the confidentiality of security-sensitive information, must be addressed.

3.1.1 Legal Issues

The FDOT, like most state departments of transportation, collects a significant volume of real-time information, such as video, sensor data, and probe information. Generally speaking, this information is not archived. In part, this is to avoid the workload that archiving would entail and the potential legal aspects of third parties seeking access to this information.

In most cases, the public is unaware that the images obtained from CCTV traffic cameras are neither recorded nor used for law enforcement purposes. Still, there is a suspicion among the traveling public that the widespread use of these surveillance technologies is violating individual privacy. However, the potential value of such information to law enforcement and security agencies in detecting suspicious behavior patterns is enormous. Consequently, serious consideration should be given to the development of FDOT policies that address legal protection for the archiving of such information when there is an overriding public safety concern, and that define how the practice would be applied, such as locations adjacent to sensitive facilities or critical infrastructures.

3.1.2 Budgetary Issues

The extent to which Florida can participate in security operations as described herein will depend on available funding. The first step will be to quantify the funding implications of the actions described. The required funding will probably have to address a combination of human resources (i.e., full-time equivalents and training), equipment, and planning needs.

In terms of funding sources, additional research is needed to determine whether any new programs are available in the *Safe, Accountable, Flexible and Efficient Transportation Equity Act (SAFETEA) of 2003*,⁹ which is the new six-year federal transportation legislation that authorizes a total of \$247.4 billion in transportation expenditures through fiscal year (FY) 2009. Other funding may be available through the DHS and its constituent administrations. To date, much of this funding has been directed towards first responders, aviation, and ports.

For the most part, it appears likely that the FDOT will have to prioritize its traditional funding sources for use in homeland security, leveraging the functionality of ITS technologies deployed for regular traffic management and travel information to support security operations.

3.2 Institutional Coordination

Whether the transportation system is the target of an attack, or the means by which an attack is delivered, it is highly probable that the same system will be the primary means by which any evacuation takes place and a logistical response is delivered. Much of the case study analysis following the September 11, 2001, attacks highlighted communications, particularly interjurisdictional communications, as an area for improvement. Much has been done in this regard across the nation and in Florida. It is an area in which the FDOT management and its operational components have much to offer, and consequently underscores the need for the FDOT to be a major player in the homeland security arena. An integral part of this involvement is the need for interagency tabletop discussions, security simulations, and real exercises, as well as an ongoing training program for key staff. Not only will this ensure that the FDOT is ready to respond, it will serve as a valuable outreach to nontraditional partners to better understand the resources and capabilities of the FDOT.

⁹ More information regarding the United States Department of Transportation's (USDOT) proposed *SAFETEA* bill is available online at <http://199.79.179.101/reauthorization/safetea.htm>.

3.3 Public – Private Cooperation

The traditional context for public-private partnerships is the development of innovative methods for the funding of major projects. Typically, the public role is to create a legal or regulatory framework into which the private sector can bring its entrepreneurial skills, protect its intellectual capacity, and create a profitable revenue stream while delivering a desired service or project. In a homeland security context, a different – and sometimes new – relationship is needed. Put simply, a terrorist attack could occur on private property. Just as an attack on public property, such as a bridge, tunnel, or command center, can be “war-gamed” and a range of responses developed, so too can a private organization do the same for its facilities. However, there quickly comes a point where evacuations and response logistics have a broader impact than the private party can manage, such as those that can occur following an attack on a theme park, sports event, or other major attraction.

The FDOT may need to play a sudden and major role handling abnormally high traffic movements, unusual mixes of travel modes (including evacuees on foot), spikes in demand for travel information, and the transport of hazardous materials (HAZMAT) and weaponry. These events may occur during off-peak hours when operational capacity in command centers may be low. Consequently, the historical relationships between the public and private sectors may need to be revisited and enhanced to ensure a coordinated response.

3.4 Intermodal Transportation

The transportation system consists of many modes, ranging from pedestrian, bicycle, and car to truck, van, bus, or other specialty vehicles. Taking a broader perspective, the transportation system as a whole includes land, sea, and air components. Not only do each of these modes and components have their own vulnerabilities and associated threats, the movement of goods and people frequently occurs in a series of stages involving several modes. This provides multiple opportunities for terrorists to strike at a particular group or commodity; it also creates additional targets in the form of intermodal facilities and connectors.

From an FDOT perspective, this has several important implications. First, while a container ship arriving from an international port falls under another agency's jurisdiction, that same container, when transferred to truck or train, may become of interest if it is attacked or if it contains a weapon. Again, this highlights the need for interagency coordination and intelligence sharing – to track sensitive loads throughout the logistics supply chain, to ensure coordinated actions that will prevent attacks, and to respond to attacks should they occur.

Second, the functional interfaces between modes may represent avoidable weaknesses in the overall operational management of the transportation system, particularly between transportation operators that do not have a tradition of interoperability. For example, a mass evacuation of trucks from a seaport or passengers from an airport, or a security incident resulting in the temporary closure of an airport or seaport, may require the advance planning of the FDOT's major and immediate operational management personnel. Once again, there is no certainty that any such response will coincide with the operating hours of the FDOT's responding centers, potentially resulting in suboptimal resource availability.

An additional thought here is that many airports and seaports are currently acquiring and deploying ITS technologies for security and traffic management functions. Florida has led other states in the application of security measures at its deep-sea ports. While the primary motivation of these measures was initially focused on criminal activity within seaports, their impact has nonetheless resulted in the greater use of ITS technologies for port security operations. Considerable potential exists for port authorities to be "reinventing the wheel" when it comes ITS architectures, and many opportunities for interoperability and resource sharing between these agencies and the FDOT may be overlooked.

3.5 Critical Infrastructure

Much of the focus across the nation since September 11th has been on the protection of critical infrastructures. This has not been limited to transportation, but has also included other industries and utilities, such as water supply, power generation, and transmission networks. Within transportation, much of the focus continues to be on airports and air travel. At a national level, seaports are seen as the next priority, particularly concern regarding the possible ease of entry of undesirable people and weapons. International borders have also witnessed a general tightening of entry requirements for both people and goods.

Florida, like other states, has its own critical infrastructure in the form of bridges, tunnels, and traffic operation centers (TOCs). Quite apart from the immediate injury and loss of life that would potentially follow an attack on a critical infrastructure, the loss of such an infrastructure for an extended period of time will cause an ongoing disruption that can have an equally devastating impact on Florida's economy and mobility. This is particularly true in situations where the loss of a bridge interrupts waterborne traffic as well as vehicular traffic. Given the economic importance of Florida's tourism industry and the contribution of seaports to local, regional, and national commerce, the FDOT's most critical infrastructure must be protected for broader reasons than the management of peak commuter flows. Once again, this highlights a need for stronger relationships with nontraditional partners, such as port authorities, the United States Coast Guard, and United States Customs and Border Protection.

3.6 Information Systems

The FDOT has previously prepared the *RTMC Security White Paper*. The RTMCs are the brains of Florida's highway network, capable of multiple functions for managing day-to-day operations and emergencies. The *RTMC Security White Paper* identified the characteristics of different types of attacks, both cyber and physical. It recommended a four-phase action plan that will focus primarily on the first of the five broad areas detailed in *Section 2* for the application of ITS to homeland security, with the objective of improving preparedness.

The four phases outlined in the action plan included research; vulnerability and threat assessments; recovery and business continuity plans; and implementation activities. The potential role of the RTMCs in responding to an attack is enormous, as was witnessed by the command-and-control role the Virginia Department of Transportation's Smart Traffic Center played in the minutes, hours, and days following the September 11th attack on the Pentagon. Protecting these valuable assets in Florida is clearly an important priority.

3.7 Other National Initiatives

The Federal Highway Administration (FHWA) public safety and security program is taking many initiatives to enhance the role of transportation agencies in homeland security. Florida is already at the forefront of some of these, as evident with the *iFlorida* model deployment. The FHWA's objectives, such as fostering partners, improving interagency communications, and coordinating with the United States Department of Defense (USDOD), certainly command Florida's attention. Current activities include bridge security; telecommunications vulnerability reduction; cargo security; and the integration of voice, data, and video demonstrations.

The DHS' Transportation Security Administration is developing a transportation worker identity card (TWIC). The TWIC project will conform to national standards to ensure that the identification cards are interoperable, allowing consistent functionality requirements to be achieved nationwide, and that transportation workers will be able to use the same credentials in multiple locations. To some extent, Florida preempted the TWIC initiative several years ago when the Florida Ports Council led the development of its own version of this card. As yet, it is too soon to be certain that the national and Florida systems will be interoperable. Either way, the FDOT should monitor developments in this regard and consider its own credentialing requirements.

4. Recommendations

This *Technical Memorandum* has reviewed the status of various transportation security initiatives currently underway in Florida and nationally. Through the *iFlorida* model deployment, Florida is already at the leading edge of several initiatives of national significance. Lessons learned from *iFlorida* over the coming three years will also benefit similar applications in Florida.

Given that homeland security is a subject most DOTs did not need to pay much attention to prior to September 11, 2001, and the legal and budgetary limitations that affect the FDOT's involvement in security operations, the road map for moving forward over the coming three years is emerging slowly. For the most part, this mirrors the emergence of related funding programs.

Subject to available funding, it is highly recommended that the FDOT adopt the recommendation for a four-phase action plan, as detailed in the *RTMC Security White Paper*, but expand it to include the broader range of topics listed above. This will enhance the FDOT's level of preparedness in the event of a homeland security emergency. In addition, lessons learned from *iFlorida* should form a basis for further development of the FDOT's approach to homeland security in the coming three years, with ITS services and technologies providing a vital element in Florida's effort to meet these critical safety and security objectives.