SOUTHERN CALIFORNIA REGION TRANSPORTATION SECURITY STUDYFOR THE 2008 RTP

FINAL REPORT
SOUTHERN CALIFORNIA REGIONAL ITS ARCHITECTURE UPDATE FOR TRANSPORTATION SECURITY

Prepared for

SOUTHERN CALIFORNIA ASSOCIATION of GOVERNMENTS

Southern California Association of Governments

June 2008

Prepared by: URS

2020 East First Street, Suite 400
Santa Ana, California 92705

In Association with:
IBI Group

TABLE OF CONTENTS

List of Figures

List of Tables

ES - Executive Summary

Background

Under TEA-21, the Federal Highway Administration (FHWA) and Federal Transit Administration (FTA) issued mandates that required regions implementing ITS project to have an ITS architecture in place by April 2005. Thereafter, all ITS must have conformance to the regional ITS architecture to be eligible for federal funding. Under SAFETEA-LU, a new federal law requires Regional ITS Architecture to incorporate security elements to the National ITS Architecture in order to fulfill the needs of increasing complicated society and its threats. The updated Regional ITS Architecture seeks input from security related agencies, such as local law enforcement, local emergency and heath agencies, including offices of emergency services. This document will serve as a supplement to the adopted Regional ITS Architecture to incorporated new security elements required by federal mandate.

The Regional ITS Architecture is an important tool to organize information and mobilize resources. It will be used by:

- Transportation operating agencies to recognize and plan for transportation integration opportunities in the region.
- Planning Agencies to better reflect integration opportunities and operational needs into the transportation planning process.
- Security, Emergency Response, and other organizations and individuals that use the transportation system in the SCAG region.

The Regional ITS Architecture provides an overarching framework that spans all of these organizations and individual transportation projects. Using the architecture, each transportation project can be viewed as an element of the overall transportation system, providing visibility into the relationship between individual transportation projects and ways to cost-effectively build an integrated transportation system over time.

Southern California Association of Governments' (SCAG) ITS, Other Resources, and Stakeholders

SCAG's ITS Architecture Update for Transportation Security provides a framework and vision for the future deployment of ITS applications through the six county region: Los Angeles, Orange, Ventura, San Bernardino, Riverside, and Imperial counties. It incorporates the existing and planned ITS projects, and sets a framework for stakeholders to plan their systems in the long term but allows the flexibility to break out their system into small and modular components that could be implemented as funding permits.

This regional ITS architecture supplement incorporates security elements to the 2004 SCAG regional architecture at the regional level. As mentioned above new federal law requires, Metropolitan Planning Organizations (MPOs) to improve the capabilities of local and county governments to protect its region's transportation systems and critical infrastructure, as well as to enhance the overall level of preparedness

for responding to harmful incidents or disasters. The region's intelligent transportation system is a critical infrastructure element that is to be protected, but it also is a resource that enables the protection of other critical infrastructure elements.

The threats of crime, terrorist activity, and natural disasters may generate casualties and injuries, damage and destruction of property and infrastructure, economic impacts, and significant disruption of daily life. The transportation sector, as other critical sectors of the country, is continuously striving to improve prevention, preparedness, response, recovery, and mitigation capabilities at all levels of society.

The Southern California is a vast region comprised of 38 thousand square miles and over 18 million persons. It has one of the worlds' largest and most dynamic economies. As a result, the region has a vast and complicated transportation infrastructure consisting thousands of miles of freeways and road miles, three important seaports, a regional aviation system, and numerous supporting systems. Not surprisingly, the region has a myriad of stakeholders representing various services and interests needed to maintain the safe, efficient, and secure movement of people and goods in the region. These stakeholders consist of cities, counties, sub-regional council, transportation commissions, transportation authorities, Caltrans districts, ports, airports, transit operators, toll road authorities, international ports of entry, law enforcements, fire departments, and offices of emergency management.

Southern California's ITS Needs and Operation Concepts

Under federal law, SCAG like other of the country's MPOs is required to take an active role in regional security transportation planning. It is to define security transportation planning as mandated by federal mandate and not hinder the activities of existing emergency stakeholders but rather assist them in the policy arena and situational awareness through a vast repository of data and information on the region. SCAG aims to improve the capabilities of local and county governments to better protect its region's transportation systems and critical infrastructure, as well as to enhance the overall level of preparedness for responding to harmful incidents or disasters. In section 5 of the ITS Architecture Supplement, there are details of SCAG's ITS security vision statement for the 2008 RTP. The vision elements described include:

- SCAG's role in Security
- SCAG's Facilitator Role
- SCAG's role in Regional Security Planning
- SCAG's role in Regional Preparedness
- SCAG's role as a Promoter of Regional ITS Solution
- SCAG's role as a Regional Provider of Data and Information

Regional ITS Project Sequencing

The regional ITS architecture is implemented through many individual ITS projects that occur over years, or even decades. An important step of the Regional ITS architectural development, is to identify a sequence of ITS projects that will contribute to the integrated regional transportation system. It also entails consensus building and setting priorities that show how ITS projects can build one another. Since these ITS projects are regional in concept, they generally represent the highest stages of ITS development, i.e. Caltrans interfaces represent the integration of data exchange between the four (4) Caltrans District systems. In section 8 of the ITS Architecture Security Supplement, it contains the listing of projects for Southern California Regional ITS Architecture by title, market package, Stakeholder(s), simple description, and the expected timing (S= short term, M=medium term, L=long term). All projects are listed irrespective of whether or not they will be funded through federal sources.

Project Standards and Considerations

Although 2004 SCAG Regional ITS System Architecture already addressed and highlighted relevant standards for transportation and related systems, the application of specific security considerations are new and a consequence to the threat environment to the region's transportation infrastructure. Hence, it is important to consider the relationship these and emerging standards have in light of the application of specific security considerations to the regional architecture. Section 9 highlights standards and related considerations drawing largely on documentation prepared for the National ITS Architecture, including "National ITS Architecture Security," prepared by the Architecture Development Team (May 2007).

Architecture Maintenance and Agency Agreements

As with the 2004 ITS Architecture, this supplement recommends tri-annual updates to coordinate with the RTIP process as required by region's counties, and interim submission of changes are also facilitated. Section 10 details Southern California Regional Architecture maintenance plan in order to enable these procedures to be simple, flexible and easy to follow and allow the architecture documents to be modified to reflect both political and technological developments.

As required by federal mandate, the region's transportation and emergency stakeholders (agencies and organizations) must have agreements to implement the integration of the Regional ITS Architecture. These agreements (existing or new) are required for operations, including at a minimum those affecting ITS projects interoperability, utilization of ITS related standards, and the operation of the projects. These requirements are to provide a list of agreements and not the agreements themselves; since, experience shows that it takes an actual project deployment to initiate the agreements process. Section 11 of this document details the agency agreements for the Regional ITS Architecture.

1.0 INTRODUCTION

1.1 SCAG TRANSPORTATION SECURITY STUDY PURPOSE AND BACKGROUND

The purpose of this study is to define the role of the Southern California Association of Governments (SCAG) with regards to improving the capabilities of local and county governments to protect its region's transportation systems and critical infrastructure, as well as to enhance the overall level of preparedness for responding to harmful incidents or disasters.

Metropolitan Planning Organizations and Security

Metropolitan Planning Organizations (MPOs) play important roles throughout the United States, primarily in the development of regional transportation infrastructure and planning. At the state level, MPOs take additional responsibility for the public welfare of their jurisdictions, such as developing crucial base and horizon year socio-economic data for planning purposes, specialized research (like the Regional Housing Needs Assessment), intergovernmental reviews, and other public benefit planning practices.

Prior to the September 11, 2001 terrorist attacks on the United States, there was not any single incident that impacted transportation facilities as result of a national consequence. These events also created a new awareness of the vulnerabilities of transportation fleets and facilities. Although natural disasters such earthquakes and hurricanes have produced significant regional casualties and property damage, none had the serious disruption to national travel and national economy as the September 11 terrorist attacks. As concern about the threat of terrorism and consequences of natural disasters has grown, government (at all levels) has taken new measures to securing the welfare of its citizens. Hurricane Katrina and other natural disaster have also brought attention to how critical emergency preparedness is to response and recovery after catastrophic events. Transportation and transit agencies throughout the United States are taking increasing steps to protect their facilities against the threats of crime, terrorist activity, and natural disasters. These events generate casualties and injuries, damage and destruction of property and infrastructure, economic impacts, and significant disruption of daily life. The transportation sector, as other critical sectors of the country, is continuously striving to improve prevention, preparedness, response, recovery, and mitigation capabilities at all levels of society. As is discussed below, MPOs can play a significant role in promoting preparedness and recovery capabilities.

Federal Mandate

Transportation safety and security emphasis is reflected in the recent transportation authorization bill, known as SAFETEA-LU (Safe, Accountable, Flexible, Efficient Transportation Equity Act – A Legacy for Users), signed into law on August 10, 2005. SAFETEA-LU authorizes the Federal surface transportation programs for highways, highway safety, and transit for the 5-year period, 2005-2009. It specifies that MPOs will conduct a metropolitan planning process that provides for consideration of projects and strategies that will 'increase the security of the transportation system for motorized and non-motorized users'.

The Federal Highways Administration released a Final Rule related to its interpretation of SAFETEA-LU, noting that the metropolitan transportation planning process should be consistent with the Strategic Highway Safety Plan, and other transit safety and security planning and review processes, plans, and programs, as appropriate. Effective March 16, 2007, under federal law, MPOs are now tasked with addressing elements of security in their transportation plans and encouraged to take a regional role in their jurisdiction.

With the federal government's continued focus on transportation security, it passed the transit security funding law, the National Transit Systems Security Act of 2007, providing $3.4 billion for the improvements of U.S. mass transit security (over the fiscal years of 2008 to 2011). It was signed into law on August 3, 2007 and will appropriate funds as follows:

- $650 million for fiscal 2008;
- $750 million for fiscal year 2009;
- $900 million for fiscal year 2010; and
- $1.1 billion for fiscal year 2011.

This funding allows for procurement of equipment related to surveillance, communication, emergency response, and automated vehicle locator (AVL) type systems.

1.2 PURPOSE OF THIS REPORT

The Southern California Association of Governments (SCAG) Regional Intelligent Transportation Systems (ITS) Architecture is a roadmap for transportation systems integration in the six county region in Southern California (Los Angeles, Orange, Riverside, San Bernardino, Ventura, and Imperial Counties). The ITS architecture was developed through a cooperative effort by the region's transportation agencies and deployed in 2005. It was to satisfy the conformity requirements established in the Transportation Equity of Act for the 21st Century (TEA-21) and continued in the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU). Under TEA-21, the Federal Highway Administration (FHWA) and Federal Transit Administration (FTA) issued mandates that required regions implementing ITS project to have an ITS architecture in place by April 2005. Thereafter, all ITS must have conformance to the regional ITS architecture to be eligible for federal funding.

The development of the Regional ITS Architecture was one of the most important steps in planning for and implementing ITS in the Southern California region. It provides a shared vision of how each agency's systems will work together in the future, encouraging inoperability, identifying standards, sharing information and resources to provide a safer, more efficient, and more effective transportation system for travelers in the region. The Regional ITS Architecture also sets a framework for stakeholders to plan their systems in the long term but allows the flexibility to break out their system into small and modular components that could be implemented as funding permits.

Security elements have been added to the National ITS Architecture in order to fulfill the needs of increasing complicated society and its threats. The updated Regional ITS Architecture seeks input from security related agencies, such as local law enforcement, Department of Homeland Security, and Office of Emergency Services. This document will serve as a supplement to the adopted Regional ITS Architecture to incorporated new security elements required by federal mandate.

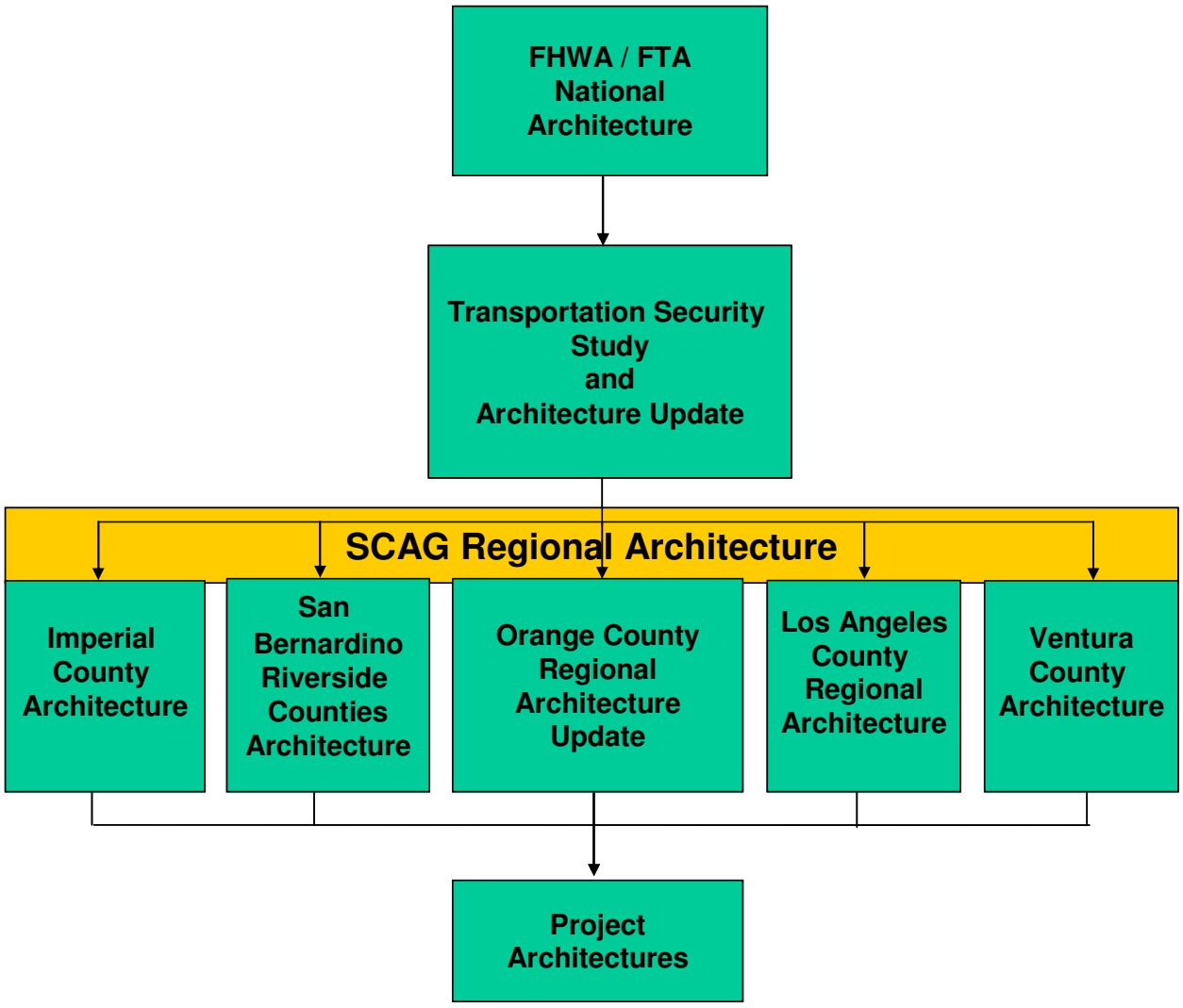
The Regional ITS Architecture is an important tool to organize information and mobilize resources. It will be used by:

- Transportation operating agencies to recognize and plan for transportation integration opportunities in the region.
- Planning Agencies to better reflect integration opportunities and operational needs into the transportation planning process.
- Security, Emergency Response, and other organizations and individuals that use the transportation system in the SCAG region.

The Regional ITS Architecture provides an overarching framework that spans all of these organizations and individual transportation projects. Using the architecture, each transportation project can be viewed as an element of the overall transportation system, providing visibility into the relationship between individual transportation projects and ways to cost-effectively build an integrated transportation system over time.

In this supplement, the National ITS Architecture Version 6 is utilized and latest version of TurboArchitecture™ database employed, Version 4.0. The Regional architecture and its market packages are detailed in a subsequent section of this document. Below, Figure 1-1 depicts the SCAG ITS Architecture approach. It takes a hierarchical approach in where National ITS Architecture provides the source of the structure for the regional and county architecture documents. This framework also incorporates existing and planned transportation projects and provides a path for new projects to follow as they conceived, designed, and deployed.

Figure 1-1 - SCAG ITS Architecture Approach Diagram



1.3 RELATIONSHIP TO 2004 SCAG REGIONAL ARCHITECTURE

The Southern California Regional ITS Architecture was completed in 2005. It provides a framework and vision for the future deployment of ITS applications through the six county region: Los Angeles, Orange, Ventura, San Bernardino, Riverside, and Imperial counties. The regional architecture incorporates the existing and planned ITS projects, and provides a path to be followed as new projects are conceived, designed, and deployed. This regional ITS architecture supplement incorporates security elements to the 2004 SCAG regional architecture at the regional and sub-regional levels.

1.4 ORGANIZATION OF REPORT

This document is organized into eleven primary sections:

Section 1 – Introduction: This section introduces the project and discusses the scope of the updated SCAG Regional ITS Architecture.

Section 2 – Regional Description: A description of the region and its transportation system is given to provide context for the development of the Southern California Regional ITS Architecture.

Section 3 – Regional Stakeholders: This section identifies the regional stakeholders, including traditional transportation organizations, local law enforcement, and emergency responders, particular entities involved in catastrophic incidents.

Section 4 – ITS Inventory: A inventory approach is taken to document the region's ITS.

Section 5 – ITS Needs and Operation Concepts: This section addresses ITS needs, services to cover those needs, and operational concepts.

Section 6 – Function Requirements: Functional requirements are list for ITS which entail defining the agencies' roles, needs, services and market package to continue developing ITS services.

Section 7 – Information Flows and Interface Requirements: This section outlines a framework view to integrate systems that benefit by sharing data.

Section 8 – Project Sequencing: This section provides a sequence of ITS projects that will contribute to the integrated regional transportation system envisioned for the region.

Section 9 – Identification of Required Standards: This section identifies the required standards for the Regional ITS Architecture, as required by federal rule.

Section 10 – Architecture Maintenance: A discussion on the approach to maintaining the Regional ITS Architectures is detailed in this section.

Section 11 – Agency Agreements: As mandated by federal rule, all agreements (existing or new) concerning ITS are identified in this section.

2.0 REGIONAL DESCRIPTION

The SCAG is the federally designated Metropolitan Planning Organization for six counties in southern California: Imperial, Los Angeles, Orange, Riverside, San Bernardino, and Ventura Counties. It covers the largest MPO area in the country, consisting of 34,000 square mile, the equivalent of the state of Ohio. SCAG has a vast geographic area ranging from coast line, mountainous terrain, to expansive deserts. It also has densely populated urban centers, as well as desolate rural areas. Los Angeles County is the most populous county in the nation and San Bernardino is the largest in land area. The region's topographic diversity and large land mass extends its borders to Arizona, Nevada, and Mexico.

The SCAG region includes 187 cities, constituting the nation's second largest MPO by population with 18.6 million persons. It is almost half of California's population. The SCAG region also remains of one the largest economic engines in the United States. It would rank 15th, if it were an independent nation. Southern California faces numerous challenges to maintaining its important role in the country and the world; including the ability to prevent, or recover from, catastrophic events. Possible threats to the region include natural disasters, terrorist and criminal activities, and pandemic outbreaks.

SCAG is primarily responsible for transportation planning and programming for the six county region. It collaborates with the California Department of Transportation (Caltrans), county transportation commissions, and other agencies in the Region that perform transportation planning and analyses and other related activities. The Southern California's Regional ITS Architecture has been developed and deployed by SCAG in 2004. In the following, this document updates the Regional ITS Architecture to incorporate new federally mandated security elements. It becomes a tremendous challenge to effectively implement an infrastructure because of the region's immense size, diversity, and complexity.

Financial constraints, lack of suitable lands, and environmental impact issues have challenged options to increase roadway capacity through construction. Hence, transportation efficiencies are sought through new technologies, more specifically Intelligent Transportation System (ITS). ITS solutions are also being employed to improve safety, and now considered an option to assist with security concerns. The region's ITS architecture is a structured view of the world of transportation technology and is intended to help optimize the benefit of individual investments, in order to capitalize on years of previous investment in transportation technology by identifying the interfaces and paths that will make it possible to integrate many systems in the future. Sharing information in this way leverages the value of original investments many times over while promoting the efficiency of regional transportation operations. Today, security elements have been added to ensure the region's transportation system operates safety and efficiently without major incident.

The Southern California Regional ITS Architecture provides a framework that includes a vision for the future deployment of ITS applications throughout the region. It incorporates existing and planned ITS projects, and provides a path to be followed as new projects are conceived, designed and deployed. In regards to security, the primary objective in ITS Architecture is to protect transportation information and infrastructure. Information technologies have become a seminal component in transportation to sense, collect, process and disseminate information to improve efficiency and safety of the movement of people and goods, as well as to provide alternatives and/or contingencies.

2.1 THREATS IN THE REGION

The SCAG region is vulnerable to many types of catastrophic events including earthquakes, floods, fires, hazardous material incidents, dam failures, civil unrest, transportation accidents, tsunamis and terrorism. In addition, there is a potential for public health and agricultural emergencies to occur within the region. Currently, there are many agencies that will participate in the response to a disastrous event and ensure their jurisdictions are prepared to respond to these hazards. Transportation is vital element to provide resources to persons involved in a disastrous situation, either as victims or emergency responders.

As concern about the threat of terrorism and consequences of natural disasters has grown, government (at all levels) has taken new measures to securing the welfare of its citizens. Hurricane Katrina and other natural disaster have also brought attention to how critical emergency preparedness is to response and recovery after catastrophic events. Transportation and transit agencies throughout the United States are taking increasing steps to protect their facilities against the threats of crime, terrorist activity, and natural disasters. These events generate casualties and injuries, damage and destruction of property and infrastructure, economic impacts, and significant disruption of daily life. The transportation sector, as other critical sectors of the country, is continuously striving to improve prevention, preparedness, response, recovery, and mitigation capabilities at all levels of society. As is discussed below, SCAG can play a significant role in promoting preparedness and recovery capabilities. It could promote to utilize the Southern California Regional ITS Architecture to disseminate information, gather information, and provide situational awareness during an event.

2.2 REGIONAL TRANSPORTATION SYSTEM

The United States is comprised of nearly 3.8 million square miles and has a population over 300 million persons. Its transportation systems continue to evolve and expand in order to accommodate its populous, workforce, and economy. Security of the nation's transportation systems and the lives of the people that utilize these systems are a top priority of government agencies at all levels. Transportation systems include airports, ports, waterways, rail, highways, and pipelines[1]. According to the Bureau of Transportation Statistics, the United States maintains over four million miles of roadway (streets, roads, highways), nearly 600 thousand bridges, 150 thousand miles of railway, over 5,000 public airports, 1.3 million miles of gas pipelines, and over 180 thousand mile of gas pipeline.

Roadways and Freeway

In the SCAG region, transportation infrastructure also comprises a vast system. Its transportation network embroiders through most of region's urbanized, suburban, and rural areas. The following outlines the region transportation system's lane miles.

Freeway Lanes Miles (excluding carpool)	9,400 miles
Carpool Lane Miles (including HOT lanes)	860 miles
Road Lane Miles (arterials)	43,550 miles

[1] The American transportation sector is dependent on foreign oil sources; in fact 46.5 percent of petroleum used in the United States is currently imported (Bureau of Transportation Statistics 2007)

Total vehicle miles traveled (VMT) in the region exceeded 150 billion in 20XX. The region consistently ranks as the most congested metropolitan region in the nation. Residents in the coastal counties (Los Angeles, Ventura, and Orange) experienced a total of **X hours** of delay per person in **20XX** compared to 34 hours of delay in San Bernardino and Riverside counties. Los Angeles County has four of the ten most congested highway locations in the U.S., namely the I-405 at the I-10 interchange, U.S. 101 at the I-405 interchange, State Route 55 at the State Route 22 Interchange, and the I-10 at the I-5 interchange. Each location average ten (10) minutes of delay per vehicle per trip during peak hours. Trucks are significant contributors to congestion but are also affected by congestion, and the resultant costs ultimately affect all residents and consumers. Truck traffic is expected to rise 33 percent by 2035 as freight commerce from the port continues to boom.

ITS programs are becoming increasingly important in the efficient movement of people and goods. The region's freeway networks are equipped with Vehicle Detection Stations (VDS), Closed-Circuit Television (CCTV) cameras, Changeable Message Signs (CMS), Ramp Meter Stations (RMS), Highway Advisory Radio (HAR), and Environmental Sensor Stations (also known as road weather information systems (RWIS)) are employed in strategic locations. These ITS field elements are connected to the Transportation Management Centers (TMCs) for the California Department of Transportation (Caltrans) Districts 7, 8 and 12.

Public Transit

The SCAG region also comprises a large public transit system, consisting of buses, light rail, and heavy rail. Currently, mass transit is becoming an increasingly important option for residents as the cost of gasoline and other goods and services rise in price. In fact, the American Public Transportation Association (APTA) reported record breaking trends in the first quarter of 2008 (June, 2008). There has been a 3.3 percent surge from the same period the year prior. Ridership trends are expected to continue as gas prices keep climbing in expense. The region is comprised of the following resources.

Buses	300 vehicles
Bus routes	640 routes
Metro Rail	73 miles and 65 Stations
Rail Network	2 subways, 3 light rail, 3 busways
Metrolink	7 routes, 512 miles, and 55 Stations

In 2006, the total number of transit boardings was nearly 740 million. Expanded transit services, particularly the heavy rail, light rail and commuter rail, attracted additional transit riders. Nevertheless, transit usage in the region currently accounts for nearly 5% of the total work trips and 2% of the total person trips. The region's two largest public transit providers are Metro and Metrolink. Metro operates approximately 2,000 peak-hour buses on an average weekday and 73.1 miles of Metro Rail service and 62 stations, consisting of the Metro Red Line subway system, the Metro Blue Line, the Metro Green Line,

and the Metro Gold Line. Metrolink serves over 45,000 passengers in 50 cities throughout Southern California. Amtrak runs the Pacific Surfliner that operates along the Pacific Coast, connecting San Diego, Los Angeles, Oxnard, San Luis Obispo, and Santa Barbara. The two basic types of transit service are fixed route and demand-responsive. The first type allows buses to operate on fixed schedules on a fixed route. Demand-responsive service allows route changes based on individual trip requests. The fixed route service also accommodates commuters using long-distance routes (also referred to as Express Routes), which provide trips to and from a single destination without intermittent stops. Demand-responsive services for the elderly and disabled are offered in the region. For both large and small fixed route systems, ITS applications are multi-faceted and may integrate two or more of the following functions: automatic vehicle location, vehicle and equipment monitoring, customer information, signal priority, fare box summaries, and central dispatch center facilities. For demand-responsive systems, the primary ITS application is automated trip scheduling and in some cases in conjunction with Automatic Vehicle Location (AVL) systems.

Emergency Management Services

The California Highway Patrol (CHP) provides traffic patrols and response to incidents and emergencies with responsibility for all freeways, conventional state routes, and some roadways in unincorporated areas of the county. The CHP also provide service under contract to the Toll Roads in Orange County. In addition, CHP along with Caltrans staff monitor traffic conditions and incident information at the Caltrans TMCs for dissemination to field staff. Information disseminated include CCTV camera images, status reports from field crews, traffic flow data, weather data, CHP incident reports, or summaries of 911 calls. The field staff includes CHP officers, Caltrans maintenance crews, local agencies, including police and transit officials, and private contractors involved in towing, roadside maintenance, or hazardous material spill cleanups. Each county also has Sheriff and Fire Departments that provide law enforcement, fire protection, and Emergency Medical Services (EMS) in unincorporated areas of the county, as well as to certain city jurisdictions under contract arrangements. County Sherriff departments are the primary law enforcement agency in Metro and Metrolink facilities. Other transit providers, such as Foothill Transit provide their own policing. Office of Emergency Services employs sheriff and fire departments from the county, it services.

These Emergency Management departments are dispatched through county 9-1-1 centers. These centers are equipped with Computer Aided Dispatch (CAD) systems, which allow dispatchers to initiate emergency response through radio dispatch communications and then track response activities performed by field personnel. Many of the larger cities also have their own police and/or fire departments, which handle law enforcement, fire protection, and EMS for their jurisdictions. The larger agencies are most often but not always CAD-equipped.

Aviation/Ports

Los Angeles International Airport (LAX) and Ontario International Airport are the region's two international airports; John Wayne Airport, Bob Hope Airport, Long Beach, Palmdale, and Palm Spring comprise its other five commercial airports. In 2007, the SCAG region accounted for 89.5 MAP (million

air passengers) and 2.7 million tons of air cargo. LAX served 61.8 MAP and carried over 2 million tons of cargo, making it one busiest air passenger and cargo facilities in the world. LAX is administered by the Los Angeles World Airports (LAWA) agency, a department of the City of Los Angeles which also manages Ontario International Airport, Palmdale Airport, and Van Nuys Airport.

The SCAG region is home to three international deepwater port facilities: the Port of Los Angeles (POLA), the Port of Long Beach (POLB), and Port Hueneme. The Ports of Los Angeles and Long Beach, together form the third largest container port complex in the world, following Hong Kong and Singapore. These two ports handle 50 percent of West Coast container cargo and 35 percent of all waterborne cargo in the U.S. The Port of Long Beach is a department of the City of Long Beach, and the Port of Los Angeles is a department of the City of Los Angeles. POLB and POLA transfer container freight between ship and land-based carriers involving multiple organizations. The ports operate in coordination with organizations such as the California Trucking Association and the Steamship Association of Southern California.

POLA and POLB have a joint project involving the use of vehicle detection, CMS and CCTV for monitoring port access routes. In 2002, the total traffic at the Ports of Los Angeles and Long Beach increased to 152.2 million tons. Close to 84% of all cargo shipments were through containers. In April 2002, the Alameda Corridor was opened and allowed faster transfer of cargo from the twin ports to eastern destinations. In addition to the Alameda Corridor, two major highways serve the twin port complex. Interstate 710, the Long Beach Freeway, is a heavy trucking corridor that carries traffic from the busy Port of Los Angeles north to downtown Los Angeles, with a connection to transcontinental Interstate 10. The numbering of I-710 as a spur of I-10 is related to the fact that both I-110 and I-710 connect that freeway with the port.

Commercial/General Aviation Ports	57
LAX ranks among world's airports	5th in passengers and 10th in cargo
Long Beach/Los Angeles ranks among world's	Container ports 5th
Share of United States Maritime Trade	40 percent.

3.0 REGIONAL STAKEHOLDERS

The SCAG region has a multitude of transportation, security, and emergency services stakeholders. Stakeholders consist of:

- Cities (187)
- Counties (6)
- Sub-regional councils (14)
- Transportation commissions (5)
- Transportation authorities (4)
- Caltrans Districts (4)
- Ports (3)
- Commercial/General Aviation Airports (57)
- Transit Operators (53)
- Toll Road Authorities (3)
- International Ports of Entry (3)
- Law Enforcement (149)
- Fire Departments (154)
- Air Quality District (4)
- Offices of Emergency Management (6)

For this supplement to the Regional ITS Architecture outreach efforts were focused on the regional level. Telephone interviews were conducted with 14 stakeholders from Caltrans, transit operators, regional transportations commissions, and Offices of Emergency Management. In addition, sub-regional councils were utilized to gather input from the various aforementioned regional stakeholders. Outreach and feedback sessions were held in downtown Los Angeles, Ventura, Redondo Beach, Ontario, and Palm Desert. Participants included sheriffs, city transportation engineers, transit agencies, city planners, ITS specialists, emergency response professionals, and other public sector professionals.

Many of these stakeholders assisted in the development of the ITS User needs document and further defined the appropriate role for the Southern California Association of Governments in the region's Security related manners. Table 3-1 lists the regional stakeholders for this supplement effort.

Table 3-1 - Regional Stakeholders

Offices of Emergency Services	• Imperial County • Los Angeles County • Orange County • Riverside County • San Bernardino County • Ventura County • City of Los Angeles
CALTRANS Districts	• District 7 • District 12 • District 8
Metropolitan Planning Organizations	• San Bernardino Association of Governments, SANBAG • Los Angeles County Metropolitan Transportation Authority, Metro • Imperial Valley Association of Governments, IVAG • Ventura County Transportation Commission, VCTC • Orange County Transportation Authority, OCTA • Riverside County Transportation Commission, RCTC • Ventura County Council of Governments • Coachella Valley Association of Governments, CVAG
Transit Agencies	• Foothill Transit • Long Beach Transit • OCTA • METRO • South Coast Area Transit (SCAT) • Ventura Intercity Service Transit Authority VISTA • SunLine Transit
Other Public Agencies	• City of Los Angeles Department of Transportation • Los Angeles County Department of Public Works • Southern California Regional Rail Authority, METROLINK • County of Orange • County of Los Angeles • Ventura County • Riverside County • San Bernardino County • Imperial County
Law Enforcement Agencies	• Orange County Sheriff • Ventura County Sheriff • Los Angeles County Sheriff • California Highway Patrol • U.S. Customs and Border Protection

4.0 ITS INVENTORY

4.1 INVENTORY APPROACH

This document is a supplement to Regional ITS Architecture deployed in 2005, in order to include security elements mandated by federal rule. In 2005, there were county-level architectures that created inventories of existing and planned systems. These systems also included multi-county level systems to evaluate their regional effectiveness and multi-regional issues. In this supplement, a multi-county level approach is taken to incorporate the security related elements to the Regional ITS architecture. Generally, the Multi-County ITS Architecture level projects focus on systems or generic categories of systems with projects that involve (or potentially involve) integration across the six county region. An example of this high level thinking is the classification of the Regional Traveler Information Systems in the inventory. This high level group includes all means and methods of disseminating traveler information regardless of whether they are public or private systems. It covers all modes of transportation and all types of information. The various Market Packages associated with the very high level systems are included. "Systems" as used in this context is a general concept that may include hardware, software, communication, and dissemination devices. For further information concerning this ITS inventory, Appendix X, contains the TurboArchitecture™ generated inventory report.

4.2 SUMMARY OF INVENTORY

4.2.1 Background

Civic infrastructure is critical to the welfare of urban areas. Transportation, utilities, communications, fuel, and water all provide services essential to the welfare and quality of life of residents. Catastrophic incidents often produce a cascading effect on the infrastructure. If one of these support systems breaks down it can have a domino effect on other elements, and the failure of multiple elements can be crippling. Basic assessments of the impacted areas are needed to produce an adequate emergency response to a disaster. An assessment of vulnerabilities to security and safety also may prevent or limit effects of a catastrophic incident.

The region's transportation system, which includes the networks and support infrastructure, are of the utmost importance to the mobility, safety, security, and economic vitality of both the region and its inhabitants. Throughout the region significant investment in ITS technologies is being used to help increase the efficient management of the transportation networks. While ITS alone will not solve the region's transportation problems, ITS applications provide key management tools that help the operational efficiency of the network. ITS applications are also expected to significantly contribute to security and safety, e.g. on high truck volume freeways and at rail/highway crossings. The greatest challenges and perhaps the greatest benefits lie in integrating major systems across the entire region.

Critical Transportation Infrastructure

Critical Transportation Infrastructure (CTI) consists of transportation facilities whose removal from service would severely impact the public safety, national security, economic activity, or environmental quality. Examples of Critical Transportation Infrastructure include:

1. Major arterial highways and bridges comprising the National Highway System (NHS), including Strategic Highway Network (STRAHNET) and National Intermodal Connectors.

2. International marine harbors, ports and airports.

3. Major railroads, including depots, terminals and stations.

4. Oil and natural gas pipelines.

5. Transportation Control Systems (e.g., air traffic control centers, national control center).

As with most regions of the world, the transportation infrastructure in Southern California plays a major role in its residents' quality of life. The region's expansive urban form makes travel critical to daily life. Not surprisingly, a 2006 public opinion survey found the overwhelming concern in the region is transportation. Although the region has among the highest cost of housing in the nation and high indices of crime, these problems are not as concerning as the exacerbating situation of traffic[2]. A failure in the transportation system as a result of natural disaster or human-caused event would bring foreseeable disruptions in the quality of life to many individuals in the region.

[2] The Ralph and Goldy Lewis Center for Regional Policy Studies UCLA School of Public Affairs.

5.0 ITS NEEDS AND OPERATIONS CONCEPTS

5.1 REGIONAL NEEDS

Under new federal law, Metropolitan Planning Organizations (MPOs) are obligated to take an active role in regional security transportation planning. SCAG's vision for security transportation planning is described in the vision elements for ITS security in the region.

5.1.1 ITS Security Vision Statement for 2008 RTP

The vision is to define security transportation planning as mandated by federal law that does not hinder the activities of existing emergency stakeholders but rather assist them in the policy arena and situational awareness through a vast repository of data and information on the region. Essentially, SCAG aims to improve the capabilities of local and county governments to better protect its region's transportation systems and critical infrastructure, as well as to enhance the overall level of preparedness for responding to harmful incidents or disasters.

5.2 VISION ELEMENTS

This section describes the elements included in SCAG's ITS security vision statement for the 2008 RTP. The vision elements described include:

- SCAG's role in Security
- SCAG's Facilitator Role
- SCAG's role in Regional Security Planning
- SCAG's role in Regional Preparedness
- SCAG's role as a Promoter of Regional ITS Solution
- SCAG's role as a Regional Provider of Data and Information

5.2.1 SCAG's Role in Security

The Southern California Association of Governments' (SCAG) Safety and Security Program seeks to support the capabilities of local and county governments to better protect its region's transportation systems and critical infrastructures, as well as to enhance the overall level of preparedness for responding to harmful incidents or disasters.

Within that construct, SCAG has four security roles:

1. Provide a policy forum to help develop regional consensus and education on security
2. Assist in the planning and programming of transportation infrastructure repairs.

3. Leverage projects and planning functions (including Intelligent Transportation Systems) that can enhance or provide benefit to transportation security efforts and those responsible for planning and responding to emergencies.

4. Become a central repository/mirror for regional geo-data that can be used for planning, training, and response and relief efforts of security and emergency stakeholders.

5.2.2 Facilitator Role

SCAG seeks a role in a policy advisory capacity. It would focus on strategic, not tactical, elements of emergency preparedness. SCAG understands that the organization does not have the authority to enforce actions on the part of jurisdictions and other agencies, but it may encourage and support recommended planning activities. Furthermore, the agency is conscientious of not wanting to compete with emergency management agencies, with regards to authority or funding. SCAG should be seen as a resource that may provide meaningful assistance with regards to planning activities and data. While SCAG's primary focus is transportation, it has been acknowledged that the region's transportation system is both an asset that needs to be protected from catastrophic events, as well as a resource used to respond to such events.

5.2.3 Regional Security Planning

SCAG does not want to replicate the functions or intrude on the roles of emergency management agencies. While there are many safety and security operations groups, there are no specific groups that focus on policies for the region. SCAG envisions filling this need in concurrence with their role in security transportation planning.

SCAG wants to bring situational awareness of security to the region for the array of potential disasters. It recognizes the fact that the region's ITS planning and deployments provide an opportunity for the region to leverage this investment to enhance situational awareness and further the efforts of the emergency management community.

- SCAG's active role in the security planning process (within the policy arena) would require:
- Emphasizing transportation as a resource and a stakeholder in security planning and operations;
- Educating officials about transportation-related issues with regards to safety and security;
- Participating in a regional security working group;
- Assisting with the identification of opportunities and resources that support emergency management;
- Leveraging federal funds to support security preparedness;
- Increasing its knowledge of best practices and how to implement them, and then identifying its role with regard to their implementation;

- SCAG would also increase its role as a data source and further serve as a clearinghouse for various types of data sets;

- SCAG should play a role in supporting situational awareness for safety and security purposes by using geospatial data.

5.2.4 Regional Preparedness

SCAG has a regional preparedness goal to prevent, protect, respond, and recover from major human-caused or natural events in order to minimize the threat and impact to lives, property and the regional economy. Its' transportation security plans will help ensure that there is a productive movement of persons and goods if a disastrous event strikes the region. SCAG has the following opportunities to elevate its role in the region as a policy forum and data clearinghouse:

- Develop proactive transportation security strategies that support economic vitality in the region;

- Enhance the effectiveness of agencies responsible for security preparedness and emergency response;

- Ensure that regional transportation technology investments meet the needs of emergency responders through interoperable, robust, and strategically redundant ITS and communications infrastructure;

- Provide a regional forum for members of the transportation and emergency management communities to coordinate transportation and security initiatives, and to reach agreement on how to work more closely together during the decision notification process prior to and following an event;

- Update the regional ITS Architecture and associated County architectures describing specific systems interoperability requirements to support regional safety and security objectives; and

- Satisfy SAFETEA-LU requirements for regional transportation planning to incorporate security considerations.

5.2.5 Promoter of Regional ITS Solution

SCAG also envisions developing a thorough Intelligent Transportation System (ITS), as it controls the regional ITS architecture, funding, and programming.

Major elements of its role include:

- Identifying more command and control for Critical Transportation Infrastructure (CTI);

- Developing mechanisms to make data available through Traffic Management Centers (TMC) to assist first responders and training first responders to take advantages of these resources;

- Identifying system detection gaps and using this to prioritize funding;
- Prioritizing command and control infrastructure through funding;
- Supporting County Office of Emergency Services (OESs) through the programming and planning of funding to TMCs and other activities;
- Continuity of government is another area SCAG may be able to provide leadership within the region. There is a lack of agreements between agencies for mutual aid (in many cases, especially in the transportation arena). SCAG finds an opportunity to facilitate this process and identify needs and prioritize agreements and planning at the regional and sub-regional level between agencies, particularly for long-term recovery after events.

5.2.6 Regional Provider of Data and Information

In the Ten Year Strategic Plan: Goals and Strategies, SCAG indicates that it wishes to be a central source for data and information about the Southern California Region. SCAG has a strong desire and commitment to be a major data repository. However, SCAG will undertake this role where and if appropriate to facilitate the planning processes and activities of local and regional stakeholders. SCAG's goal is to be an acquirer and source for regional level data and information. The review of several relevant transportation and security planning documents illustrates that SCAG has a challenging task in serving the region. It also has a tremendous opportunity not only to serve the region in transportation security planning efforts, but to serve as an example to the rest of the nation. As mentioned above, federal mandates have recently passed to make security planning part of the purview of MPOs. On the other hand, the mandates are not clear of the roles of MPOs and specific steps have not been defined. Essentially, SCAG will be breaking new ground on the role of a MPO for its jurisdiction in the arena of transportation security planning.

5.3 Recommended Transportation Security User Services for the Region

This section provides a general definition and the characteristics of user services. Using this as a foundation it goes on to list all of the user services bundles that include security related user services and provides a description of each security related user service. Following this is a description of the ITS Security Areas included in the National ITS Architecture. The term "Security Area" represents areas of ITS which can be used to enhance surface transportation security. Finally, all of the security related ITS needs and priorities from each SCAG sub-region are prioritized in a series of matrices.

5.3.1 General Definition

A user service is defined as: **One or more specific ITS applications that address specific needs for a specific set of users**.

User services document what ITS should do from the user's perspective. A broad range of users are considered, including the traveling public as well as many different types of system operators. To date, thirty-three User Services have been jointly developed by US DOT and ITS America with substantial stakeholder input. A set of requirements covering each of these User Services are the basis for the

National ITS Architecture definition. The User Services entry point leads you to the full set of user service requirements and allows easy traversal between the user service requirements and the components of the architecture that satisfy these requirements.

The concept of user services allows system or project definition to begin by establishing the high level services that will be provided to address identified problems and needs.

5.3.2 Characteristics of User Services

The national ITS program is focused on the development and deployment of a collection of inter-related user services. Thirty-three (33) user services have been defined to date. This list of user services is neither exhaustive nor final. There is a wide variety of transportation services that could develop that are not included in this list. Furthermore, the services here are expected to change over time. Some will develop largely as envisioned, new services will emerge, and others, for various reasons, may never be developed. This list of services and the accompanying descriptions are expected to evolve through program plan updates and new editions.

The users of a particular service will vary and could include travelers of any mode, operators of transportation management centers, transit operators, Metropolitan Planning Organizations (MPOs) such as SCAG, commercial vehicle owners and operators, state and local governments, and many others who ultimately may take advantage of ITS including homeland security agencies.

Although each user service is unique, they share several common characteristics. User services are:

Composed of Multiple Technological Elements

A single user service will usually depend upon several technologies such as advanced communications, mapping, and surveillance, and may be shared with other services.

Building Blocks

Once the basic technological functions, such as communications or surveillance, have been deployed for one or more service, the additional functions needed by one or more related services may require only a small incremental cost. The added functions will in turn produce supplementary benefits. User services can be combined for deployment in a variety of ways depending upon local priorities, needs, and market forces.

Adaptable to Rural, Urban, and Suburban settings

ITS user services are not specific to a particular location. Rather, the function of the service can be adapted to meet local needs and conditions.

Table 5-1 - User Service Bundles & User Services

User Services Bundle	User Services[3]
1. Travel and Transportation Management	1.1 Pre-trip Travel Information 1.2 En-route Driver Information 1.3 Route Guidance 1.4 Ride Matching And Reservation **1.5 Traveler Services Information** 1.6 Traffic Control **1.7 Incident Management** 1.8 Travel Demand Management 1.9 Emissions Testing And Mitigation **1.10 Highway Rail Intersection**
2. Public Transportation Operations	2.1 Public Transportation Management 2.2 En-route Transit Information 2.3 Personalized Public Transit **2.4 Public Travel Security**
3. Electronic Payment	3.1 Electronic Payment Services
4. Commercial Vehicle Operations	4.1 Commercial Vehicle Electronic Clearance 4.2 Automated Roadside Safety Inspection **4.3 On-board Safety And Security Monitoring** 4.4 Commercial Vehicle Administrative Processes **4.5 Hazardous Materials Security And Incident Response** 4.6 Freight Mobility
5. Emergency Management	**5.1 Emergency Notification And Personal Security** **5.2 Emergency Vehicle Management** **5.3 Disaster Response And Evacuation**
6. Advanced Vehicle Safety Systems	6.1 Longitudinal Collision Avoidance 6.2 Lateral Collision Avoidance 6.3 Intersection Collision Avoidance 6.4 Vision Enhancement For Crash Avoidance 6.5 Safety Readiness 6.6 Pre-crash Restraint Deployment 6.7 Automated Vehicle Operation
7. Information Management	**7.1 Archived Data**
8. Maintenance & Construction Management	8.1 Maintenance And Construction Operations

Out of the 33 user services, there are ten than can be considered "security related". These ten security related user services are described in more detail in the following sections.

5.3.3 Travel and Traffic Management

The Travel and Traffic Management user services deal with information collection, dissemination, and processing for the surface transportation system. These services collect and process information about the surface transportation system, and provide commands to various traffic control devices. Travel management services disseminate this information to travelers. These services also provide information to

[3] Security Related User Services shown in **BOLD**

support the Public Transportation Management and Information Management bundles. Thus, the Travel and Traffic Management bundle will be of interest to transportation policy makers, public and private sector operators of transportation management centers, those involved in accident response or travel demand management, and private sector vendors supplying travel information products and services.

5.3.3.1 Traveler Services Information

The **Traveler Services Information** service provides a business directory, or "yellow pages," of information on travel-related services and facilities, for example the location, operating hours, and availability of food, lodging, parking, auto repair, hospitals, and police facilities. Traveler services information would be accessible in the home, office or other public locations to help plan trips, and it would also be available en-route. The service includes not only the traveler services information, but the capability to make reservations for many of the traveler services.

5.3.3.2 Incident Management

The **Incident Management** service uses advanced sensors, data processing, and communications to improve the incident management and response capabilities of transportation and public safety officials, the towing and recovery industry, and others involved in incident response. This service will help these groups to quickly and accurately identify incidents and implement a response which minimizes traffic congestion and the effects of these incidents on the environment and the movement of people and goods.

5.3.3.3 Highway Rail Intersection (HRI)

The **Highway Rail Intersection (HRI)** service uses ITS technologies to provide improved control of highway and train traffic to avoid or decrease the severity of collisions that occur between trains and vehicles at HRIs.

5.3.4 Public Transportation Management

The Public Transportation Management user services describe those services provided by public transit organizations throughout the country. They address fixed route and demand response systems, as well as those passenger rail systems operated by transit agencies. Aspects of the transit system ranging from operations, to maintenance and security are covered. This bundle includes a transit traveler information aspect that also supports services in the Travel and Traffic Management bundle.

5.3.4.1 Public Travel Security

The **Public Travel Security** service creates a secure environment for public transportation patrons, operators, and support staff. It provides systems that monitor the environment in transit facilities, transit stations, parking lots, bus stops and on-board transit vehicles and generate alarms, either automatically or manually, when necessary. The service also provides systems that monitor key infrastructure of transit (rail track, bridges, tunnels, bus guideways, etc.). This improves security, and with it, the perception and acceptance of transit. Transit agencies can integrate this user service with other anti-crime activities.

5.3.5 Commercial Vehicle Operations

These user services support the goals of improving the efficiency and safety of commercial fleet operations, and will benefit both the states and the motor carrier industry. The bundle is organized around the use of advanced computer and communication technologies to improve the safety and productivity of the motor carrier industry throughout North America. From a technical perspective, the foundation for all the commercial vehicle operations user services is the exchange of information on the motor carrier, the vehicle, the driver, and, in some cases, the cargo. The services are interrelated in terms of the specific types and functionality of information and data required. This network of information will be accessible by states and motor carriers nationwide.

5.3.5.1 On-board Safety and Security Monitoring

The **On-board Safety and Security Monitoring** service will non-intrusively monitor the driver, vehicle, and cargo and notify the driver, carrier, and possibly enforcement personnel if an unsafe situation arises during operation of the vehicle. Such an unsafe situation might involve the status of driver fatigue, vehicle systems, or cargo shift. This service will tie into the later stages of the Automated Roadside Safety Inspection and Commercial Vehicle Electronic Clearance services.

5.3.5.2 Hazardous Materials Security and Incident Response

The **Hazardous Materials Security and Incident Response** system will provide emergency personnel at the scene of hazardous materials incident immediate information on the types and quantities of hazardous materials present in order to facilitate a quick and appropriate response.

5.3.6 Emergency Management

Emergency management and public safety (police, fire, and emergency medical services) agencies use emergency management services to improve their management of and response to emergency situations. In addition this bundle covers the coordination between public safety organizations and the other transportation organizations (e.g. traffic, transit, and maintenance) to address situations ranging from traffic incidents to disasters to evacuations.

5.3.6.1 Emergency Notification and Personal Security

The **Emergency Notification and Personal Security** user service focuses on reducing the time from occurrence of an emergency or non-emergency incident until the notification of the appropriate response personnel and on providing an accurate estimate of the location of the vehicle in need of assistance.

5.3.6.2 Emergency Vehicle Management

The **Emergency Vehicle Management** user service is oriented towards reducing the time from receipt of notification of an incident by a Public Safety Answering Point operator to arrival of the emergency vehicles on the scene. This user service is divided into three sub services: Emergency Vehicle Fleet Management, Route Guidance, and Signal Priority.

5.3.6.3 Disaster Response and Evacuation

The **Disaster Response and Evacuation** user service uses ITS to enhance the ability of the surface transportation system to respond to disasters. The user service provides enhanced access to the scene for response personnel and resources, provides better information about the transportation system in the vicinity of the disaster, and provides more efficient, safer evacuation for the general public if needed. In addition, the transportation system includes a wealth of trained professionals and resources that constitute a portion of the disaster response. Use of ITS to prioritize, allocate, and track these personnel and resources also provides a more effective response to disasters.

5.3.7 Information Management

This bundle is the logical offshoot of both the Travel and Traffic Management and Public Transportation Management user service bundles. Both of the two original bundles focus on measuring transportation data for real-time use and disseminating it to the traveling public. However, the copious amount of data gathered in the process is also useful to planners, safety personnel, and other organizations. The single user service in the Information Management bundle addresses how to process and store the data acquired by ITS monitoring systems in a manner that is efficient, thorough, and user-friendly.

5.3.7.1 Archived Data

The **Archived Data** user service (ADUS) describes the need for an ITS historical data archive and expands the National ITS Architecture to encompass the needs of the stakeholder groups of this user service. ADUS requires ITS-related systems to have the capability to receive, collect, and archive ITS-generated operational data for historical, secondary, and nonreal-time uses. ADUS prescribes the need for a data source for external user interfaces and provides data products to users. The goal is the unambiguous interchange and reuse of data and information throughout all functional areas.

ITS technologies generate massive amounts of operational data that are presently used primarily in real-time to effect traffic control strategies. Examples include the adjustment of ramp meter timing based on freeway flow conditions and the use of dynamic message signs to communicate traffic incidents to travelers. These data offer great promise for uses beyond the execution of ITS control strategies, such as applications in transportation administration, policy, safety, planning, operations, and research. In most cases, ITS-generated data are similar to data traditionally collected for these applications, but are much more voluminous in quantity and geographical and temporal coverage. ITS has the potential to provide data needed for planning, performance monitoring, program assessment, policy evaluation, and other transportation activities, including multimodal and intermodal applications. This user service describes the need for the collection, manipulation, retention, and distribution of data generated by ITS for use in other transportation activities.

5.3.8 Security Related User Services

User services represent what the system will do from the perspective of the user. A user might be the public or a system operator. The concept of user services allows the process of system or project definition to begin by thinking about what high level services will be provided to address identified problems and needs. The 33 user services are combined into eight bundles. There are ten security related user services shown below in relation to their respective user service bundle.

Table 5-2 - Security Related User Services

User Service Bundle	Security Related User Service
Travel and Traffic Management	• Traveler Services Information • Incident Management • Highway-Rail Intersections
Public Transportation Management	• Public Travel Security
Commercial Vehicle Operations	• On-Board Safety and Security Monitoring • Hazardous Material Security and Incident Response
Emergency Management	• Emergency Notification and Personal Security • Emergency Vehicle Management • Disaster Response and Evaluation
Information Management	• Archived Data

5.3.8.1 Security Update to the National ITS Architecture

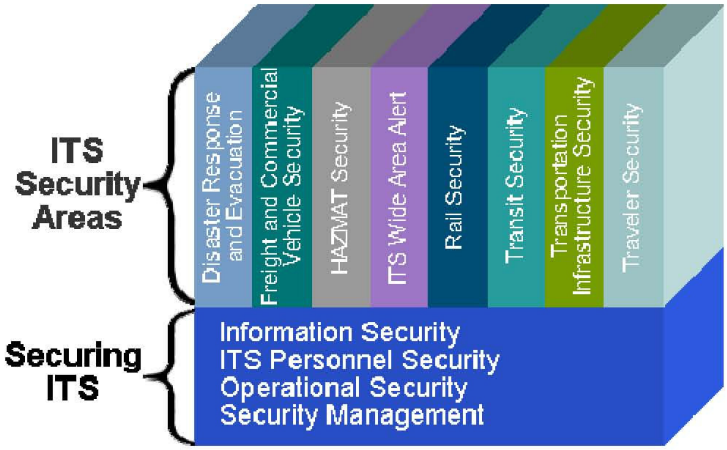
Security, in the context of the National ITS Architecture, is to protect the surface transportation information and infrastructure. The focus of the security update to the National ITS Architecture is the security services or mechanisms that meet this high-level objective.

Although previous versions of the National ITS Architecture addressed some areas of ITS security (e.g., Traveler Security), it was felt that a comprehensive ITS security review and update to the National ITS Architecture would be beneficial for protecting surface transportation. Surface transportation is now, more than ever, relying on information technologies to sense, collect, process and disseminate information to improve the efficiency of moving goods and people, improve the safety of our transportation system and provide travel alternatives.

Security is represented in the National ITS Architecture in two ways:

1. **Securing ITS:** ITS is an information system in its own right that must be protected so that ITS applications are reliable and available when they are needed. This aspect of security applies to all the subsystems and architecture flows in the National ITS Architecture. "Securing ITS" is shown as the foundation since the ITS systems must be secure before ITS can reliably be used to improve the security of the surface transportation system.

2. **ITS Security Areas:** ITS can be used to enhance the security of the surface transportation system. Eight security areas define the ways that ITS can be used to detect, respond to, and recover from threats against the surface transportation system. These eight ITS security areas are shown at the top of the figure below, supported by the "Securing ITS" security services that make ITS secure. Specific subsystems, architecture flows, market packages, and supporting physical and logical architecture definitions have been defined for each ITS security area.



Consider a transit surveillance system that includes CCTV cameras and a control center to illustrate these two views of security. From one perspective, we need to make sure that the cameras can only be controlled by the control center, that they can't easily be taken off-line, and that any sensitive images that may be collected are protected from unauthorized disclosure. These are all considerations associated with securing the transit surveillance system and are addressed as part of "Securing ITS". From another perspective, the transit surveillance system is an ITS system that provides both a deterrent and a response tool that improves the security of the transportation system. This view of the transit surveillance system is defined in one of the eight security areas ("Transit Security").

The term "Security Area" represents areas of ITS that can be used to enhance surface transportation security. The National ITS Architecture provides entities (subsystems and terminators), functions, and interfaces that cover aspects of eight ITS security areas in the figure below. For each ITS security area, the following sections discuss the scope of the area along with its architecture representation including appropriate market packages.

5.3.8.2 Disaster Response and Evacuation

The Disaster Response and Evacuation (DRE) Security Area uses intelligent transportation systems to enhance the ability of the surface transportation system to respond to and recover from natural disasters, terrorist acts, and other catastrophic events. DRE improves access to the scene for response personnel and resources, provides better information about the transportation system in the vicinity of the disaster, supports resource coordination and sharing of current situation information, and provides more efficient, safer evacuation for the general public if needed.

All types of disasters are considered including natural disasters (hurricanes, earthquakes, floods, winter storms, tsunamis, etc.) and technological and man-made disasters (hazardous materials incidents, nuclear power plant accidents, and national security emergencies such as terrorism, nuclear, chemical, biological, and radiological weapons attacks terrorist acts.). Broad inter-agency coordination is critical in all disaster scenarios, with transportation professionals performing well-defined roles in the larger context of the multi-agency response to the disaster. DRE defines how ITS can be used to coordinate and integrate DRE activities within diverse organizations in order to improve the safety of the responders and the public at large, and improve the performance and effectiveness of the transportation system as a part of the overall disaster response.

In the physical architecture, DRE centers on the Emergency Management Subsystem, which represents the interface to local, county, state, and federal public safety, emergency management, and other allied response agencies. In DRE, this subsystem represents both the Emergency Operations Centers and the Incident Command Systems that are established when disaster strikes. DRE focuses on the interfaces between this subsystem and the subsystems that represent the transportation operators and information providers (Traffic Management Subsystem, Transit Management Subsystem, Information Service Provider, Maintenance and Construction Management, Rail Operations, etc.). DRE builds on existing Incident Management capabilities that were already defined in the National ITS Architecture prior to Version 5.0.

The Disaster Response and Evacuation security area centers around the Emergency Management subsystem and is best characterized in the National ITS Architecture by four market packages: Early Warning System (EM07), Disaster Response and Recovery (EM08), Evacuation and Reentry Management (EM09), and Disaster Traveler Information (EM10).

5.3.8.3 Freight and Commercial Vehicle Security

The area of freight and commercial vehicle security considers the awareness aspect of security through the surveillance of either commercial vehicles or freight equipment. Freight equipment includes containers (with or without chassis), the chassis, or trailers. In addition, the interface with intermodal facilities is another aspect of this area. There are four major functions included as part of this security area.

- The first functional area is tracking commercial vehicle or freight equipment locations to determine if an asset has deviated from its planned route. The carrier's operation center (FMS, Fleet and Freight Management Subsystem) would be responsible for monitoring the route. In addition, the commercial vehicle's on-board system can correlate its current location to the planned route and notify the operation center of a route deviation. If a route deviation exceeds the established limits, the operation center would be responsible for formulating a response plan, which could include notifying public safety agencies.

- The second functional area is to monitor the identities of the driver, commercial vehicle and freight equipment for consistency with the planned assignment. The carrier's operation center (FMS) determines if an unauthorized change has occurred and is responsible for implementing a response plan, which could include notifying public safety agencies. In support of a seamless intermodal system, assignment information is exchanged with intermodal facilities and shippers.

- The third functional area is to monitor freight equipment for a breach or tamper event. A breach or tamper event includes the nature of event, time, location, freight equipment identity, monitoring device status and environmental threat sensor readings (chemical, biological, etc.).

- The fourth functional area is to monitor the commercial vehicle for a breach or tamper event. A breach or tamper event, in this instance, includes the nature of event, time, location, commercial vehicle identity, driver identity and monitoring device status.

The Freight and Commercial Vehicle Security area is largely comprised of four market packages. The Fleet Administration (CVO01) market package includes the capability to identify commercial vehicle route deviations. The location of the Commercial Vehicle can be monitored by the Fleet and Freight Management subsystem and route deviations exceeding the established limit are flagged. The Fleet and Freight Management subsystem is responsible for formulating a response plan, which could include notifying public safety agencies.

The Freight Administration (CVO02) market package includes the capability to identify route deviations, and breach and tamper events of freight equipment. The Fleet and Freight Management subsystem monitors the route by obtaining location information directly from the freight equipment or via the commercial vehicle. The Fleet and Freight Management subsystem monitors shipments to make sure that no tampering or breach of security occurs to the freight equipment. For security related incidents, the Fleet and Freight Management subsystem is responsible for formulating a response plan, which could include notifying public safety agencies.

The On-board CVO and Freight Safety and Security (CVO08) market package includes the capability for the Fleet and Freight Management subsystem to detect and respond to commercial vehicle breach and tamper events. In addition, both commercial vehicle and freight equipment breach or tamper events are made available to the Commercial Vehicle Check subsystem.

The Freight Assignment Tracking (CVO13) market package provides for the planning and tracking of three aspects of commercial vehicle shipments. For each shipment, the commercial vehicle, the freight equipment, and the commercial vehicle driver, are monitored for consistency with the planned assignment. The Fleet and Freight Management subsystem determines any unauthorized changes, and is responsible for formulating a response plan which could include notifying public safety agencies.

5.3.8.4 HAZMAT Security

The HAZMAT Security area's purpose is to reduce the likelihood of a successful hijacking of security sensitive HAZMAT cargo and its subsequent use as a weapon.

- The first major function is tracking security sensitive HAZMAT cargo carrying commercial vehicles and report unexpected and significant deviations or operations on restricted roadways to police. In order to protect business confidential operational information, the operational tracking and the determination of a significant route deviation requiring notification of public safety is done by a commercial carrier's operations center (FMS).

- The second major function is detection of security sensitive HAZMAT cargoes on commercial vehicles by remote sensing and imaging from the roadside. By also reading electronic tag information (carrier ID, vehicle ID and driver ID) from a sensed commercial vehicle, any detected security sensitive hazmat can be correlated with existing credentials, to determine if the cargo being carried is a permitted operation. If not, the vehicle can be asked to pull-in, and public safety may be notified.

- The third major function is authentication of drivers and notification to public safety if an unexpected driver attempts to operate a vehicle carrying security sensitive HAZMAT. As with tracking security sensitive HAZMAT cargo, the commercial fleet management center acts to validate and verify any discrepancies prior to notification of public safety.

The HAZMAT Security area is largely represented by four market packages. The Fleet Administration (CVO01) market package includes the capability to track commercial vehicles by a Fleet and Freight Management center. If the Fleet Management Center notices a significant discrepancy, it may notify police.

The CV Administrative Processes (CVO04) market package includes the distribution of usable and non-usable local and national HAZMAT routes with associated administrative restrictions by time and for specific classes of HAZMAT cargoes. This map information is distributed by public agencies to Information Service Providers, Fleet and Freight Management functions and map update providers.

The Roadside HAZMAT Security Detection and Mitigation (CVO11) market package is used to detect HAZMAT cargoes at the roadside, and correlate the detected operations with existing credentials to determine if a detected HAZMAT cargo is a permitted activity. If a non-permitted activity is detected, the Commercial Vehicle Check station may notify police.

The CV Driver Security Authentication (CVO12) market package authenticates a commercial vehicle driver based on information downloaded to the vehicle from the Fleet Management Center. If an unauthenticated driver is detected, a vehicle may be safely disabled by the Fleet Management Center, and the Fleet Management Center may notify police.

5.3.8.5 ITS Wide Area Alert

The ITS Wide Area Alert security area notifies the traveling public in emergency situations such as child abductions, severe weather watches and warnings, natural and human-caused disasters, military operations, and civil emergencies where lives and/or property are at stake. It utilizes ITS driver and traveler information technologies to immediately provide information and instructions to the traveling public, improving public safety and enlisting the public's help in some scenarios. The ITS technologies supplement and support other emergency and homeland security alert systems such as the Emergency Alert System (EAS).

When an emergency situation is reported and verified and the terms and conditions for system activation are satisfied, a designated agency broadcasts emergency information to traffic agencies, transit agencies, information service providers, the media, and other ITS systems that have driver or traveler information capabilities. The ITS systems, in turn, provide the alert information to the traveling public using ITS technologies such as Variable Message Signs, Highway Advisory Radios, in-vehicle displays, transit displays, 511 traveler information systems, and traveler information web sites. The service providers for this security area include the emergency management, homeland security, military and public safety agencies that issue the Wide Area Alert, the traffic, transit, and traveler information organizations that convey the information to the traveling public, and the traveling public itself.

In the physical architecture, the Emergency Management Subsystem represents the agency/system that broadcasts the emergency information to the ITS systems. This subsystem provides the alert information to the Traffic Management Subsystem, Transit Management Subsystem, Information Service Provider, Maintenance and Construction Management Subsystem, and Toll Administration Subsystem, which in turn provide the alert information to system operators and the traveling public.

The ITS Wide Area Alert security area centers around the Emergency Management subsystem and is best characterized in the National ITS Architecture by the Wide Area Alert (EM06) market package. The Wide Area Alert market package uses ITS driver and traveler information systems to alert the public in emergency situations such as child abductions, severe weather events, civil emergencies, and other situations that pose a threat to life and property. The alert includes information and instructions for transportation system operators and the traveling public, improving public safety and enlisting the public's help in some scenarios. The ITS technologies will supplement and support other emergency and homeland security alert systems such as the Emergency Alert System (EAS).

When an emergency situation is reported and verified and the terms and conditions for system activation are satisfied, a designated agency broadcasts emergency information to traffic agencies, transit agencies, information service providers, toll operators, and others that operate ITS systems. The ITS systems, in turn, provide the alert information to transportation system operators and the traveling public using ITS technologies such as dynamic message signs, highway advisory radios, in-vehicle displays, transit displays, 511 traveler information systems, and traveler information web sites.

5.3.8.6 Rail Security

The general area of Rail Security includes ITS functionality to monitor and secure trains, rail cars, fixed assets (track, wayside equipment and highway-rail intersections) and personnel. Rail Security focuses on freight rail (security aspects of passenger rail are covered under transit security). The current version of the National ITS Architecture addresses a subset of the overall area of rail security, specifically interfaces between rail entities and highway entities. These are the interfaces relating to highway rail intersections (HRI) and the interfaces from rail operations to traffic and emergency management functions of the architecture.

The primary security function associated with HRI is surveillance of the intersection, which is performed in the architecture by the Roadway subsystem. The market package that provides this function is ATMS14, Advanced Railroad Grade Crossing.

The interface between rail operations and the traffic management functions is expressed in the architecture as the interface between the Rail Operations terminator and the Traffic Management Subsystem and contains incident and advisory information. It is included in market packages ATMS13 (Standard Railroad Grade Crossing), ATMS14 (Advanced Railroad Grade Crossing), and ATMS15 (Railroad Operations Coordination).

The interface between rail operations and the emergency management function is expressed in the architecture as the interface between the Rail Operations terminator and the Emergency Management Subsystem. The market packages that address this interface are ATMS08 (Traffic Incident Management System), for normal incidents; EM08 (Disaster Response and Recovery), for disaster response; and EM09 (Evacuation and Reentry Management), for coordination during evacuations.

5.3.8.7 Transit Security

The area of transit security addresses passenger, facility, and asset security for passenger rail and bus transit systems. The area addresses surveillance and sensor monitoring of transit stations, stops, facilities, infrastructure, and vehicles. The surveillance includes both video and audio surveillance. The sensor monitoring includes threat sensors (e.g. chemical agent, toxic industrial chemical, biological, explosives, thermal, acoustic and radiological sensors), object detection sensors, motion or intrusion detection sensors, and infrastructure integrity sensors.

Transit-related systems also include analysis of sensor or surveillance outputs for possible threats and automatic notification of appropriate transit or public safety personnel to potential threats. The Transit Security area supports traveler or transit vehicle operator initiated alarms that are monitored by central dispatch or the local police. This area also includes a security management and control capability that not only provides detection, identification and notification of threats or incidents, but also allows the transit agency to take response measures such as remote vehicle disabling. In addition, this area also provides access control to transit vehicles, requiring positive operator identification before transit vehicles can be operated.

Another aspect of the Transit Security area of the National ITS Architecture is to provide emergency information to travelers using the transit system by visual (signs) or audio messages on-board the transit vehicle, at transit stops, or in transit facilities. Finally, the transit security area will interface with appropriate security agencies (e.g., the Transit Information Security Analysis Center) to assist in analysis of threats and to report threats.

The Transit Security area's key market package is Transit Security (APTS05). This market package includes six key interfaces.

- The first key interface is between the Transit Vehicle Subsystem and the Transit Management Subsystem for traveler or vehicle operator initiated alarms, vehicle disabling, and vehicle operator authentication.

- The second key interface is between the Transit Vehicle Subsystem and Emergency Management Subsystem (representing either a public safety agency or the public safety aspects of a transit agency e.g., transit police) for traveler or vehicle operator initiated alarms, surveillance, and sensor monitoring.

- The third key interface is between the Remote Traveler Support Subsystem (representing devices in public transit areas such as transit stations) and Emergency Management Subsystem for traveler initiated alarms, surveillance, and sensor monitoring.

- The fourth key interface is between the Security Monitoring Subsystem (representing devices in non-public transit areas such as transit yards) and Emergency Management Subsystem for surveillance and sensor monitoring.

- The fifth key interface is between the Transit Management Subsystem and Emergency Management Subsystem for sharing emergency information and coordinating incident response.

- The sixth key interface is between the Emergency Management Subsystem (representing either a public safety agency or the public safety aspects of a transit agency e.g., transit police and the Alert and Advisory Systems terminator for sharing of threat information or threat data for analysis.

5.3.8.8 Transportation Infrastructure Security

Transportation infrastructure can be monitored and protected by a broad array of ITS technologies. Transportation infrastructure security includes the monitoring of transportation infrastructure (e.g., bridges, tunnels and management centers) for potential threats using sensors and surveillance equipment. Threats to infrastructure can result from acts of nature (e.g., hurricanes, earthquakes), terrorist attacks or other incidents causing damage to the infrastructure (e.g., stray barge hitting a bridge support). Barrier and safeguard systems are used to preclude an incident, control access during and after an incident or mitigate impact of an incident.

The Emergency Management Subsystem monitors the transportation infrastructure. Information on threats is shared primarily with the Other EM, TMS, and MCMS subsystems but can also be shared with other subsystems. The Traffic Management Subsystem controls the barrier and safeguard equipment although Emergency Management can request deployment. The security of transportation infrastructure is covered primarily in the Transportation Infrastructure Protection (EM05) market package.

5.3.8.9 Traveler Security

The Traveler Security area is responsible for increasing the safety and security of travelers in public areas including public transit facilities, bicycle paths, bridges, tunnels, parking facilities and (major) intersections and other roadway features.

- There are four key market packages that represent the Traveler Security area.

- The Transit Security (APTS05) market package provides for traveler security through surveillance and sensor monitoring to warn of hazardous situations as well as allowing travelers to report emergencies.

- The Transportation Infrastructure Protection (EM05) market package includes the monitoring of transportation infrastructure (e.g., bridges, tunnels and management centers) for potential threats using sensors and surveillance equipment.

- The Wide-Area Alert (EM06) market package uses ITS driver and traveler information systems to alert the public in emergency situations that pose a threat to life and property.

- Finally, the Disaster Traveler Information (EM10) market package uses ITS to provide disaster-related traveler information to the general public, including evacuation and reentry information and other information (possibly responsive to specific traveler requests) concerning the operation of the transportation system during a disaster.

5.4 OPERATIONAL CONCEPTS

5.4.1 Operational Premise & Objectives

The discussion of a security and emergency response concept of operations in this document is somewhat unique in that ITS security functionality and operations is truly a subset of the more traditional transportation ITS functionality and operations. As noted in the User Needs discussion of this security supplement, there is a very wide range of security needs in relation to ITS in the SCAG region, and there is just as wide a potential range of operational concepts and details. This section takes a look at high level ITS security concept of operations, as it may be applied in two areas:

- Securing ITS systems and infrastructure, and
- Monitoring, identifying, responding to, and recovering from security and environmental infrastructure threats.

Both of these areas are derived directly from the National ITS Security Documentation, but this section looks to place these in context with the overall transportation operations relating to ITS. As the variation between specific system and project needs, objectives, and designs is substantial, this concept of operations is meant to serve as a starting point for considering security operational concepts in relation to transportation oriented ITS. For each ITS project with potential security related functions and needs, the specific operations and operations stakeholders should be identified, and security operations outlined and documented during system development, deployment, and/or upgrades.

Premise

The basic premise of security ITS operational concepts is to improve the efficiency and safety of the transportation component of emergency monitoring, response, and recovery. All security related objectives and operations concepts should be able to trace their origins back to this basic premise and answer the question of, "How will this functionality or operational process improve the monitoring, response, and/or recovery of the transportation network from potential terrorist, security, and/or environmental threats?"

Objectives

In support of the basic ITS security operational premise, are a series of basic operational objectives that should be supported by the system and the functional/operational processes being considered:

- Improved Coordination – There should be the potential for enhanced coordination internal to and amongst the operational stakeholders who will typically include a mix of personnel and agencies with transportation and security/enforcement related responsibilities.
- Improved Communications – Clear, reliable, and secure communications are key to any form of effective transportation security/emergency activity regardless if the communications are voice or data. Communications could be direct in terms of the ability of internal or multi-agency stakeholders communicating during an event, or it could relate to the planning and coordination prior to an event.

- Improved Responsiveness/Flexibility – Transportation security related systems and project should enhance the responsiveness of transportation security and infrastructure resources, as well as enhance the flexibility in terms of how these resources may be applied.

- Improved Efficiency – Finally, the systems and project should enhance the operational efficiency of the near- and long-term response to security and environmental threats to the transportation network not only by achieving the objectives above, but by allowing and supporting more appropriate and effective decisions to be made.

It should be noted that these objectives apply both to ITS projects that support long-range planning and preparation aspects of security, as well as the real-time monitoring, response, and recovery from actual threats.

Operations Stakeholders

It is traditional in a concept of operations to identify the specific stakeholders involved in the system/operations and their roles and responsibilities. In this specific circumstance, it is not possible to achieve that level of detail, as almost any conceivable agency and stakeholder could have an operations role relating to the wide range of ITS transportation security applications. Where specific ITS security projects are discussed in this document, more specific stakeholders have been identified, but some generalizations are noted in the table below.

Table 5-3 - Operations Stakeholders

Agency/Type of Agency	Operational Role(s)
SCAG	Planning, preparation, and facilitation in advance of events, and potential role as data clearing house and resource tracking prior, during, and following events.
Other Regional Agencies (Regional Associations of Governments, Port Authorities, etc.)	Similar to SCAG but with more specific geographic or operational areas of focus.
Individual Transportation Agencies (Caltrans, Transit Agencies, Cities, etc.)	Planning and practice prior to event, with both near-term transportation management and restoration activities during an event, and long-term recovery following an event.
Emergency Services Agencies (Law enforcement, fire, medical, etc.)	Planning, coordination, and practice prior to an event, with overall event management and coordination during and following an event with an emphasis on safety and security.
Federal/State Agencies (FEMA, FBI, National Guard, US DOT, etc.)	Overall notification of threat levels and types, as well as large-scale event management, response, and recovery.
Other Stakeholder (Private/Public)	Varies, although they are likely to be users of the transportation network which is stressed under the event with roles for coordination, event management, response, and recovery.

For each ITS security project that moves forward with planning and deployment, the specific operations stakeholders should be identified along with their respective roles and responsibilities from a security perspective in relation to the system in question. The individual roles and responsibilities of stakeholders are likely to vary significantly based on the type of threat/event, and the scale of that event.

Foundation for Operations

For specific concepts of operations, the existing and planned systems are discussed in some detail, however for the purposes of this architecture supplement it is more appropriate to discuss some crucial operational aspects that relate to the planning, development, and deployment of ITS security systems. These aspects form a foundation for the sound development of any system which serves security functions in an exclusive or supplemental manner.

- Preplanned Scenarios and Responses – For any ITS application to have effective use for security purposes it must be designed, developed, and modified/deployed in conjunction with a series of preplanned security scenarios and responses. Scenarios could range from a general threat which prompts the increased monitoring and application of security resources in order to better protect transportation infrastructure, to a full regional response to a massive incident which destroys a wide range of transportation infrastructure and resources. For each system, there should be a series of example scenarios and response situations that the system is proposed to support and/or address.

- Clear Stakeholder Roles & Responsibilities – For each system, the primary and secondary stakeholders should be defined, and the ownership and maintenance responsibilities of each major component of the system should be defined. This is particularly important in the case where some aspects of the system support shared functionality and operations. For the specific security related scenarios and responses discussed above, the manner in which each stakeholder will make use of and/or support the system should be identified.

- Integrated Communications – Most systems will require some form of integrated communications which may either be system specific or shared across multiple systems. It is important for security related ITS applications to understand and describe the operational issues related to the integrated communications in terms of reliability, capacity, survivability, and redundancy. Multiple methods of communications with fallback options should be considered for any system expected to respond during or post event.

- Common System Standards – The region is already well versed in the benefits and application of common standards for data, communications, and operations. Most ITS security applications rely on the use of shared system functionality, data, and resources which should be based on agreed to standards. Potential security related standards and their applicability is discussed at a high-level elsewhere in this document, but it is important to identify in any system specific concept of operations in the applicable standards being used and what functions (particularly shared functions) that they support.

- Integrated Resource Sharing – Beyond the simple application of and operations using national and regional standards, the integrated operation and sharing of resources must be addressed. This includes identifying which potential users and uses have priority over shared resource under particular scenarios. For example, the integrated use and sharing of transportation surveillance video can serve many functions at various levels of events and responses from identifying threats to infrastructure, to assessing/managing evacuations, to long-term management of transportation infrastructure and resources during recovery. Operational concepts should identify shared resources, by whom, and how they will be used.

- Creative and Flexible Application of ITS Resources – The one certainty about security and emergency situations is that they are uncertain. ITS systems and projects should seek to integrate operational and functional flexibility that leaves open the path for creative application and use of resources. Operational concepts relating to security applications of ITS should define the range of situations under which they system(s) would be used, as well as where operational flexibility is most desirable. This aspect of operations can best be defined through the coordinated and collective planning of the all of the identified stakeholders.

- Stakeholder Communications – Security situations and events of a major nature involving the transportation infrastructure can sometimes be infrequent or intermittent. This means that methods for on-going stakeholder communications involving ITS applications and their use in operations are essential. Ideally, applications and operations can be tried out and tested during practice and training situations which involve operations staff and enhance their level of familiarity with each others resources, data, and operational methods.

Each of these foundational aspects should be considered and applied when ITS security applications or the potential use of transportation ITS for security needs is considered. It should be highlighted that ITS is only a resource and a tool, and it is through the manner and methods that it is applied which achieve the desired objectives before, during, and following an event.

Operations Processes

As noted previously, it is advised that operational concepts and processes be identified for each specific security ITS application or system as they are developed and deployed. It is useful to highlight some high level security related processes relating to transportation ITS. These processes are most likely to be of use to transportation professionals and specialists in assessing what roles their systems or resources may have in terms of security applications.

Following the National ITS Security Documentation, two basic high level process flows were developed with stakeholders, process steps, and commentary included with each flow.

- **Figure 5- 1 -** Securing ITS basic process flow – Looks at high-level processes relating to access and data threats and security for ITS systems.

- **Figure 5- 2 -** Event security related process flow – Provides a high-level process description for basic monitoring, event identification, response, and recovery actions.

Review of these flows may prove helpful in developing more specific operational concepts and system functionality.

Figure 5-1 - Securing ITS Basic Process Flow

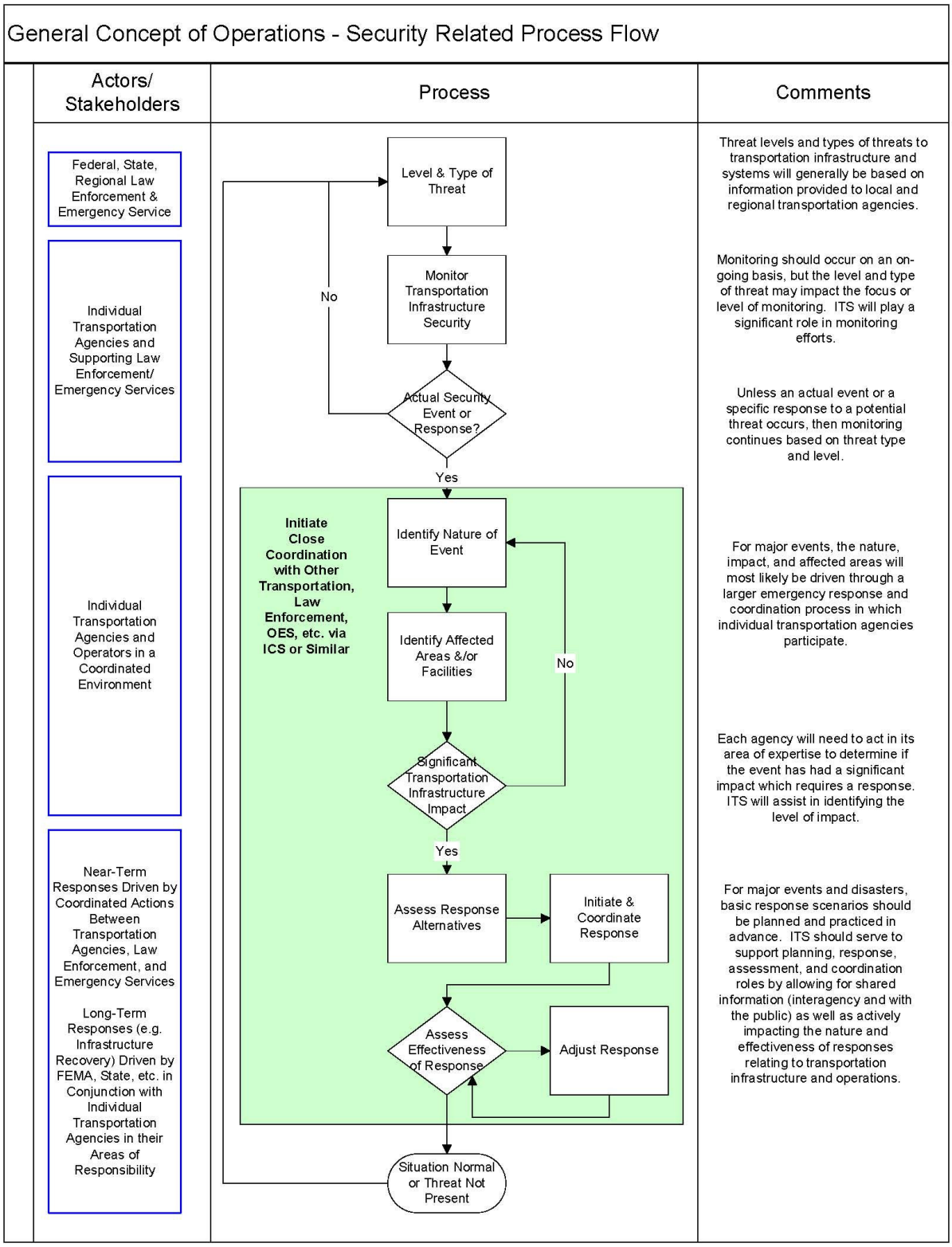
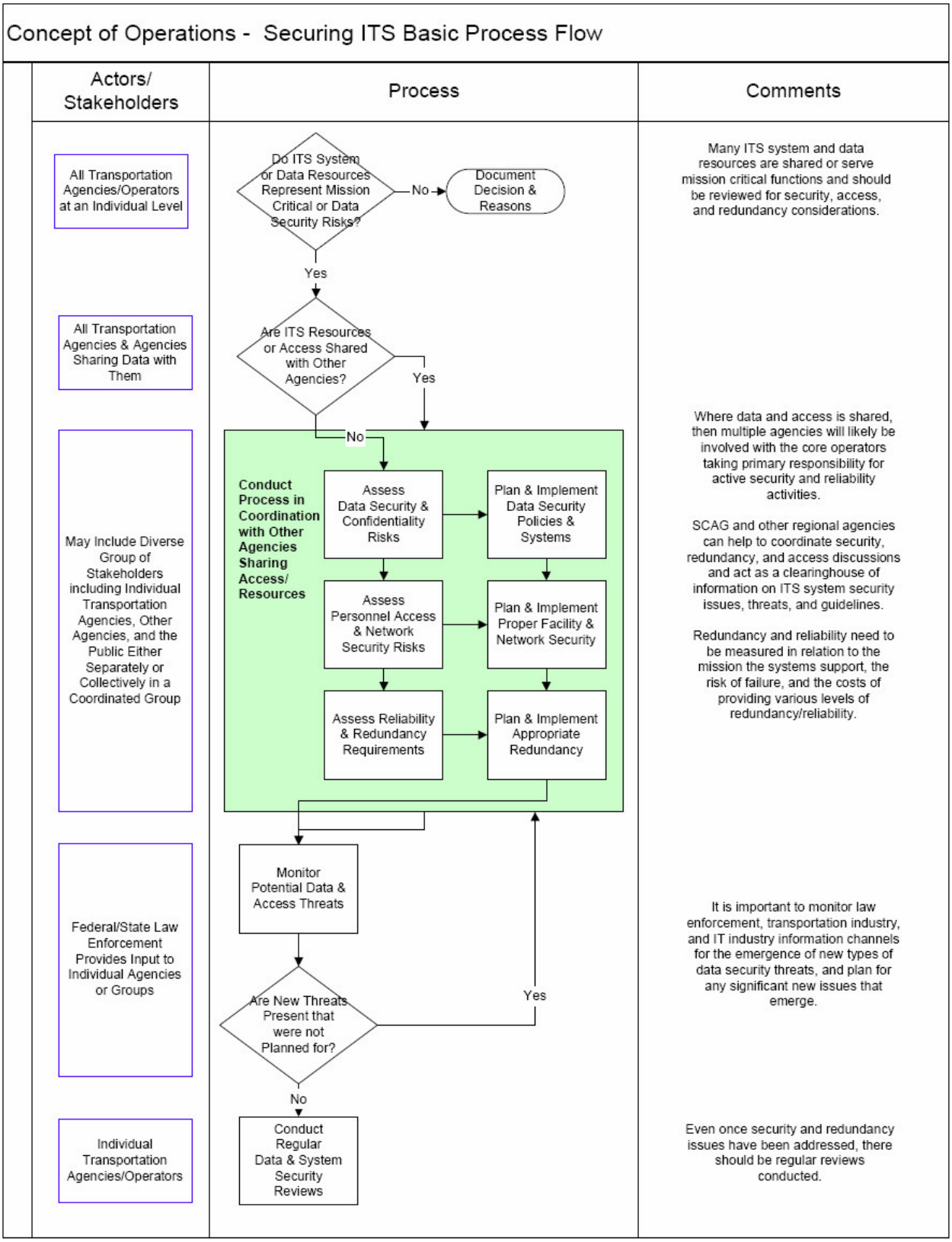


Figure 5-2 - Event Security Related Process Flow



6.0 FUNCTIONAL REQUIREMENTS

At this point the needs, services and market packages as well as the roles of the agencies have been defined in order to continue to developing ITS services. The next step is to list the tasks or activities that are performed by the systems themselves. This can be either the existing systems or those that are planned. Functional requirements can be high level in nature for a plan such this. For a project architecture leading to the procurement of a system, they will, of necessity, be very detailed. The following functional requirements are based on the supplemental security project list, found in Table 8-2.

1. Stakeholder: SCAG, MPO's, Transit Agencies, EMC's
   System: Regional Traveler Information Systems
   - The system(s) shall provide all and any information to users that will improve emergency notification and evacuation.
2. Stakeholder: SCAG, MPO's, Transit Agencies, EMC's
   System: Multi-agency Video Sharing and Distribution
   - The system(s) shall provide a common web enabled and secure clearinghouse for transportation video surveillance.
   - The system(s) shall provide the ability for images to be converted to a common selected and web capable format and then distributed through secure Internet and commercial wireless channels.
3. Stakeholder: SCAG, MPO's, Transit Agencies, EMC's, Local Jurisdictions
   System: Multi Transportation Agency Regional Interfaces
   - The Stakeholders shall develop special event management systems to coordinate seasonal traffic, emergency management, disaster operations, and wide area evacuation.
   - The system(s) shall enable the sharing of traffic information among the Southern California Caltrans districts and transportation agencies to support a regional control strategy.
   - The system(s) shall provide the ability to relinquish control of local agency signals to regional TMC during significant events or natural disasters to maintain regional traffic flows.
4. Stakeholder: SCAG
   System: ITS Data Systems Repository
   - The Stakeholder shall develop and implement a web-based regional education tool for transit agencies, transportation agencies, law enforcement, and emergency responders to provide relevant data, links, and contact information to enhance awareness and use of existing ITS related data including traffic information, emergency preparedness and response, and evacuation plans.
5. Stakeholder: Caltrans
   System: Interstate DOT Information Exchange
   - The system(s) shall provide the ability for Caltrans to coordinate and exchange data with Nevada and Arizona DOT for incident management, emergency response, and evacuation.

6. Stakeholder: LAWA, Airport Operators
   System: Airport Security Enhancement
   - The system(s) shall provide the ability for surveillance and sensor monitoring of airports, support facilities, infrastructure, and vehicles.

7. Stakeholder: Caltrans, MPO's, EMC's, Law Enforcement, Local Agencies, Transit Agencies
   System: Traffic Management Center and EMC Communications
   - The system(s) shall provide new and improve existing communication systems between traffic management centers (TMC's) and between TMC's and EMC's
   - The system(s) shall enable information exchange between all SCAG region Caltrans Districts
   - The system(s) shall enable information exchange between all SCAG region Caltrans Districts and other local agencies
   - The system(s) shall enable communications between Sherriff, CHP, Caltrans, Emergency Operations Centers, and local agencies during emergency events
   - The system(s) shall enable information exchange between and among transit agencies
   - The system(s) shall enable the sharing of traffic information and control among traffic management centers to support a regional control strategy, adding the communication links and integrated control strategies that enable integrated inter-jurisdictional traffic control.

8. Stakeholder: SCAG, Caltrans, TMC operators, EMC's
   System: Evacuation and Emergency Response Resource Management
   - The Stakeholders shall develop sub-regional focal points to refer all citizens during emergency events
   - The system shall provide the ability for Caltrans, EMC, and TMC's to track all response resources including maintenance and construction vehicles
   - The system shall provide a database of regional resources to monitor and track all response resources including vehicles and all assets that are necessary during an emergency event such as food, water, medical supplies, temporary shelters, etc.

9. Stakeholder: UP, BNSF, SCCRA, Amtrak
   System: Regional Rail Grade Crossing Security
   - The system(s) shall provide for the installation of sensors and surveillance to monitor at-grade rail crossings
   - The system(s) shall provide for the installation highway-railroad intersections with train detectors and advance warning systems
   - The system(s) shall provide the ability to link train detectors to traffic signal system and EMS dispatch
   - The system(s) shall provide for the installation ITS systems to direct vehicles to alternate routes at and in advance of blocked at-grade rail crossings on major arterials during train events (HAZMAT, derailment, train-vehicle collision)
   - The system(s) shall provide the ability to view and control CCTV through a Windows based system that is compatible with Intelligent Roadway / Rail Interface System (IR/RIS) program and sub-regional ATMS and ATIS.

10. Stakeholder: Ports, Law Enforcement, Emergency Responders, Commercial Vehicle Operators
    System: Common Format Hazardous or High Priority Vehicle Tracking
    - The system(s) shall provide a common format and standard for secure tracking of high priority safety concern vehicles or goods movement.
    - The system(s) shall enable information dissemination, including manifest information, through a common interface to emergency services, law enforcement, and other relevant agencies.
11. Stakeholder: Transit Agencies, EMC's, TMC Operators
    System: Emergency Notification of Transit Operators
    - The system(s) shall enable emergency information dissemination to transit operators via connections from EMC and TMC's
12. Stakeholder: SCAG, MPO's, Caltrans
    System: Regional Centralized Information Clearinghouse
    - The Stakeholders shall develop a regional forum for members of the transportation and emergency management communities to coordinate transportation and security initiatives, and to reach agreement on how to work more closely together during the decision notification process prior to and following an event.
    - The system shall extract information to enhance the effectiveness of agencies responsible for security preparedness and emergency response.
13. Stakeholder: SCAG
    System: Regional Integrated GIS Database
    - The Stakeholder shall develop a regional repository of GIS data for use by local agencies in emergency planning, and response, in a standardized format.
14. Stakeholder: Transit Agencies, SCCRA, Amtrak
    System: Transit Station Surveillance
    - The system(s) shall provide the ability for surveillance and sensor monitoring of transit stations, stops, facilities, infrastructure, and vehicles.
15. Stakeholder: UP, BNSF, SCCRA, Amtrak, EMC's
    System: Rail Infrastructure Security
    - The system(s) shall provide for the installation of ITS devices including communication backbone to monitor and secure trains, rail cars, fixed assets (tracks, wayside equipment), highway-rail intersections and personnel
    - The system shall provide interfaces to traffic and emergency management centers.
16. Stakeholder: Transportation Agencies, Local Jurisdictions
    System: Critical Transportation Infrastructure Surveillance & Information Dissemination
    - The system shall provide for the installation of ITS devices to implement traffic management systems and field elements on corridors with security concern or significances and or identified critical transportation infrastructure that are monitored and controlled by local agencies including CCTV, HAR, RWIS, DMS, vehicle detection stations, communications infrastructure, related to surveillance or information dissemination.

17. Stakeholder: Caltrans, MPO's
    System: Traffic Control & Management Systems
    - The system shall provide for the installation of ITS devices to implement traffic control and management systems to enhance emergency response and evacuation
    - The system shall provide centralized traffic control systems (TCS) to cities for signal monitoring and control, incident management, event management, transit coordination, ITS element control and provide connection to sub-regional TMC and adjacent cities.
    - The system shall provide Advanced Traffic Management System (ATMS) to detect and monitor signal status, identify traffic congestion and incidents, and display information through a fully integrated mapping function.
    - The system shall provide ATMS data sharing capability to coordinate operations with Caltrans and adjacent cities and provide arterial information to a traveler information system covering a larger area and multiple modes.
18. Stakeholder: Transit Agencies, Law Enforcement, Caltrans, MPO's, Emergency Responders, EMC's
    System: Emergency Event Communications Equipment
    - The system shall enable transit operators, law enforcement, transportation agencies, and emergency personnel to communicate with each other and EMC's during events resulting in a power outage (satellite phones, inter-regional radio system, etc.).
19. Stakeholder: Transit Agencies, Law Enforcement, Caltrans, MPO's, Emergency Responders, EMC's
    System: Emergency Response Communications Infrastructure
    - The system shall enable information sharing and communication between transit operators, law enforcement, transportation agencies, and emergency personnel during significant events or natural disasters.
    - The system shall provide the ability for local agencies to share data collected from local traffic management systems with other agencies, transit operators, emergency services, and law enforcement.
20. Stakeholder: UP, BNSF, EMC's, Emergency Responders
    System: Rail Location and Notification
    - The system shall provide the ability for rail operators (UP, BNSF) to notify public agencies in SCAG region of manifest data within 24hrs of receiving the data to allow first responders to properly respond in an emergency event.
    - The system shall provide installation of necessary ITS systems to share train location and ID data with public agencies.
21. Stakeholder: Local Jurisdictions
    System: Arterial Interfaces
    - The system shall provide the ability for sharing of real-time traffic conditions across county boundaries by local agencies.

22. Stakeholder: SCAG, MPO's, Caltrans
    System: Data Archive
    - The system shall provide regional archiving capability for long term planning to assist in preparation and response to emergency events.
23. Stakeholder: Ports
    System: Ports Security
    - The system shall provide installation of sensor and surveillance equipment to monitor all entrance points, critical infrastructure, perimeter security, and to track commercial vehicles/freight equipment, monitoring identities, monitoring freight equipment, and monitor commercial vehicles.
24. Stakeholder: I-5 JPA, Ports, Gateway COG
    System: Ports Traffic Information
    - The system shall provide for the installation of ITS systems to enhance existing Port traffic information dissemination
    - The system shall enable the ports to receive real-time traffic conditions from local agencies and disseminating real-time port information and traffic conditions to local agencies and to Commercial Vehicle Operators.
25. Stakeholder: SCRRA, MTA, Amtrak, EMC's
    System: Passenger Information System
    - The system shall provide the ability for all rail operators to disseminate real-time train information and emergency response and evacuation information to rail passengers via automated in-train audio and video devices, mobile electronic devices, and websites
26. Stakeholder: SCAG, EMC's
    System: Infrastructure Damage and Readiness Tracking System
    - The system shall provide the ability for a web enabled database and GIS infrastructure data tracking system.
    - The system shall provide the ability for information to be entered through mobile field devices and web enabled client terminals over radio/cell.
27. Stakeholder: SCAG, EMC's, Transportation Agencies, Law Enforcement, Emergency Services
    System: Security Threat and Guidance Clearinghouse
    - The Stakeholders shall develop a database and GIS resources with a security threat and response guidance expert system and information process.
    - The system shall allow for the receipt of generalized threat information from federal, state, and regional law enforcement and security agencies, and then translate it into meaningful areas of security focus for transportation agencies.
    - The system shall provide a series of guidelines and expert input to boil threats down into key focus areas and suggestions distributed to transportation agencies via e-mail, fax, and/or web.

7.0 REGIONNAL ARCHITECUTURE INFORMATION FLOWS

Although it is important to identify the region's ITS stakeholders and various systems, the primary purpose of the ITS Architecture is to identify the connectivity between ITS systems in the region, existing, planned, and future. The interconnect diagram illustrates high level relationship of the elements in the region. The customized market packages represent services that can be deployed as an integrated capability. The market package diagrams show the information flows between the subsystems and elements within the region that are most important to the operations. The interactions between these systems are an integral part of the overall architecture.

Above mentioned in the regional stakeholders section, there are over five hundred elements identified as part of the SCAG ITS Architecture, including safety and security stakeholders. These elements include cities, counties, transportation commissions, law enforcement, fire departments, international ports of entry, airports, seaports, offices of emergency management, and public service agencies. All (entities) would be essential to the existing and planned physical components that contribute to the regional intelligent transportation system. Under new federal rule, Regional ITS Architectures now incorporate safety and security stakeholders.

In the following, the regional ITS architecture outlines a framework for integrating systems that reap the benefits of sharing data. The National Architecture Interconnects and Information Flows is the point at which the framework for integration is identified and the potential flows are examined.

The interconnects are graphically illustrated using TurboArchitecture™ in a figure in Appendix D. The detailed flows are illustrated using TurboArchitecture™ for the sequencing of projects identified in Section 8.

8.0 PROJECT SEQUENCING[4]

The regional ITS architecture is implemented through many individual ITS projects that occur over years, or even decades. In this step of the Regional ITS architectural development, a sequence of ITS projects that will contribute to the integrated regional transportation system is identified. An ITS project is defined by FHWA as "Any project that in whole or in part funds the acquisition of technologies or systems of technologies that provide or significantly contribute to the provision of one or more ITS user services as defined in the National Architecture." Since these projects are regional in concept, they generally represent the highest stages of ITS development, i.e. Caltrans interfaces represent the integration of data exchange between the four (4) Caltrans District systems. They tend to represent the top level of sequencing of projects. Lower level projects are to be found in the County level architectures.

The FHWA Regional ITS Guidance Document also refers to project sequencing as representing consensus building about setting priorities that show how ITS projects can build one another. For this document, Stakeholder meetings and discussions were used to identify the projects listed below.

Table 8 1 - 2004 Architecture Project Sequencing contains the listing of projects from the 2004 Southern California Regional ITS Architecture by title, market package, Stakeholder(s), simple description, and the expected timing (S= short term, M=medium term, L=long term). This table has been supplemented with a reference system. "AP-1", and subsequent numbering, has been added to assist in referencing projects from the 2004 SCAG Regional ITS Architecture with "AP" being an acronym for "Architecture Project". The projects listed in this table were taken directly from Table 8-1: Project Sequencing, Page 8-2, of the Southern California Regional ITS Architecture, 2004. Security related architecture projects included in this security supplement are referred to as SAP-1, SAP being an acronym for "Security Architecture Project". These projects are listed in Table 8-2. All projects are listed irrespective of whether or not they will be funded through federal sources.

[4] This text for this section was taken in whole from the 2004 Southern California Regional ITS Architecture. However, Table 8-2 has been added to include the security related ITS projects related to this addendum.

Table 8-1 - 2004 Architecture Project Sequencing

Project Number	Project Title	Market Package(s)	Stakeholder(s)	Description	Timing
2004 AP-1[5]	Multi Caltrans Districts Interfaces	ATMS7: Regional Traffic Control	Caltrans	Sharing of traffic information among the Southern California Caltrans districts to support a regional control strategy.	M
2004 AP-2	Arterial Interfaces	ATMS7: Regional Traffic Control	Local Jurisdictions	Sharing of real-time traffic conditions across county boundaries by local agencies.	L
2004 AP-3	Data Archive	AD3: ITS Virtual Data Warehouse	Regional Partners	Provide for a regional archiving capability for long term planning.	L
2004 AP-4	Data Dictionary	Standards Development	Regional Partners	Develop and maintain a data dictionary for the region. The resulting output of the data dictionary will be standards that the region could use to promote consistency of data exchange. No market package is currently available now to describe this project. It might lead to the development of a new market package in Archived Data Management System	M/L
2004 AP-5	Ports Traffic Information	ATMS01: Network Surveillance	I-5 JPA/Ports	The Ports are currently planning to install Closed Circuit Television (CCTV) cameras, Changeable Message Signs (CMS), and gate queue detectors. These devices will allow the ports to disseminate real-time port information to commercial vehicle operators. The ports will be receiving real-time traffic conditions from local agencies.	M
2004 AP-6	Ports General Traffic Dissemination	CVO01: Fleet Administration	I-5 JPA/Ports	Disseminate general port information to the Commercial Vehicle Operators.	M
2004 AP-7	Upgraded Rail Fare System	APTS4: Transit Passenger and Fare Management	SCRRA	Includes future capital projects entailing the following: • Ticket vending machine and validator purchase/upgrade	M
2004 AP-8	Upgraded Passenger Information system	APTS4: Transit Passenger and Fare	SCRRA	Includes future capital projects entailing the following:	M

[5] AP-1, and subsequent numbering, has been added to assist in referencing projects from the 2004 SCAG Regional ITS Architecture. "AP" is an acronym for "Architecture Project". The projects listed in this table were taken directly from Table 8-1: Project Sequencing, Page 8-2, of the Southern California Regional ITS Architecture, 2004. Security related architecture projects included in Table 8-2 will be referred to as SAP-1, SAP being an acronym for "Security Architecture Project".

Project Number	Project Title	Market Package(s)	Stakeholder(s)	Description	Timing
		Management		• Electronic passenger information system	
2004 AP-9	Rail Sealed Corridor	ATMS 14: Advanced Railroad Grade Crossing	SCRRA	Various alternatives will be studied including quad gates for the best line protection to prevent drivers from penetrating the line as trains approach and enhance safety. The first priority locations are the Antelope Valley Line and Ventura County Line. These segments are also within the California High Speed Rail Corridor	S
2004 AP-10	Quad Gate Synchronization	ATMS 14: Advanced Railroad Grade Crossing	SCRRA	Investigate alternate means of clearing the crossing by detecting vehicles that are still in the crossing as the first barrier is lowered and synchronize actions with traffic signal systems in the vicinity	S
2004 AP-11	Rail Fiber Communication	ATMS 15: Railroad Operations Coordination	SCRRA	A fiber communication backbone is gradually being installed throughout the system to enable both voice and data transmission linking to central dispatch in Pomona	S/M
2004 AP-12	Rail Camera Surveillance	ATMS 1: Network Surveillance ATMS 15: Railroad Operations Coordination	SCRRA	Camera to be installed at Union station using a Homeland Security grant.	S/M
2004 AP-13	GPS Train Location System	ATMS 15: Railroad Operations Coordination	SCRRA	Project is underway and will be on-going for some time. The completion of the fiber communication is of importance. Human interpretation of information remains of importance in understanding train delays before posting of information. There is no fully automated on-time performance system.	S
2004 AP-14	Rail Information Dissemination	ATMS 6: Traffic Information Dissemination	SCRRA	Future real-time information projects including PDAs, e-mail and pagers, displays in trains. The current website has only static displays.	L
2004 AP-15	Rail Ticket Vending Machines (TVMS) & Validation Equipment	APTS 4: Transit Passenger and Fare Management	SCRRA	Future upgraded systems will take multiple media for inter-operability including Metro's Universal Fare System (UFS).	L
2004 AP-16	Rail Automated	APTS 4: Transit Passenger and Fare	SCRRA	These sub-systems would be capable of monitoring all boarding and alighting and down loading information for	L

Project Number	Project Title	Market Package(s)	Stakeholder(s)	Description	Timing
	Passenger Counters	Management		central processing.	
2004 AP-17	Parking and Electronic Signage at Metrolink Stations	ATMS 15: Railroad Operations Coordination	SCRRA	Pursuing funding to support this project.	L
2004 AP-18	Rail Automated Maintenance Support	APTS 6: Transit Maintenance	SCRRA	Long-term goal as funding becomes available.	L
2004 AP-19	Rail Data Archiving	AD 2: ITS Data Warehouse	SCRRA	Long-term, electronic collection and delivery of Section XV data	L
2004 AP-20	Emergency Management / Security Region Wide Integration	To be determined	Regional Partners	A study under planning to examine the components of integration including concept of operation, roles and responsibilities, functional requirements. To arrive at a regional architecture for the topic plus the identification of the projects.	L
2004 AP-21	Regional Traveler Information	ATIS 1:Broadcast Traveler Information ATIS 2: Interactive Traveler Information	Regional Partners	A general project category that covers potential multi-agency initiatives to increase integrated dissemination of traveler information as widely as possible throughout the Southern California Region.	S/M

Table 8-2 - 2008 Security ITS Project Sequencing

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-16	Regional Traveler Information for Evacuation Routing and Emergency Diversion	• EM09 Evacuation and Reentry Management • EM10 Disaster Traveler Information	SCAG, MPO's, Transit Agencies, EMC's[7]	Based on 2004 AP-21[8] This project should provide the ability to implement a multi-jurisdictional Advanced Traveler Information System (ATIS) to collect, process, validate, and disseminate both pre-trip and en route real-time information to public agencies, private stakeholders, and the public including: • Emergency and evacuation information regionally to inform travelers of an emergency event, affected areas, and evacuation instructions • Freeway/arterial congestion, video images, and links to alternative transportation services via web page(s) • Interstate/inter-region traveler information covering a wide area (targeted to CVO) • Supporting the MATIS system.	S/M
2008 SAP-2	Multi-agency Video Sharing and Distribution	• ATIS06 – Transportation Operations Data Sharing	SCAG, MPO's, Transit Agencies, EMC's	Establish a common web enabled and secure clearing house for transportation video surveillance for use by multiple transportation and security agencies for security and event preparation, response, and evacuation. Provide the ability for images to be converted to a common selected and web capable format and then distributed through secure Internet and commercial wireless channels.	M

[6] SAP is an acronym for "Security Architecture Project".
[7] EMC is an acronym for "Emergency Management Center" that includes Office of Emergency Services (OES), Emergency Operation Center (EOC), and all facilities of this type.
[8] 2004 AP-21 refers to a Southern California Regional ITS Architecture project. To assist in referencing these projects, a numbering system was created. "AP" is an acronym for "Architecture Project". Please see Table 8-1 in this report for the list of projects in the 2004 Southern California Regional ITS Architecture.

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-3	Multi Transportation Agency Regional Interfaces	• ATMS03 – Surface Street Control • ATMS07 – Regional Traffic Management • ATMS08 – Traffic Incident Management System • EM08 – Disaster Response and Recovery • EM09 – Evacuation and Reentry Management	Caltrans, SCAG, MPO's, Transit Agencies, EMC's, Local Agencies	Based on 2004 AP-1, AP-2 Develop special event management systems to coordinate seasonal traffic, emergency management, disaster operations, and wide area evacuation by sharing traffic information among the Southern California Caltrans districts and transportation agencies to support a regional control strategy. Provide the ability to relinquish control of local agency signals to regional TMC during significant events or natural disasters to maintain regional traffic flows.	M/L
2008 SAP-4	ITS Data Systems Repository	• AD2 – ITS Data Warehouse	SCAG, MPO's, Caltrans	Develop and implement a web-based regional education tool for transit agencies, transportation agencies, law enforcement, and emergency responders to provide relevant data, links, and contact information to enhance awareness and use of existing ITS related data including traffic information, emergency preparedness and response, and evacuation plans.	S
2008 SAP-5	Interstate DOT Information Exchange	• ATMS07 – Regional Traffic Management	Caltrans, NDOT, AZDOT	Provide the ability for Caltrans to coordinate and exchange data with Nevada and Arizona DOT for incident management, emergency response, and evacuation.	M
2008 SAP-6	Airport Security Enhancement	• EM05 – Transportation Infrastructure Protection • APTS05 – Transit Security	LAWA, Airport Operators	Provide the ability for surveillance and sensor monitoring of airports, support facilities, infrastructure, and vehicles. The surveillance includes both video and audio surveillance. The sensor monitoring includes threat sensors (e.g. chemical agent, toxic industrial chemical, biological, explosives, thermal, acoustic and radiological sensors), object detection sensors, motion or intrusion detection sensors, and infrastructure integrity sensors.	S

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-7	Traffic Management Center and EMC Communications	• ATMS07 – Regional Traffic Management • APTS07 – Multi-modal Coordination • ATMS03 – Surface Street Control • ATMS04 – Freeway Control • EM09 – Evacuation and Reentry Management • ATIS06 – Transportation Operations Data Sharing	Caltrans, MPO's, EMC's, Law Enforcement, Local Agencies, Transit Agencies	Based on 2004 AP-1 This project will utilize ITS to develop new and improve existing communication systems between traffic management centers (TMC's) and between TMC's and EMC's through: • Improving information exchange between all SCAG region Caltrans Districts • Improving information exchange between all SCAG region Caltrans Districts and other local agencies • Improving communications between Sherriff, CHP, Caltrans, Emergency Operations Centers, and local agencies during emergency events • Improving information exchange between and among transit agencies • Sharing of traffic information and control among traffic management centers to support a regional control strategy, adding the communication links and integrated control strategies that enable integrated inter-jurisdictional traffic control	M/L
2008 SAP-8	Evacuation and Emergency Response Resource Management	• AD2 – ITS Data Warehouse • EM01 – Emergency Call-Taking and Dispatch • EM08 – Disaster Response and Recovery • EM09 – Evacuation and Reentry Management • APTS01 – Transit Vehicle Tracking	SCAG, Caltrans, TMC operators, EMC's	Utilized ITS to facilitate enhanced regional evacuation and emergency response by: • Developing sub-regional focal points to refer all citizens during emergency events • Providing the ability for Caltrans, EMC, and TMC's to track all response resources including maintenance and construction vehicles • Developing a database of regional resources to monitor and track all response resources including vehicles and all assets that are necessary during an emergency event such as food, water, medical supplies, temporary shelters, etc.	M

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-9	Regional Rail Grade Crossing Security	• ATMS08 – Traffic Incident Management System • ATMS13 – Standard Railroad Grade Crossing • ATMS14 – Advanced Railroad Grade Crossing • ATMS15 – Railroad Operations Coordination	UP, BNSF, SCCRA, Amtrak	Based on 2004 AP-9, AP-10, AP-11, AP-12 Improve rail grade crossing security and response to emergency events by: • Using sensors and surveillance to monitor at-grade rail crossings • Improving highway-railroad intersections with train detectors, advance warning systems and link train detectors to traffic signal system and EMS dispatch • Utilizing ITS elements to direct vehicles to alternate routes at and in advance of blocked at-grade rail crossings on major arterials during train events (HAZMAT, derailment, train-vehicle collision) • Providing the ability to view and control CCTV through a Windows based system that is compatible with Intelligent Roadway / Rail Interface System (IR/RIS) program and sub-regional ATMS and ATIS.	M

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-10	Common Format Hazardous or High Priority Vehicle Tracking	• CVO01 – Fleet Administration • CVO02 – Freight Administration • CVO03 – Electronic Clearance • CVO04 – CV Administrative Process • CVO07 – Roadside CVO Safety • CVO08 – On-board CVO and Freight Safety and Security • CVO10 – HAZMAT Management • CVO11 – Roadside HAZMAT Security Detection and Mitigation • CVO12 – CV Driver Security Authentication • CVO13 – Freight Assignment Tracking	Ports, Law Enforcement, Emergency Responders, Commercial Vehicle Operators	Provide a common format and standard for secure tracking of high priority safety concern vehicles or goods movement. Provide information through a common interface to emergency services, law enforcement, and other relevant agencies. Include manifest information for proper response efforts.	S/M
2008 SAP-11	Emergency Notification of Transit Operators	• ATMS08 – Traffic Incident Management System	Transit Agencies, EMC's, TMC Operators	Enable emergency information dissemination to transit operators via connections from EMC and TMC's	S/M

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-12	Regional Centralized Information Clearinghouse		SCAG, MPO's, Caltrans	Based on 2004 AP-3 Provide a central information clearinghouse by: • Developing proactive transportation security strategies that support economic vitality in the region; • Enhancing the effectiveness of agencies responsible for security preparedness and emergency response; • Ensuring that regional transportation technology investments meet the needs of emergency responders through interoperable, robust, and strategically redundant ITS and communications infrastructure; • Providing a regional forum for members of the transportation and emergency management communities to coordinate transportation and security initiatives, and to reach agreement on how to work more closely together during the decision notification process prior to and following an event; • Updating the regional ITS Architecture and associated County architectures. describing specific systems interoperability requirements to support regional safety and security objectives; and • Satisfying SAFETEA-LU requirements for regional transportation planning to incorporate security considerations.	S
2008 SAP-13	Regional Integrated GIS Database	• AD2 – ITS Data Warehouse	SCAG	Based on 2004 AP-3 SCAG shall offer a regional repository of GIS data for use by local agencies in emergency planning, and response, in a standardized format.	M/L

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-14	Transit Station Surveillance	• APTS05 – Transit Security	Transit Agencies, SCCRA, Amtrak	Based on 2004 AP-12 Provide the ability for surveillance and sensor monitoring of transit stations, stops, facilities, infrastructure, and vehicles. The surveillance includes both video and audio surveillance. The sensor monitoring includes threat sensors (e.g. chemical agent, toxic industrial chemical, biological, explosives, thermal, acoustic and radiological sensors), object detection sensors, motion or intrusion detection sensors, and infrastructure integrity sensors.	S
2008 SAP-15	Rail Infrastructure Security	• ATMS06 – Traffic Incident Management System • ATMS13 – Standard Railroad Grade Crossing • EM05 – Transportation Infrastructure Protection • PTS05 – Transit Security	UP, BNSF, SCCRA, Amtrak, EMC's	Based on 2004 AP-11 Install ITS devices including communication backbone to monitor and secure trains, rail cars, fixed assets (tracks, wayside equipment), highway-rail intersections and personnel with interfaces to traffic and emergency management centers.	S
2008 SAP-16	Critical Transportation Infrastructure Surveillance & Information Dissemination	• EM05 – Transportation Infrastructure Protection • ATMS01 – Network Surveillance • ATMS06 – Traffic Information Dissemination • MC03 – Road Weather Data Collection	Transportation Agencies, Local Agencies	Implement traffic management systems and field elements on corridors with security concern or significances and or identified critical transportation infrastructure that are monitored and controlled by local agencies including CCTV, HAR, RWIS, DMS, vehicle detection stations, communications infrastructure, related to surveillance or information dissemination.	S/M

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-17	Traffic Control & Management Systems	• ATIS01 – Broadcast Traveler Information • ATMS07 – Regional Traffic Management • ATMS03 – Surface Street Control • ATMS08 – Traffic Incident Management System • EM09 – Evacuation and Reentry Management • EM10 – Disaster Traveler Information	Caltrans, MPO's	Based on 2004 AP-2 Implement traffic control and management systems to enhance emergency response and evacuation including: • Providing centralized traffic control systems (TCS) to cities for signal monitoring and control, incident management, event management, transit coordination, ITS element control and provide connection to sub-regional TMC and adjacent cities. • Implement an Advanced Traffic Management System (ATMS) to detect and monitor signal status, identify traffic congestion and incidents, and display information through a fully integrated mapping function. • Provide ATMS data sharing capability to coordinate operations with Caltrans and adjacent cities and provide arterial information to a traveler information system covering a larger area and multiple modes.	L
2008 SAP-18	Emergency Event Communications Equipment		Transit Agencies, Law Enforcement, Caltrans, MPO's, Emergency Responders, EMC's	Provide the ability for transit operators, law enforcement, transportation agencies, and emergency personnel to communicate with each other and EMC's during events resulting in a power outage (satellite phones, inter-regional radio system, etc.).	S
2008 SAP-19	Emergency Response Communications Infrastructure	• EM08 – Disaster Response and Management • ATMS08 – Traffic Incident Management System	Transit Agencies, Law Enforcement, Caltrans, MPO's, Emergency Responders, EMC's	Improve information sharing and communication between transit operators, law enforcement, transportation agencies, and emergency personnel during significant events or natural disasters. Provide the ability for local agencies to share data collected from local traffic management systems with other agencies, transit operators, emergency services, and law enforcement.	M/L

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-20	Rail Location and Notification	• ATMS08 – Traffic Incident Management System	UP, BNSF, EMC's, Emergency Responders	Based on 2004 AP-13 Provide the ability for rail operators (UP, BNSF) to notify public agencies in SCAG region of manifest data within 24hrs of receiving the data to allow first responders to properly respond in an emergency event. Implement necessary ITS elements to share train location and ID data with public agencies.	S/M
2008 SAP-21	Arterial Interfaces	• ATMS07 – Regional Traffic Management • ATMS08 – Traffic Incident Management System • EM08 – Disaster Response and Recovery • EM09 – Evacuation and Reentry Management	Local Agencies	Based on 2004 AP-2 Develop special event management systems to coordinate seasonal traffic, emergency management, disaster operations, and wide area evacuation by sharing of real-time traffic conditions across county boundaries by local agencies.	L
2008 SAP-22	Data Archive	• AD2 – ITS Data Warehouse	SCAG, MPO's, Caltrans	Based on 2004 AP-3 Provide for a regional archiving capability for long term planning to assist in preparation and response to emergency events.	M/L
2008 SAP-23	Ports Security	• EM05 – Transportation Infrastructure Protection • CVO03 – Electronic Clearance • CVO07 – Roadside CVO Safety • CVO11 – Roadside HAZMAT Security Detection and Mitigation	Ports	Based on 2004 AP-5 Enhance existing Port security systems through sensor and surveillance equipment to monitor all entrance points, critical infrastructure, perimeter security, and to track commercial vehicles/freight equipment, monitoring identities, monitoring freight equipment, and monitor commercial vehicles.	S

Project Number	Project Name	Market Package(s)	Stakeholder(s)	Project Description	Timing
2008 SAP-24	Ports Traffic Information	• ATMS01 – Network Surveillance • APTS06 – Traffic Information Dissemination	I-5 JPA/Ports/ Gateway COG	Based on 2004 AP-6 Enhance existing Port traffic information dissemination through Closed Circuit Television (CCTV) cameras, Changeable Message Signs (CMS), and gate queue detectors. Enable the ports to receive real-time traffic conditions from local agencies and disseminating real-time port information and traffic conditions to local agencies and to Commercial Vehicle Operators.	M
2008 SAP-25	Passenger Information System	• APTS08 – Transit Traveler Information	SCRRA, MTA, Amtrak, EMC's	Based on 2004 AP-8, AP-14 Provide the ability for all rail operators to disseminate real-time train information and emergency response and evacuation information to rail passengers via automated in-train audio and video devices, mobile electronic devices, and websites.	M
2008 SAP-26	Infrastructure Damage and Readiness Tracking System	• AD2 – ITS Data Warehouse • EM07 – Early Warning System • EM08 Disaster Response and Recovery	SCAG, EMC's	Deploy a web enabled database and GIS infrastructure data tracking system. The system would provide a ready multi-agency/multi-modal method for identifying high level damage, required repairs, and readiness of transportation infrastructure following major events. The system will allow information to be entered through mobile field devices and web enabled client terminals over radio/cell.	M
2008 SAP-27	Security Threat and Guidance Clearinghouse	• AD2 – ITS Data Warehouse • EM07 – Early Warning System	SCAG, EMC's, Transportation Agencies, Law Enforcement, Emergency Services	Develop a SCAG database and GIS resources with a security threat and response guidance expert system and information process. Allow for the receipt of generalized threat information from federal, state, and regional law enforcement and security agencies, and then translate it into meaningful areas of security focus for transportation agencies. Include a combination of upfront threat identification and risk classification to allow for generalized threats as an input. Provide a series of guidelines and expert input to boil threats down into key focus areas and suggestions distributed to transportation agencies via e-mail, fax, and/or web.	M

9.0 IDENTIFICATION OF REQUIRED STANDARDS

9.1 SECURITY RELATED STANDARDS AND CONSIDERATIONS

The application of specific security considerations to regional architectures is relatively new, and represents a response to the threat environment posed to our transportation infrastructure. The standing SCAG Regional ITS System Architecture already addresses and highlights relevant standards for transportation and related systems. However, it is important to consider the relationship these and emerging standards have in light of the application of specific security considerations to the regional architecture. This section highlights standards and related considerations drawing largely on documentation prepared for the National ITS Architecture, including "National ITS Architecture Security," prepared by the Architecture Development Team (May 2007) and available for download at: http://www.iteris.com/itsarch/documents/security/security.pdf

There are two levels at which security standards and potential application of these standards should be considered:

1. Application of confidentiality and data protection stemming from or used by transportation systems – While not specifically driven by individual technical standards, the National ITS Architecture Security documentation does provide some guidance on areas where data security and confidentiality may be a concern from a security perspective. System and data security can be a function of many factors including network access, network security, data standards, data encryption, and many other layers of software and physical security. The information in this section seeks to highlight some areas of potentially sensitive data, and stakeholders deploying systems with potential security applications or links to potential security applications are asked to consider both physical and data security in light of potentially increasing data and access security issues. In establishing regional data standards for the areas highlighted in this section, stakeholders should consider some of the guidance in this section and the National ITS Architecture Security documentation.

2. Technical standards which may be of particular interest in light of security related applications of transportation systems – Most of these can be applied for general transportation systems standards applications, but some are highlighted because they seem particularly relevant to the security needs and applications of transportation systems. Links to more information on each of the standards is provided for additional reference and updates. It should be noted that the standards highlighted here should be considered as a supplement and not a replacement for the standards discussion in the adopted SCAG Regional ITS Architecture.

9.2 GENERAL DATA AND SYSTEMS SECURITY CONSIDERATIONS

The following areas of potential transportation systems deployment should prompt stakeholders to give additional consideration to physical and data access security, and seek to consider security in their development and application of regional data and interface standards:

1. Archived Data Management: sensitive information in the archive requires significant security safeguards. In many cases, the critical objectives for data archives are data integrity, accuracy and reliability; archives are used to measure the performance of the transportation system and provide data to support operations and planning. Archive entries should be reviewed to ensure security is consistent with the sensitivity of the data.

2. Commercial Vehicle Administration: handling of personal and business sensitive information, such as financial data, requires high confidentiality to safeguard the information. Additionally, the information should be available to ensure safe and efficient transportation of cargo with a high level of integrity to prevent unauthorized clearance.

3. Commercial Vehicle Check: handling of personal and business sensitive information requiring high confidentiality to safeguard the information and support electronic screening. Additionally, the information should be available to support safety inspections and electronic screening for safe and efficient commercial vehicle checking.

4. Commercial Vehicle Subsystem: contains screening and safety data to support roadside electronic screening. The handling of personal and business sensitive information (including cargo) about the commercial vehicle needs to have a relatively high degree of confidentiality to safeguard the information.

5. Roadway: the Roadway System performs a broad range of roadway network monitoring and control services that have particular security considerations based on implementation. Traffic signal systems, gates and barriers are safety-critical systems that can directly endanger motorists if improperly operated. Security services should be established such that the systems operated with very high levels of integrity and availability and system operation degrades in a fail-safe manner. The information associated with the operation of these systems is no confidential and typically does not require special measures to protect it from disclosure.

6. Security Monitoring: the subsystem includes surveillance and sensor equipment used to provide enhanced security and safety for transportation facilities or infrastructure. Improper operation of these systems can directly endanger motorists requiring security services to be established such that these systems operate with very high levels of integrity and availability and system operation degrades in a fail-safe manner. The information associated with operation of these systems is confidential and typically will need special measures to protect it from disclosure.

9.3 HIGHLIGHTED STANDARDS WITH RELEVANT SECURITY APPLICATIONS

Some key market packages, particularly those related to personal security and surveillance, have greater potential for security applications, even if they are initially or primarily deployed for transportation systems management purposes. Highlighted market packages and related standards are listed below for reference purposes. This standards information is meant to serve as a supplement to the SCAG Regional ITS System Architecture and the other regional ITS architectures, and not as a replacement. Deployment of systems in these areas should particularly consider the application of accepted or open standards in

order to allow for future security system integration and application, even if initial deployment of these systems is specifically for transportation needs only.

ATMS01 Network Surveillance (Market Package)

Available: http://www.iteris.com/itsarch/html/mp/mpatms01.htm

Traffic images – high fidelity, real-time traffic images suitable for surveillance monitoring by the operator or for use in machine vision applications.

- NTCIP C2F: Center-to-Field Standards Group
- NTCIP 1201: Global Object Definitions
- NTCIP 1205: Object Definitions for Closed Circuit Television (CCTV) Camera Control
- NTCIP 1208: Global Definitions for Closed Circuit Television (CCTV) Switching

Video surveillance control – information used to configure and control video surveillance systems

- NTCIP C2F: Center-to-Field Standards Group
- NTCIP 1201: Global Object Definitions
- NTCIP 1205: Object Definitions for Closed Circuit Television (CCTV) Camera Control
- NTCIP 1208: Global Definitions for Closed Circuit Television (CCTV) Switching

Transit Communications Standards Development Category

Available: http://www.iteris.com/itsarch/html/standard/transitstdscat.htm

Alerts and advisories – assessments, advisories, and alerts. Provides supporting descriptive detail on incidents, threats, and vulnerabilities to increase preparedness and support effective response to threats against the surface transportation system.

Candidate for future standardization

APTS05 Transit Security (Market Package)

Available: http://www.iteris.com/itsarch/html/mp/mpapts05.htm

Provides for the physical security of transit passenger and transit vehicle operators using on-board equipment including surveillance, sensor, and alarms.

Secure area surveillance control – information used to configure and control audio and video surveillance systems used for transportation infrastructure security in secure areas.

- NTCIP C2F: Center-to-Field Standards Group
- NTCIP 1201: Global Object Definitions
- NTCIP 1205: Object Definitions for Closed Circuit Television (CCTV) Camera Control
- NTCIP 1208: Global Definitions for Closed Circuit Television (CCTV) Switching

Secure area surveillance data – data collected from surveillance systems used to monitor secure areas. Includes video, audio, processed surveillance data, equipment operational status, and alarm indicators when a thread has been detected.

- NTCIP C2F: Center-to-Field Standards Group
- NTCIP 1201: Global Object Definitions
- NTCIP 1205: Object Definitions for Closed Circuit Television (CCTV) Camera Control
- NTCIP 1208: Global Definitions for Closed Circuit Television (CCTV) Switching

Incident report – of an identified incident including incident location, type, severity and other information necessary to initiate an appropriate incident response

IEEE IM: Incident Management Standards Group

NTCIP C2C: NTCIP Center-to-Center Standards Group

Data Collection and Monitoring Control

Available: http://www.iteris.com/itsarch/html/af/af402.htm

Data collection and monitoring system - information used to configure and control data collection and monitoring systems

- NTCIP C2F: NTCIP Center-to-Center Standards Group
- NTCIP 1201: Global Object Definitions
- NTCIP 1204: Object Definitions for Environment Sensor Stations (ESS)
- NTCIP 1206: Object Definitions for Data Collection and Monitoring (DCM) Devices
- NTCIP 1209: Data Element Definitions for Transportation Sensor Systems (TSS)

Remote Surveillance Control

Available: http://www.iteris.com/itsarch/html/af/af174.htm

Remote surveillance control – commands used to remotely operate another center's sensors or surveillance equipment so that roadside surveillance assets can be shared by more than one agency. (For Traffic Management)

- NTCIP C2C: NTCIP Center-to-Center Standards Group
- ITE TMDD 2.1: Traffic Management Data Dictionary and Message Sets for External TMC Communication (TMDD and MS/ETMCC)

10.0 ARCHITECTURE MAINTENANCE

A discussion on the approach to maintaining the Regional ITS Architectures is a required element for each of the documents. The intent of this requirement is to promote the following:

- Use of the architectures;
- Maintenance of Stakeholder dialogue and understanding;
- Support for seeking funding;
- Support for project implementation;
- Progression of regional integration;
- Support for updates to the documentation; and
- Communication of updates, revisions and changes to the MPO.

Since the history of developing the deployment of ITS in Southern California varies greatly from county to county (reflecting different levels of maturity) it is to be expected that different approaches to organizing maintenance will also be adopted. This will be no different with the addition of the security elements of the architecture. The following is an overview of the approaches being adopted by the six counties. It should be noted that while tri-annual updates to coordinate with the RTIP process will be required by all counties, interim submission of changes are also facilitated. In the final phase of this Southern California Regional Architecture update project a maintenance plan will be followed that relies on the outlined procedures for when changes are made. The intent is that these procedures be simple, flexible and easy to follow and allow the architecture documents to be modified to reflect both political and technological developments.

10.1 LOS ANGELES COUNTY

There are two linked efforts in Los Angeles County. Los Angeles is the only county that at this point has developed a recognized Regional network for multi-agency, multi-system data exchanges. This is referred to as the Regional Integration of ITS (RIITS) network. The Metropolitan Transportation Authority (Metro) has established a formal configuration management process for the network whose voting membership is all agencies that contribute source data. The Los Angeles Regional ITS Architecture is one of the documents managed by the configuration management process and will be maintained with support from the RIITS administrator which is staffed by the Metro. In addition, the County of Los Angeles is developing a very large project called the Information Exchange Network (IEN) which when fully deployed will support the exchange of arterial based data across the county. An interface between the IEN and the RIITS network is part of the future vision. The IEN will also create a configuration management team drawing from all of the participating traffic forum members. Coordination between the two sets of activities will be maintained through Metro participating staff. In

addition, the Metro has adopted a policy that will require all ITS projects funded by any source administered by the Metro to be consistent with the Los Angeles Regional ITS Architecture and to utilize systems engineering and standards as required. The Metro will have lead responsibility for forwarding updated information to SCAG which will include the project sequencing information required for RTP updates.

10.2 Inland Empire – San Bernardino and Riverside Counties

The Inland Empire Regional ITS Architecture was the first of the county-level architectures to be completed. They propose to manage architecture maintenance through an Inland Empire Architecture Maintenance Team, which includes San Bernardino Associated Governments, Riverside County Transportation Commission, SCAG, Caltrans Traffic Operations and Caltrans Transportation Planning. The Maintenance Team will operate by consensus in agreeing on any changes that need to be made to the architecture. They would receive input from the individual county Technical Advisory Groups (TAGs.) It is agreed that one lead agency will take responsibility for making physical changes for maintaining the architecture. All maintenance Stakeholders will be involved in decision making regarding changes to the architecture.

The authors of the architecture document identified the following approach to architecture updates. They plan on the most significant portions of the architecture being maintained through updates in the electronic database using TurboArchitecture™. Also the following documents would be updated at regular intervals on an as needed basis:

- Project Sequencing;
- Operational Concept;
- Functional Requirements; and
- List of Agency Agreements.

The Inland Empire is committed to updating the architecture every three years to support the RTP process and ensuring that SCAG receives all necessary documentation.

10.3 Ventura County

Ventura County has a very different history of ITS planning, development and deployment. The ITS Deployment Plan, and now their Regional ITS Architecture, is firmly linked to their Congestion Management Program that is updated every three years. Their intent is to maintain and update their architecture in line with their Congestion Management Program update initiatives. The Ventura County Transportation Commission (VCTC) takes lead responsibility for these activities that include close coordination with all of the cities, county and Caltrans Stakeholders. VCTC will take responsibility for maintaining the project sequencing and forwarding this information to SCAG in support of the RTP process. Any other significant changes to the documentation would also be forwarded to SCAG.

10.4 IMPERIAL COUNTY

The Imperial County Regional ITS Architecture is the first ITS planning effort in the County and some ninety Stakeholders have been contacted in its development. The County and Cities lack knowledgeable ITS staff and will need leadership to help maintain the progress that has been made and support Regional ITS Architecture maintenance activities. Lack of funding will likely mean that progress is measured and architectural changes will be few in the early years. Maintenance activities will be simple and will support RTP updates and local needs. Imperial Valley Association of Governments (IVAG) will be responsible for the maintenance of the document and the stakeholder lists. IVAG will also be responsible for forwarding updates to SCAG for the tri-annual RTIP process, when requested to do so. The continuance of the dialogue that has been established will be promoted through Stakeholders sharing the facilitation of meeting opportunities. Continued dialogue will also be supported by groups of stakeholders proceeding with project development. Caltrans will be available to lend their technical advice when requested. FHWA has volunteered to continue to support Imperial Valley Stakeholders understanding of ITS when requested to do so.

10.5 ORANGE COUNTY

Orange County is a relatively advanced county in terms of ITS deployments and in the past has had both a Traffic Forum and an ITS Management Group that have taken leadership roles in ITS development. Both groups have now lapsed. OCTA lead the development of an ITS Strategic Plan update in 2007 which assembled a large group of stakeholders for the Regional ITS Architecture update and OCTA is probably taking the lead to develop an ITS group that meets regularly and provides architecture guidance.

OCTA has agreed to take responsibility for maintaining the documentation and stakeholder lists and forwarding updates to SCAG. Caltrans has agreed to continue with the ITS transportation forums working with the expanded stakeholder base. It is anticipated that these activities will grow over time and lead to improved stakeholder coordination in support of the updated architecture.

10.6 MULTI-COUNTY ISSUES

To fulfill the maintenance requirements at the MPO level, SCAG should have electronic copies of all of the county-level Regional ITS Architecture documentation including the electronic databases in TurboArchitecture™. It would be appropriate that these be posted on SCAG's website in .PDF format and would be available in one location for all Stakeholders in the six-counties. SCAG should also keep on file all significant modifications to the documentation. Only when major revisions are made to the individual architectures would electronic replacements for the website be submitted.

To maintain the Multi-County issues documentation the Stakeholder group should meet regularly to review progress made on projects and decide at what point documentation updates need to be produced. At a minimum, such updates would be made tri-annually in support of the RTP process.

SCAG will be responsible for issuing timely notification of the need for county-level Regional ITS Architecture updates to support the tri-annual RTP process. Project sequencing updates and any other significant updates that the county Stakeholders have made will need to be submitted to SCAG.

A separate Update and Maintenance Plan for the Southern California Regional Architecture was prepared and relates all maintenance activities for the county-level architectures to the needs of SCAG as the MPO including transportation security related matters. The process for the architecture maintenance to be followed for the Southern California Regional ITS Architecture is set out in this document and should continue to be maintained.

11.0 AGENCY AGREEMENTS

Agreements among the different Stakeholder agencies and organizations are required to implement the integration described in the Regional ITS Architecture. According to the FHWA Regional ITS Architecture Guidance, any agreements (existing or new) required for operations, including at a minimum those affecting ITS projects interoperability, utilization of ITS related standards, and the operation of the projects identified in the Regional ITS Architecture are required by the Rule/Policy. The requirement however is only to provide a list of agreements and not the agreements themselves. Experience shows that it takes an actual project deployment to initiate the agreements process.

The typical process of agreements list development starts from existing agreements that support sharing of information, funding, or specific ITS projects. These agreements are reviewed and assessed to determine if they can be extended and used to support the cooperative implementation and operation of ITS. The list of the required agreements was developed based on the regional operational concepts, knowledge of the types of ITS existing or planned for implementation in the county, and the information that needs to be exchanged in order to operate those systems. The detailed agreement work, including the preparation and execution of the identified agreements will be performed to support ITS projects as they are implemented in the future.

There is considerable variation between ITS projects and among Stakeholders regarding the types of agreements that are created to support ITS integration. Some common types of agreements provided by the Regional ITS Architecture Guidance are shown in Table 11-1.

Table 11-1 – Stakeholder ITS Project Agreement Types

Type of Agreement	Description
Handshake Agreement	• Early agreement between one or more partners • Not recommended for long-term operations.
Memorandum of Understanding (MOU)	• Initial agreement used to provide minimal detail and usually demonstrating a general consensus. • Used to expand a more detailed agreement like an Interagency Agreement that may be broad in scope but contains all of the standard contract clauses required by a specific agency. • May serve as a means to modify a much broader Master Funding Agreement, allowing the master agreement to cover various ITS projects throughout the region and the MOUs to specify the scope and differences between the projects.
Interagency Agreement	• Between public agencies (e.g., transit authorities, cities, counties, etc.) for operations, services or funding. • Documents responsibility, functions and liability at a minimum.
Intergovernmental Agreement	• Between governmental agencies (e.g., Agreements between universities and State DOT, MPOs, etc.).
Operational Agreement	• Between any agency involved in funding, operating, maintaining or using the right-of-way of another public or private agency. • Identifies respective responsibilities for all activities associated with

Type of Agreement	Description
	shared systems being operated and/or maintained.
Funding Agreement	• Documents the funding arrangements for ITS projects (and other projects). • Includes at a minimum standard funding clauses, detailed scope, services to be performed, detailed project budgets, etc.
Master Agreements	• Standard contract and/or legal verbiage for a specific agency and serving as a master agreement by which all business is done. These agreements can be found in the legal department of many public agencies. • Allows states, cities, transit agencies, and other public agencies that do business with the same agencies on a regular basis (e.g., cities and counties) to have one Master Agreement that uses smaller agreements (e.g., MOUs, Scope-of-Work and Budget Modifications, Funding Agreements, Project Agreements, etc.) to modify or expand the boundaries of the larger agreement to include more specific language.

Table 11-2 presents the list of agreements for Southern California regional ITS development. Each entry identifies the ITS service addressed by the agreement, the Stakeholders involved, the type of agreement anticipated, high-level status (near-term or long-term), and a concise description of the purpose of the agreement. Another column can be added to the table in the future to note any issues or barriers in agreement execution during the architecture maintenance cycle.

Table 11-2 - Regional List of Agreements

ITS Service	Stakeholder	Type of Agreement	Status	Agreement Description
Multi Caltrans Districts Interfaces	Caltrans Districts	MOU	Long Term	Specifies interface requirement, responsibilities, and functions for all participating Caltrans districts
Arterial Traffic Control Interfaces	Jurisdictions	Interagency Agreement	Near Term	Specifies interface requirement, responsibilities, and functions for all participating and neighboring cities
Data Archive System	Regional Partners	Interagency Agreement	Near Term	Specifies data source, access control, and configuration requirement
Emergency Management / Security Region Wide Integration	Regional Partners	Interagency Agreement/or MOU	Long Term	Provides the guidelines of the integration of emergency management system, including the roles and responsibilities of each agency as well as the functions required for each of their systems
Multi-agency Video Sharing and Distribution	Regional Partners	Interagency Agreement	Long Term	Specifies interface & configuration requirements, functions, data sources, and access control for all participating agencies

ITS Service	Stakeholder	Type of Agreement	Status	Agreement Description
Multi Transportation Agency Regional Interfaces	Regional Partners	Interagency Agreement	Long Term	Specifies interface requirement, responsibilities, and functions for all participating agencies
Interstate DOT Information Exchange	Caltrans, NDOT, AZDOT	Interagency Agreement/or MOU	Near Term	Specifies interface requirement, responsibilities, and functions for all participating agencies
Traffic Management Center and EMC Communications	TMC and EMC operators	Interagency Agreement	Long Term	Specifies interface requirement, responsibilities, and functions for all participating agencies
Common Format Hazardous or High Priority Vehicle Tracking	Ports, Law Enforcement, Emergency Responders, Commercial Vehicle Operators	Interagency Agreement/or MOU	Long Term	Specifies interface requirement, responsibilities, and functions for all participating agencies
Emergency Notification of Transit Operators	Transit Agencies, EMC's, TMC Operators	Interagency Agreement	Near Term	Specifies interface requirement, responsibilities, and functions for all participating agencies
Regional Centralized Information Clearinghouse	Regional Partners	Interagency Agreement/or MOU	Near Term	Provides the guidelines of the integration of emergency management planning and resources, including the roles and responsibilities of each agency
Rail Location and Notification	UP, BNSF, EMC's, Emergency Responders	Interagency Agreement/or MOU	Near Term	Specifies interface requirement, responsibilities, and functions for all participating agencies
Security Threat and Guidance Clearinghouse	Regional Partners	Interagency Agreement /MOU	Near Term	Provides the guidelines of the integration of security threat and guidance system, including the roles and responsibilities of each agency
Ports Traffic Information	I-5 JPA, Ports, Gateway COG	Interagency Agreement /MOU	Near Term	Specifies interface requirement, responsibilities, and functions for all participating and neighboring agencies