National ITS Architecture Security

Prepared by the

Architecture Development Team

Prepared for:

Federal Highway Administration
US Department of Transportation
Washington D.C. 20590

October 2003

Table of Contents

Table of Figures

Table of Tables

1. INTRODUCTION AND BACKGROUND

This Security Document presents an overview of security as it is represented in the National ITS Architecture and provides guidance for using the security-related parts of the National ITS Architecture. The objective of 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. The heightened concern of potential terrorist threats to the homeland spurred the introduction of new and updated User Services and User Service Requirements that drove the security-related parts of Version 5.0 of the National ITS Architecture.

Section 2 of this document discusses the security-related updates to the National ITS Architecture. There are two key facets of ITS security that are presented in section 2:

1) Securing ITS – Protecting ITS systems and the communications between them, and

2) ITS Security Areas – Use of ITS to detect, respond to, and recover from threats against the surface transportation system.

These two facets of security are complementary. A secure ITS system is a prerequisite and a foundation for ITS applications that improve surface transportation security.

Section 3 describes security considerations associated with regional ITS architecture development and deployment. As described in section 3, it is important to consider security as part of architecture development. It is always easier and more effective to plan and implement security services up front rather than after systems have been deployed.

The security analysis that is described in this document is general in nature and not intended to be a substitute for the security analysis that should be performed for each ITS system. It is incumbent upon the user to consider, review and modify these generalized security services as appropriate to the specific situation.

2. SECURITY AND THE NATIONAL ITS ARCHITECTURE

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

1. Securing ITS: ITS is a collection of information systems 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 and is described in section 2.1. "Securing ITS" is shown as the foundation in Figure 1 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 are described in section 2.2 that 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 Figure 1, 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.

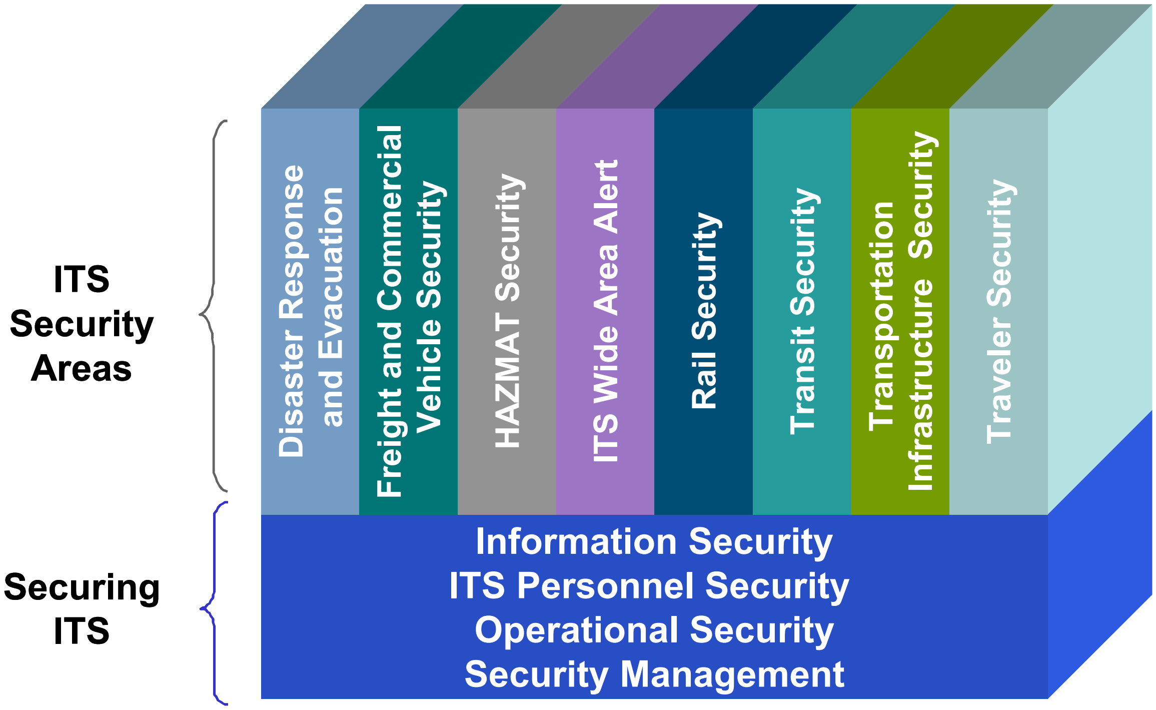
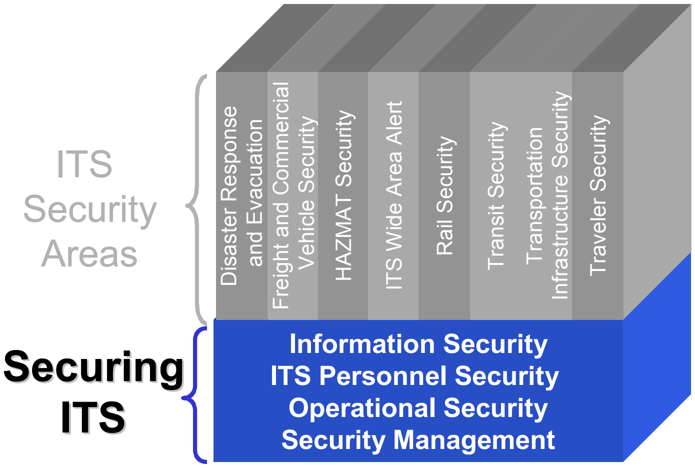


Figure 1. Security in the National ITS Architecture

To illustrate these two views of security, consider a transit surveillance system that includes CCTV cameras and a control center. 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 in section 2.1 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 ITS security areas ("Transit Security") that are described in section 2.2.

2.1 Securing ITS



ITS systems are subject to security threats like any other information technology system. This is true not only for systems that process personal or financial information (i.e., electronic toll collection systems), but also for many other types of ITS systems. Dynamic message signs are subject to tampering and unauthorized use, traffic signal control systems must operate flawlessly and fail in a safe manner when disruptions do occur, and many ITS operations centers may be called upon to play an important role in disaster response and recovery. ITS systems can only contribute to a disaster response if the ITS systems are robust and secure enough to operate reliably in crisis situations. Note from these examples that security is not only concerned with preventing unauthorized disclosure of sensitive information. Comprehensive security also addresses a broad range of threats that can disrupt or alter system operation.

System security is based on the basic interrelated concepts shown in Figure 2. Essentially, security services (also known as safeguards or countermeasures) are selected that support security objectives and protect against identified threats. The actual analysis that is performed for a specific system is based on an analysis of the threats (are they credible?), the system vulnerabilities to those threats (is the system vulnerable?), and an overall risk analysis that balances the cost of the security service against the likelihood of the threat and the consequences if the threat is realized. As shown in Figure 2, security objectives drive the process by defining what is to be accomplished with regard to security. A number of excellent resources are identified in section 5 that fully explain the process of applying security in the design, development, and operation of an information system.

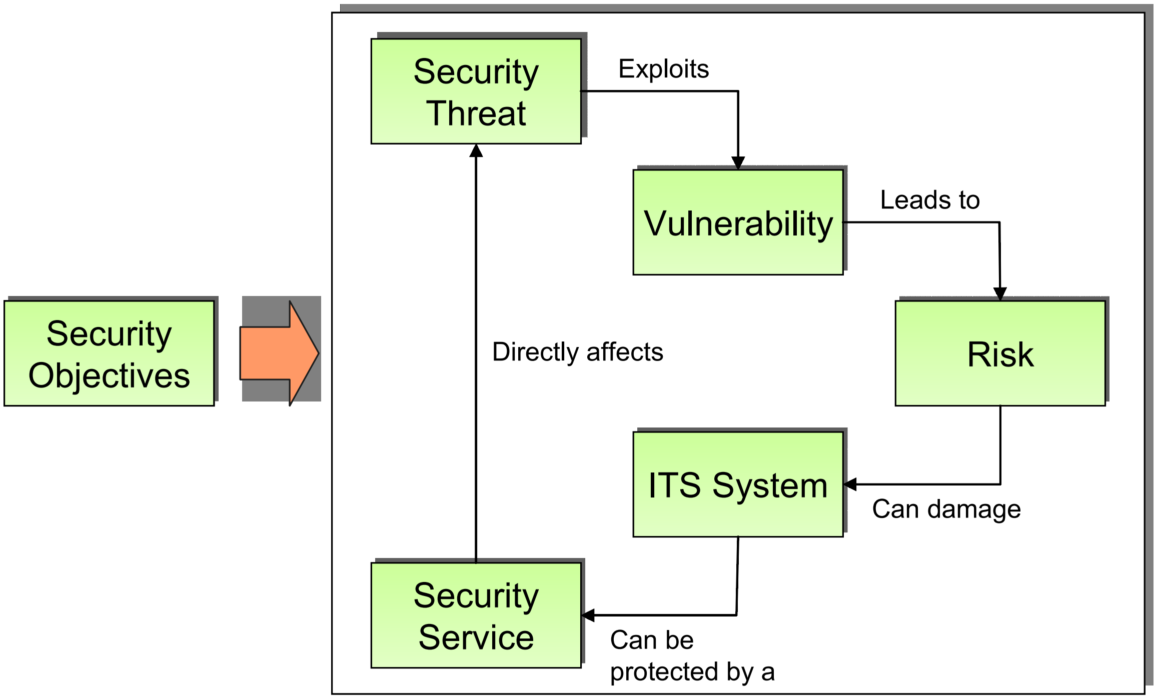


Figure 2. Applying Security to an ITS System

The National ITS Architecture was enhanced in version 5.0 to include some of the security concepts in Figure 2, but in a way that preserves the architecture's implementation independence. Some of the concepts that are shown were not included in the National ITS Architecture because they can only be defined for a specific system implementation. For example, system vulnerabilities are assessed based on the technologies employed, the security services that are already in place, and the environment in which the system operates. Similarly, a risk assessment must be based on actual system implementation. The assessment of benefits and costs that is part of a risk assessment can only be calculated for a specific system implementation.

Given these limitations, the National ITS Architecture was enhanced in version 5.0 to include general security objectives, threats, and services that are implementation independent. Instead of the specific computer and communications systems (the "ITS Systems" in Figure 2.) that are considered in a traditional security analysis, these general security concepts are applied to subsystems and information flows that are defined in the National ITS Architecture, as shown in Figure 3. The security analysis that is included in the National ITS Architecture is high-level, but representative of the initial security analysis that is performed for any system. This section discusses how securing ITS is represented in the National ITS Architecture. It defines general security objectives and threat rankings and describes how those lead to suggested security services for subsystems and architecture flow groups. Section 3 describes how this general security analysis can serve as a starting point for a more specific security analysis associated with a specific regional ITS architecture or ITS system.

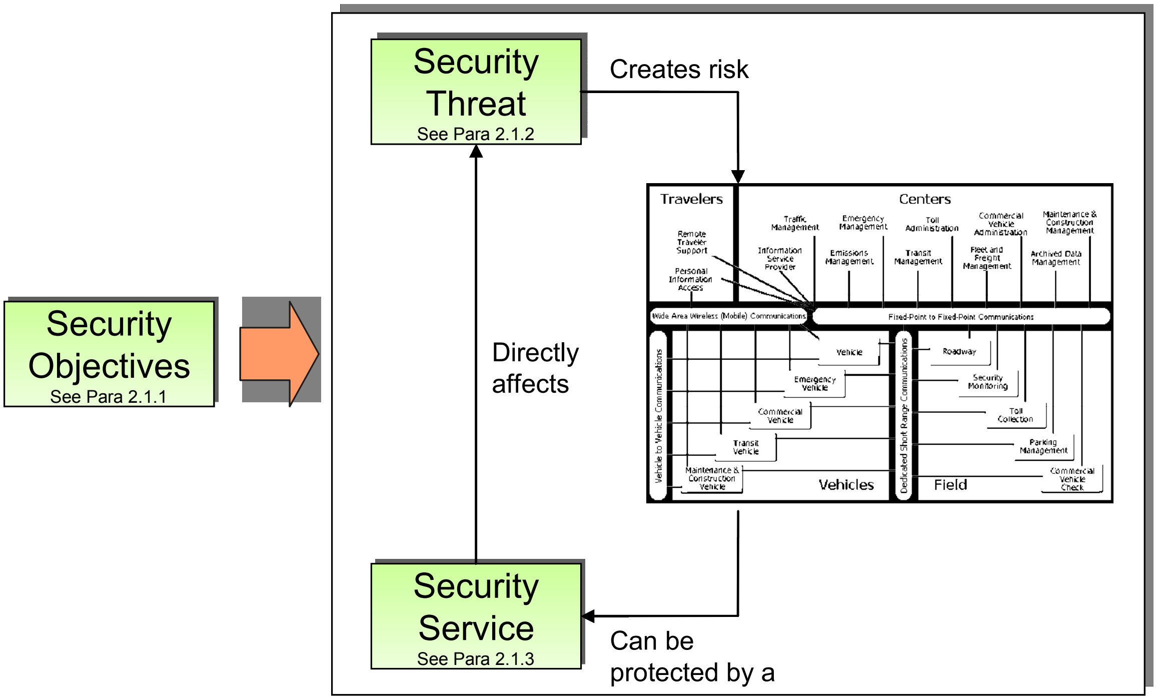


Figure 3. Applying Security to the National ITS Architecture

2.1.1 Security Objectives

The main security principles or objectives apply to any security program - including ITS security. The major security objectives identified for the National ITS Architecture are very likely to apply to some degree in almost any ITS implementation. All security services are implemented to support one or more of these objectives. Similarly, all threats undermine one or more of these objectives. How well a security system performs can be measured by the extent to which it meets the desired objectives. The National ITS Architecture was evaluated in terms of meeting the three overarching security objectives of Confidentiality, Integrity and Availability.

The *Confidentiality* objective ensures that information is not disclosed to unauthorized individuals, processes, or systems (e.g., protecting trucking company records). This security objective deals with the prevention of unauthorized disclosure of information deemed sensitive. The confidentiality security objective defines the level of restriction to sensitive information that is transmitted or stored within a system.

The *Integrity* objective ensures the accuracy and reliability of information and systems, and defines the level of protection from unauthorized intentional or unintentional modifications. This objective is related to auditing accountability, authentication, and access control services for sensitive information.

The *Availability* objective ensures that systems and information are accessible and usable to authorized individuals and/or processes.

Since each of the objectives can be more or less critical to different parts of the architecture, the objectives were assigned with a level – High, Medium, Low, and Minimal – in the security analysis of the National ITS Architecture.

2.1.2 Security Threats

Security threats are events or circumstances that adversely impact a surface transportation system or communication between systems. Threats cover a broad spectrum and include errors, fraud, disgruntled employees, fire, water damage, hackers, terrorist acts, viruses, and natural disasters. For the National ITS Architecture, general threat categories are identified that encompass all of these specific threats, but allow threats to be categorized in a general way. The four general threat categories are as follows:

- *Deception*: a circumstance or event that may result in an authorized entity receiving false data and believing it to be true.

- *Disruption*: a circumstance or event that interrupts or prevents the correct operation of system services and functions.

- *Usurpation*: a circumstance or event that results in control of system services or functions by an unauthorized entity.

- (Unauthorized) *Disclosure*: a circumstance or event whereby an entity gains access to data for which the entity is not authorized.

The system implementer and system manager must ultimately identify and analyze specific threats to determine the likelihood of their occurrence and their potential to harm a specific ITS system. Security Threats, along with Security Objectives, provide the basis for evaluating appropriate security services.

2.1.3 Security Services

Security services are general countermeasures or safeguards that improve system security, address security threats, and help to fulfill the security objectives of the system. Security services protecting ITS should take into account the degree of (1) preventing theft or damage to hardware, (2) preventing theft or damage to information, and (3) preventing disruption of service. The general security services identified for the National ITS Architecture are implemented using various specific technologies and processes. The specific techniques that are used to provide a security service are commonly referred to as security mechanisms. Specific mechanisms are only provided as illustrative examples in the National ITS Architecture. The security services are grouped into four categories as depicted in Figure 1: Information Security, Operational Security, ITS Personnel Security and Security Management.

Information Security deals with securing the origin, transmittal and destination of the information itself. For example, an "access control" information security service would limit access to the resources of a subsystem to only those users and other subsystems that are properly authorized. Operational Security is responsible for protecting ITS assets against both physical and environmental threats. This area, for example, provides monitoring of critical ITS assets. The ITS Personnel Security category ensures that ITS personnel do not inadvertently or maliciously cause harm to ITS assets and have proper training in the event there is a security-related incident. The Security Management category connects all of the other security services together in order to provide security controls throughout ITS. Security Management ties in with the Information, Operational, and Personnel security aspects of securing ITS as well as the eight security areas described in section 2.2. Security services can be directed towards the potential for an attack as well as countering the attack after it has occurred. Appendix A categorizes and defines the security services in detail.

2.1.4 Securing ITS and the National ITS Architecture

Identification of security objectives, threats, and security services to address the threats and meet the objectives are relevant in any information system, and should be evaluated whenever security is a concern. Of course, different parts of ITS are subject to different security concerns based on the criticality of the application and the sensitivity of the information that is exchanged. In the following sections, each of the subsystems (section 2.1.4.1) in the National ITS Architecture and major architecture flow groups (section 2.1.4.2) are discussed to highlight those additional security concerns to consider.

2.1.4.1 Securing ITS Subsystems

Version 5 of the National ITS Architecture defines 22 subsystems, each of which have potential security considerations. Appendix B provides a description of these potential security considerations for each subsystem. These high-level descriptions are intended to highlight the confidentiality, integrity, and availability objectives that apply to each subsystem. Because of the breadth of function and diverse nature of the processing within each subsystem, the specific security considerations for a given ITS implementation must be developed by understanding the objectives, threats, and the system vulnerabilities to these threats.

2.1.4.2 Securing ITS Architecture Flows

The focus of the ITS program is for systems to be able to seamlessly exchange information. Protecting system interfaces is critical to securing ITS. The interfaces, or architecture flows, as defined in the National ITS Architecture have been analyzed to ascertain the relative importance of applicable security services. In order to keep the security considerations for architecture flows manageable, architecture flow groupings were created for architecture flows that share similar security objectives, threats and security services.

Architecture flows have been placed into one of sixteen groups that are based on unique security considerations. In cases where an architecture flow could be allocated to multiple groups, the most appropriate security group was chosen. Each architecture flow group has been given typical security service, security objectives and security threat classifications of high, medium, low or minimal. Similar architecture flows are grouped together so that security services can be consistently applied. The security service classifications are based on the security objective and threat importance. For example, the combination of a high level of integrity (i.e., unauthorized modification of the information) and a high level for the threat of deception would necessitate, among other services, a high or great need for the Access Control security service.

The information content of the architecture flow coupled with its operational role was considered in the security service classifications. In some cases, the security service, objective or threat is not applicable and thus will not be in the corresponding table. The security service considerations are typical; it is incumbent on the user to tailor the security considerations as appropriate to the ITS application (e.g., sensitive archive data might require a higher classification than the nominal “Low” designation identified in the National ITS Architecture).

The security information for all architecture flows is available in the hypertext presentation on the website and CD-ROM. To illustrate the types of security information available, one of the sixteen Architecture flow groups of flows – the “Operational Information – Safety” group, is presented and explained here.

The "Operational Information – Safety" architecture flow group contains architecture flows that carry information used to support operation of the transportation system that is safety critical; the loss of such information could impact public safety.

For each architecture flow group, there are three tables. The first table (Table 1) includes a list of the applicable security services and their relative importance, which have been derived from the security objectives and threats depicted in the subsequent two tables (Table 2 and Table 3). Consider, for example, one of the architecture flows in this group, “barrier system status” representing the status of HOV gates. As shown in Table 1, all of the security services for architecture flows in this group are of high importance except confidentiality. The disclosure of the status of the HOV gate is not important; that is, information about whether the gate is up or down is not sensitive. On the other hand, the integrity security service is important because the system, for safety reasons, should not falsely give the status of the gate as up when it is in fact down.

Table 1. "Operational Information - Safety" Security Services

Service	Importance	Service Description
Confidentiality	Low	The system should prevent unauthorized disclosure of information deemed sensitive.
Integrity	High	The system should ensure that information is protected from unauthorized intentional or unintentional modifications.
Availability	High	The system should protect critical ITS services in order to prevent degradation or denial of the ITS services to users of the services. Single points of failure should be avoided.
Accountability	High	The system should provide protection against a sender of an information transmission later denying that they sent the information. The system should provide protection against a receiver of an information transmission later denying that they received the information. This concept is known as Non-Repudiation or Accountability.
Authentication	High	The system should verify the identity of a user and/or other system prior to granting access to a requested resource.
Auditing	High	The system should have the capability to trace ITS subsystem and individual user actions and activities. The auditing function of the system places the actions and activities in an audit trail that is protected from unauthorized access and modification.
Access Control	High	The system should limit access to the resources of a subsystem to only those users and other subsystems that are properly authorized. After authenticating an entity, the system should have the capability to limit system access to information or resources based on that entity's access privileges. The system should limit software modifications and upgrades to users and other systems that have authorization.

The security services and their importance (Table 1) have been derived from the security objectives and their classifications (Table 2) and the security threats and their importance (Table 3). The low classification of the confidentiality security objective coupled with the low importance for the threat of disclosure resulted in a low importance for the confidentiality security service. Similarly, the level of importance assigned to each of the other security services was derived by taking into account the security objectives and threats.

Table 2. “Operational Information – Safety” Security Objectives

Objective	Classification	Class Description
Confidentiality	Low	Information that is generally available to ITS personnel
Integrity	High	Unauthorized or unintended modification of the information could result in degradation of public safety.
Availability	High	Loss of the information could jeopardize public safety.

Table 3. “Operational Information – Safety” Security Threats

Threat	Importance	Threat Description
Deception	High	A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
Disclosure	Low	A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
Disruption	High	A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Following the three tables on the National ITS Architecture website and CDROM is a list of the architecture flows that have been placed in this architecture flow group, in this case the “Operational Information – Safety” group.

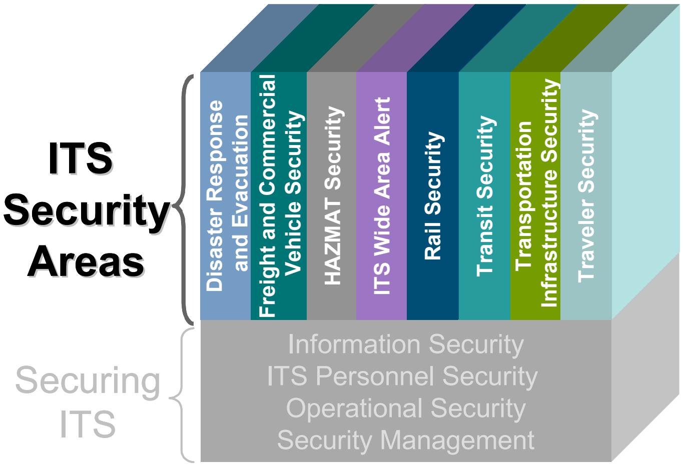
Architecture flows for the “Operational Information – Safety” group

AHS control data
AHS control information
AHS status
AHS vehicle data
alerts
arriving train information
barrier system status
emergency traffic control information
emergency traffic control request
highway control status
hri operational status
infrastructure monitoring sensor data
intersection blockage notification
intersection status
multimodal crossing status
rail system status assessment
railroad advisories
road network status assessment
roadway equipment coordination
roadway information system data
safeguard system status
track status
transit system status assessment
transit vehicle operator authentication information
transit vehicle operator authentication update
transportation system status
vehicle to vehicle coordination

The architecture flow group descriptions for all sixteen groups are defined in Appendix C. Further information regarding the corresponding security objectives, threats, security services and applicable architecture flows for each group can be found on the National ITS Architecture CDROM or website hypertext by selecting "Security" from the left-hand menu and following the links.

2.2 ITS Security Areas

The previous section dealt with securing ITS from the National ITS Architecture perspective of categorizing ITS subsystems and architecture flows based on security objectives, threats and services. Securing ITS as depicted in the figure to the right, forms the foundation for securing the ITS Security Areas of the National ITS Architecture. The term "Security Area" represents areas of ITS which 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. For each ITS security area, this section discusses the scope of the area along with its architecture representation including appropriate market packages.



2.2.1 Disaster Response and Evacuation

2.2.1.1 Description/Scope

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.

2.2.1.2 Architecture Representation and Market Package(s)

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).

2.2.2 Freight and Commercial Vehicle Security

2.2.2.1 Description/Scope

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.

2.2.2.2 Architecture Representation and Market Package(s)

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 & 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.

2.2.3 HAZMAT Security

2.2.3.1 Description/Scope

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.

2.2.3.2 Architecture Representation and Market Package(s)

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.

2.2.4 ITS Wide Area Alert (WAA)

2.2.4.1 Description/Scope

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.

2.2.4.2 Architecture Representation and Market Package(s)

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.

2.2.5 Rail Security

2.2.5.1 Description/Scope

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.

2.2.5.2 Architecture Representation and Market Package(s)

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.

2.2.6 Transit Security

2.2.6.1 Description/Scope

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.

2.2.6.2 Architecture Representation and Market Package(s)

The Transit Security area's key market package is Transit Security (APTS5). 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.

2.2.7 Transportation Infrastructure Security

2.2.7.1 Description/Scope

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.

2.2.7.2 Architecture Representation and Market Package(s)

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.

2.2.8 Traveler Security

2.2.8.1 Description/Scope

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

2.2.8.2 Architecture Representation and Market Package(s)

There are four key market packages that represent the Traveler Security area. The Transit Security (APTS5) 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.

3. SECURITY CONSIDERATIONS - ITS PLANNING AND DEPLOYMENT

Security should be considered as an integral part of ITS planning and deployment. Experience has shown that it is very difficult to implement security measures properly and successfully after a system has been developed, so security should be integrated early in the system lifecycle. The regional ITS architecture development effort provides an important opportunity to address security early in the planning process. Since the regional ITS architecture provides the framework for ITS integration in a region, this framework should also address security so that the integration opportunities that are identified do not ultimately accentuate vulnerabilities and adversely impact the mission-readiness of the regional transportation system. The regional ITS architecture provides a natural starting point for a top-level security policy and strategy for a secure regional transportation system.

The objective of this section is not to define a single process for regional ITS architecture development or to prescribe the only way to apply security considerations to this process. The objective is to increase awareness of security and its implications for regional ITS architecture development. A number of security-related products are discussed in this section; collectively, these products are referred to as a security plan for the region. This is a convenient way to refer to the collection of security products, but it is not meant to imply that the security products must be packaged as a single "Security Plan" document. Although the focus of this section is on regional ITS architectures, the security considerations are also applicable to project ITS architectures.

Recall that security in the National ITS Architecture has two perspectives: 1) "Securing ITS" that defines the security services necessary to secure ITS, and 2) the eight "ITS security areas" that define different ways that ITS can improve surface transportation security. Security in a regional ITS architecture can be viewed from the same two perspectives. The first perspective is the focus of this section – defining security considerations that will improve the security of the ITS systems in the region. The second perspective - the eight ITS security areas - can be incorporated into a regional ITS architecture like any other ITS service since the National ITS Architecture has been updated to include this new security functionality. The process to include these services in a regional ITS architecture is described in the *Regional ITS Architecture Guidance* document.

Figure 4 identifies the steps in the regional ITS architecture development process that are defined in the *Regional ITS Architecture Guidance* document. On the left side of the figure, there are security-related activities associated with "Securing ITS" that are related to each of these process steps. Each of these activities is further defined in the following paragraphs.

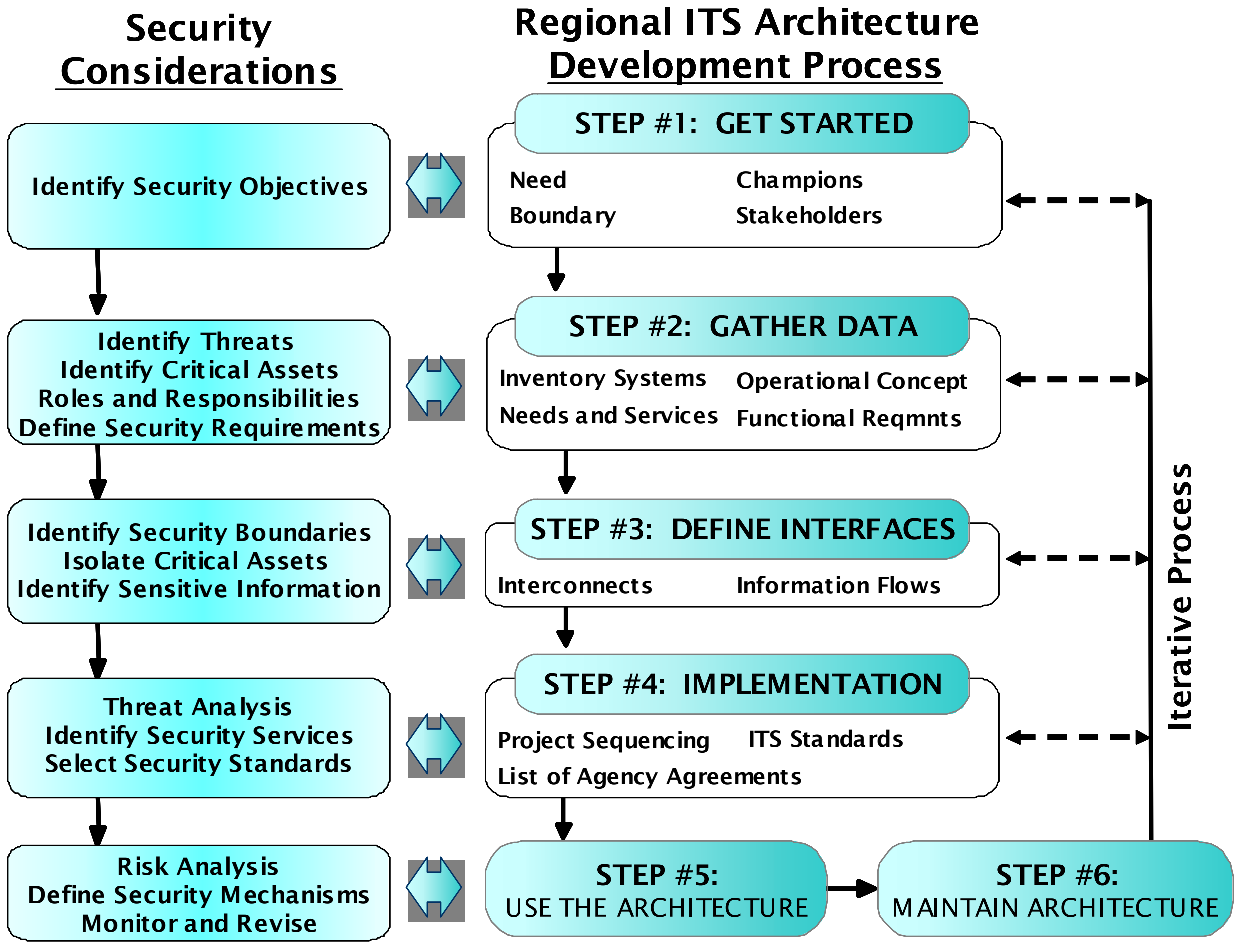


Figure 4. Addressing Security in Regional ITS Architecture Development

3.1 Step #1: Get Started

The regional ITS architecture development effort begins with a focus on the institutions and people involved. From a security perspective, this is the time to establish a basic commitment to security by the regional ITS architecture stakeholders. As the boundary of the regional ITS architecture is established and stakeholders are identified, the basic security objectives – confidentiality, integrity, and availability – should be included in the formative inputs to the regional ITS architecture. At this point, the objectives may be included in a high-level security policy statement that will guide regional ITS architecture development in subsequent steps. The basic statement of objectives that is crafted at this step will be elaborated and refined as critical assets, threats, and security related roles and responsibilities are defined in subsequent steps. Establishing the basic need for security at the outset is particularly important since regional ITS architectures rely on participation and support from public safety, emergency management, and other organizations where security is critical. Different organizations will be willing to accept different levels of risk; the security objectives provide an initial shared statement that can encourage organizations to participate in the regional ITS architecture development and subsequent integration projects.

3.2 Step #2: Gather Data

Once the stakeholders are involved and a basic commitment to the security objectives for the region is established, a review of the regions security plan or policy (if it exists) should be performed. Security-related data can be gathered and an initial or updated security analysis can be performed and documented in a security plan for the region. The elements of this high-level security analysis build on the basic regional ITS architecture development steps that occur in Step #2.

Identify Threats: Version 5.0 of the National ITS Architecture contains general threat categories that can be used as a starting point for identifying threats that may apply to the regional transportation system. Any existing threat assessments for ITS systems in the region should also be gathered and used. Each of the threat categories in the National ITS Architecture covers a broad range of specific threats that should be considered for the region. A more detailed description of the threat categories (referred to as "threat consequences") and their relationship to specific threats can be found in RFC 2828: Internet Security Glossary.

Identify Critical Assets: In conjunction with threat identification, the regional ITS inventory that is compiled should be reviewed to identify critical assets – systems that, if lost, would jeopardize the ability of the regional transportation system to provide a primary function or threaten public safety. Any existing regional analysis of critical assets can be used as a starting point, if available. In later steps, the regional ITS architecture will be organized to protect these critical assets and security services. Security mechanisms will be defined to isolate these critical assets from non-critical assets in order to reduce the number of assets that need stringent security mechanisms. The security analysis associated with each National ITS Architecture subsystem can provide an input to the identification of the security-critical elements in the ITS inventory (refer to section 2.1.4.1).

Roles and Responsibilities: Within the regional ITS architecture development process, operational roles and responsibilities are identified as part of the "operational concept". From a security perspective, there are roles and responsibilities associated with making sure the security objectives are met. These roles and responsibilities can also be established at this step, leveraging on organizations in the region that have specific interest and expertise in information security.

Security Requirements: In conjunction with functional requirements definition, security requirements can also be defined that identify security constraints and functions that will protect the confidentiality, integrity, and availability of the connected systems and the data that will pass between them. The initial security requirements will be iterated and refined in subsequent steps as the regional architecture is fully defined and implemented in stepwise fashion, project by project. In general, the security requirements included in the regional ITS architecture will focus on those requirements associated with system integration and sharing of data between systems. Each individual system will still have responsibility for protecting the systems and data within their own domain. These internal system requirements are normally not the focus of the regional ITS architecture.

A security plan may be created to document the overall security objectives, identified threats, security requirements, and the roles and responsibilities that ensure that the security objectives will be met and the security threats are countered. The security plan takes into account the region's needs and services that require some level of security and should be consistent with the region's operational concept.

3.3 Step #3: Define Interfaces

In the next step in the regional ITS architecture development process, the connections between ITS systems are identified, creating a framework for integration that will support the exchange of information between ITS systems. These connections enable coordinated operation and resource and information sharing, but they also can create system vulnerabilities that should be addressed through security. This step defines the security implications for the interfaces between systems. At the completion of this step, the security plan will broadly define the types of access to system data and the conditions under which access is allowed, reflecting the following analysis.

Identify Security Boundaries: Each ITS system may be governed by its own security policy – perhaps an overall policy for the organization or a specific policy for the system, or both. Some organizations may not have a formally documented security policy, which normally means that the associated system should be treated as insecure until it is analyzed. The interfaces between these ITS systems represent security boundaries between the different governing security policies that should be identified and addressed. Interfaces between secure and insecure systems should be identified.

Isolate Critical Assets: In particular, the interfaces to any ITS system identified as critical in the previous step should be partitioned to limit interfaces and permit only a deliberate flow of authorized information between the critical system and other ITS systems in the region. The regional ITS architecture, by its nature, helps to partition ITS systems from each other by providing focus on the interfaces. Security concerns may result in the reduction of architecture flows or interconnects to and from critical ITS systems in the regional ITS architectural framework.

Identify Sensitive Information: As architecture flows are identified for the regional ITS architecture, they should be examined with respect to the security objectives of availability, confidentiality, and integrity. By evaluating each architecture flow against the three objectives, the most sensitive information is identified that should be afforded special security protections when the systems are integrated. The National ITS Architecture includes a basic assessment of each architecture flow against the three security objectives that can be used to support this process. In conjunction with the security objectives, specific threats associated with the architecture flows can be identified, extending the threats identified in the previous step to include threats to the system interfaces. As in the previous step, the general threat categories identified in the National ITS Architecture can be used as a starting point for an analysis that identifies specific threats to information transfers between ITS systems in the region. The initial threat analysis performed in this and the preceding step will culminate in an overall documented threat analysis in Step #4.

3.4 Step #4: Implementation

The implementation step in regional ITS architecture development defines additional products that guide project implementation. Some of the products that are defined have security implications. For example, agreements between agencies should include security assumptions and definition of security approaches and services. The list of agreements should include agreements that are necessary to connect systems with disparate security requirements and governing security policies. Also, project sequencing should take security into account, expediting projects that implement basic security services that will support future interoperability and sharing of information. Several specific security products can also be prepared that will highlight specific security considerations for proposed projects.

Threat Analysis: A threat analysis considers the potential threats, the likelihood of occurrence, the system's vulnerability to those threats, and the damage that may occur if the threat is realized. Both qualitative and quantitative approaches may be used. It is likely that in the early planning stages, the analyses will be more qualitative and transition to a more quantitative analysis as projects are developed in the next step.

Identify Security Services: The threat analysis ultimately identifies the threats that pose the most significant risk to the system. Security services can then be identified that are necessary to blunt or remove the most significant threats and satisfy the region's security objectives. The National ITS Architecture includes a set of security services, interrelated with security objectives and threats, and associated with specific architecture flows, that can provide a starting point for security service definition for the region. The security services can be associated with ITS systems, the interfaces between these systems, or specific information that is defined in the regional ITS architecture. Recognizing the uniqueness of each system, interface, and piece of information allows a layered security strategy to be used – planning for fewer or lower assurance security services to protect less critical systems and higher assurance solutions only for the most critical areas.

Select Security Standards: It is critical that appropriate ITS standards are chosen with security requirements in mind. Agencies should consider ITS Standards that address security services (e.g., NTCIP 2103, NTCIP 1105). Although many message sets are being standardized in order to attain interoperability, incompatible security policies, requirements and services between ITS systems has the potential to severely restrict interoperability. Security program designers should consider interoperability and portability in the identified security services so that the security capabilities will be effective in the multi-jurisdictional environment covered by a regional ITS architecture.

3.5 Step #5: Use the Regional ITS Architecture

The regional ITS architecture is used to support transportation planning and project implementation. The security objectives, security requirements, general threat analysis, security services, and security-related standards that are defined in the previous steps are all products that can be used to inform project implementation.

One of the clearest differences between ITS and conventional transportation solutions is the level of interdependency that exists between projects and the degree to which information, facilities, and infrastructure can be shared with mutual benefit. Project ITS architectures should focus on the project's security needs and its interfaces to other projects. There is a cost for integrating ITS systems, especially in the realm of security. In some cases it may be cost-prohibitive to institute security services across legacy ITS systems. Careful planning and adherence to the architecture baseline, including the security plan, is necessary to minimize the impact to future regional ITS interoperability. As projects are defined and implemented, several additional security products are developed:

Risk Analysis: As part of project development, more specific risk analysis can be performed than was possible in earlier steps. At this point, better information will exist that will allow the analyst to estimate the value of the system or information to be protected, estimate the anticipated loss including both monetary loss and intangibles, possibly annualized, and also estimate the cost of the specific security mechanisms. A variety of techniques can be used to identify the risks that should be addressed and characterize the residual risk that will remain when the security mechanisms are implemented. The object is not to drive the residual risk to zero since it is normally cost-prohibitive (if not impossible) to eliminate all risk and there are also competing operational needs that must be addressed. It may be necessary to modify or adjust security objectives due to other operational requirements.

Define Security Mechanisms: Although the National ITS Architecture and this Security document do not focus on security mechanisms such as firewalls, virus protection, public key encryption, intrusion detection systems, and redundant, distributed systems, these mechanisms will be defined and included in project implementation. This step in the process identifies and defines the mechanisms that implement the security services defined in the security plan. For the most critical assets, layered security mechanisms may be used so that the sophisticated attacker must circumvent more than one layer of protection. Since security has a cost both in real dollars and operational efficiency, every security mechanism that is implemented should be justified. Every security mechanism should support one or more security services, and every security service should support one or more security objectives. A cost-benefit analysis can be used to determine the most cost-effective security mechanisms.

3.6 Step #6: Maintain the Regional ITS Architecture

The regional ITS architecture is maintained over time as projects are implemented and the scope of ITS in the region changes. As new ITS systems are implemented and integrated, new threats and vulnerabilities will be identified that must be addressed on an on-going basis.

Monitor and Revise: Despite our best efforts, vulnerabilities will still exist in a system as complex as a regional surface transportation system. In some cases, the vulnerabilities will be known but still exist due to cost considerations or trade-offs for operational efficiency. In other cases, vulnerabilities may not be identified until a system is fielded and subject to evolving threats. Organizations should establish capabilities to detect and respond to evolving security threats and actual attacks, manage single points of failure in their systems, and implement a reporting strategy. New vulnerabilities that are identified should be reflected back into the security plan for the project and/or region. A configuration management process for making changes to the architecture baseline, including security considerations, should be established and maintained.

4. CONCLUSION

ITS, by its nature, is susceptible to electronic and physical threats to its mission. Security services are general countermeasures or safeguards that improve system security, address security threats, and help to fulfill the security objectives of the system. Security services protecting ITS should take into account the degree of (1) preventing theft or damage to hardware, (2) preventing theft or damage to information, and (3) preventing disruption of service. Security is usually an afterthought; in many cases the security services are an impediment to interoperability and system performance. It is therefore critical that the proper stakeholder security needs and requirements are defined up front. Security services are the most effective when they are instituted at the beginning of ITS deployment. Retrofitting existing systems with security services must be done with the utmost caution. It is strongly recommended that the ITS community consider this representative security process in their planning and implementation endeavors. The reader is encouraged to use additional security resources to further investigate security mechanisms that implement and satisfy the security services discussed in this document.

5. REFERENCES

"All In One CISSP Certification Exam Guide", Shon Harris, McGraw Hill, 2002.

"Improving Surface Transportation Security – A Research and Development Strategy", National Research Council, National Academy Press, Washington, D.C., 1999.

"Intelligent Transportation Systems (ITS) Information Security Analysis", Mitretek Systems, FHWA-JPO-98-009, November 1997.

"Making The Nation Safer – The Role of Science and Technology in Countering Terrorism", National Research Council, National Academy Press, Washington, D.C., December 2002.

"Protecting Our Transportation Systems: An Information Security Awareness Overview", Mitretek Systems, FHWA-OP-03-094 (Revised), April 2003.

"Regional ITS Architecture Guidance – Developing, Using, and Maintaining an ITS Architecture for Your Region", National ITS Architecture Team, FHWA-OP-02-024, October 7, 2001.

RFC 2828: Internet Security Glossary

"Security Architecture: Design, Deployment, and Operations", King, C., RSA Press, 2001

Various NIST SP-800 Series Publications including "Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, 1992.

Appendix A

A.1 Security Services

This appendix contains descriptions of security services (also known as safeguards or countermeasures) that are mapped to the National ITS Architecture. The security services applied to the National ITS Architecture are selected based on support for specific security objectives and protection against identified threats.

A.1.1 Information Security

Information Security deals with securing the origin, transmittal and destination of the information itself. Information security services include: confidentiality, integrity, availability, accountability, authentication, auditing and access control. Security services can be directed towards the potential for an attack as well as countering the attack after it has occurred.

A.1.1.1 Confidentiality

The system should prevent unauthorized disclosure of information deemed sensitive.

A.1.1.2 Integrity

The system should ensure that information is protected from unauthorized intentional or unintentional modifications.

A.1.1.3 Availability

The system should protect critical ITS services in order to prevent degradation or denial of the ITS services to users of the services. Single points of failure should be avoided.

A.1.1.4 Accountability

The system should provide protection against a sender of an information transmission later denying that they sent the information. The system should provide protection against a receiver of an information transmission later denying that they received the information. This concept is known as Non-Repudiation or Accountability.

A.1.1.5 Authentication

The system should verify the identity of a user and/or other system prior to granting access to a requested resource.

A.1.1.6 Auditing

The system should have the capability to trace ITS subsystem and individual user actions and activities. The auditing function of the system places the actions and activities in an audit trail that is protected from unauthorized access and modification.

A.1.1.7 Access Control

The system should limit access to the resources of a subsystem to only those users and other subsystems that are properly authorized. After authenticating an entity, the system should have the capability to limit system access to information or resources based on that entity's access privileges. The system should limit software modifications and upgrades to users and other systems that have authorization.

A.1.2 Operational Security

Operational Security is responsible for protecting ITS assets against both physical and environmental threats. This area provides monitoring, access control, configuration control and security incident and materials management of critical ITS assets.

A.1.2.1 Physical and Environmental Protection

The system should protect against adverse environmental conditions (e.g., temperature extremes, moisture and humidity, wind, dust). The system should provide capabilities to minimize the affects of power disruptions and surges. The system should protect against telecommunications failures. The system should provide capabilities like fire prevention, detection, and suppression.

A.1.2.2 Physical Access Control

The system should prevent unauthorized physical access to critical ITS facilities, field equipment, and other ITS assets. The system should log all attempts to physically access ITS facilities, field equipment, and other assets. The system should notify operations staff when a breach of physical access is attempted.

A.1.2.3 Security Monitoring

Critical ITS facilities, field equipment, and other ITS assets should be monitored. Manual and automated alarms should be provided.

A.1.2.4 Security Incident Management

Security incidents should be actively managed via identification, operations, and recovery. The incident should be reviewed and analyzed to determine how to improve security to prevent future occurrences. Procedures should be deployed that manage these incidents, including the review and analysis processes. These procedures should be continually improved and updated to mitigate future occurrences of the same type of incident. This could include defining different types of security incidents, and the procedures in place for preventing future occurrences of each – these procedures may be different depending on the type of incident.

A.1.2.5 Contingency Planning

Operational continuity and disaster recovery plans should be prepared and periodically tested and revised to ensure the integrity and continuity of operations and minimize the impact to the system from a disaster. The system should implement a comprehensive strategy for backup and restoration.

A.1.2.6 System Maintenance

Only authorized software, hardware, and devices should be installed or used. System changes should be documented, authorized, and tested prior to deployment. Change management procedures should be used.

A.1.2.7 Sensitive Materials Management

Sensitive information should be securely stored, protected, and properly disposed of.

A.1.3 ITS Personnel Security

This security service ensures that ITS personnel do not inadvertently or maliciously cause harm to ITS assets and have proper training in the event there is a security-related incident.

A.1.3.1 Personnel Screening

ITS Personnel with access to sensitive information or in security-critical positions should be subject to pre-employment screening, including background checks when appropriate per the security policy in effect. ITS Personnel in these sensitive positions should be subject to periodic reinvestigation.

A.1.3.2 Supervisory Controls

Supervisory practices should be followed that ensure that ITS Personnel roles and responsibilities are properly exercised.

A.1.3.3 Awareness and Training

All critical ITS Personnel should be trained on relevant security policies, practices, and guidelines.

A.1.3.4 Separation of Duties

Duties should be identified such that one person acting alone cannot compromise the security of critical ITS services. Job rotation should be used for sensitive ITS positions.

A.1.3.5 Least Privilege

ITS Personnel should be granted the level of access needed to fulfill their role and no more.

A.1.3.6 Accountability

ITS Personnel should understand their responsibility and be accountable for their actions. Audit trails and logs should be reviewed to detect improper access.

A.1.3.7 Termination

The system should prevent unauthorized access by transferred or terminated employees.

A.1.4 Security Management

The security management service connects all of the other security services together in order to provide security controls throughout ITS. Security Management ties in with the

Information, Operational, and Personnel security aspects of securing ITS as well as the eight security areas described in section 2.2. The security management service includes user and system assignment of appropriate access control, password management and a host of other security mechanisms.

Security Management is often implemented by a combination of manual and automated controls. Security Management includes the definition, implementation, and enforcement of the following: security policies and procedures, roles and responsibilities, and system configuration. System configuration management provides the means for ensuring all aspects of the ITS deployment are configured to provide an effective, efficient, and secure operating environment. Interfaces between architecture entities should be designed and implemented such that each security-related specific interface has minimal and closely controlled functionality in providing system access.

Appendix B

B.1 Subsystem Security Descriptions

Version 5 of the National ITS Architecture defines 22 subsystems, each of which have potential security considerations. This appendix provides a description of these potential security considerations for each subsystem. These high-level descriptions are intended to highlight the confidentiality, integrity, and availability objectives that apply to each subsystem. Because of the breadth of function and diverse nature of the processing within each subsystem, the specific security considerations for a given ITS implementation must be developed by understanding the objectives, threats, and the system vulnerabilities to these threats.

B.1.1 Archived Data Management

The Archived Data Management Subsystem security considerations are directly related to the sensitivity of the data contained in the archive. Some ITS archives include crash reports, personal information, and other sensitive information that requires significant security safeguards. Most archives are much less sensitive, containing bulk ITS information that is not confidential and does not require special security measures. Like confidentiality, the required availability of each archive must be considered based on the archive's application. In many, but not all, cases, archives are used for off-line applications where short-term loss of availability will not cause serious impact to the transportation system. In many cases, the most critical objective for data archives will be data integrity. Since archives are frequently used to measure performance of the transportation system and provide data that supports operations and planning, the accuracy and reliability of the data contained in the archive is paramount. Each archive should be reviewed by the system manager and data owners to ensure that security is consistent with the sensitivity of the archived data.

B.1.2 Commercial Vehicle Administration

The Commercial Vehicle Administration Subsystem manages credentials, financial data, border clearance, safety data, and other sensitive information. In general, the Commercial Vehicle Administration Subsystem handles personal and business sensitive information, such as financial data information that needs to have a relatively high degree of confidentiality in order to safeguard the information. In addition, it is important that the information is available in order to ensure that cargo is transported as safely and efficiently as possible. The integrity of the information is also important to consider in order to prevent unauthorized clearance.

B.1.3 Commercial Vehicle Check

The Commercial Vehicle Check Subsystem contains safety and credentials data to support electronic screening. The safety data also supports roadside safety inspections. For international borders, data from trade regulatory agencies (i.e. Department of Homeland Security) supports commercial vehicle border screening. In general, the Commercial Vehicle Check Subsystem handles personal and business sensitive commercial vehicle information that needs to have a relatively high degree of confidentiality in order to safeguard the information. In addition, it is important that the information is available to support safety inspections and electronic screening for safe and efficient commercial vehicle checking. The integrity of the information is also important to consider in preventing possible deceptive screening.

B.1.4 Commercial Vehicle Subsystem

The Commercial Vehicle Subsystem contains screening and safety data, and is used to support roadside electronic screenings. Cargo content information should be protected from unauthorized access for knowledge of this information, especially security sensitive HAZMAT cargo, could target the vehicle for hijacking or terrorist attack. In support of driver authentication, driver identity characteristics (i.e. biometrics, Personal Identification Number (PIN)) would be stored on-board the vehicle and appropriate measures should be taken to protect this personal information. In general, the Commercial Vehicle Subsystem handles personal and business sensitive information about the commercial vehicle including container content information that needs to have a relatively high degree of confidentiality in order to safeguard the information. In addition, it is important that the information about the commercial vehicle and its cargo is available to the Commercial Vehicle Administration subsystem. The integrity of the information from the commercial vehicle is also important to prevent deceptive practices.

B.1.5 Emergency Management

The Emergency Management Subsystem provides critical functions that directly impact public safety. It handles sensitive information, must "operate through" and be available in distressed environments, and is subject to numerous threats including both physical and cyber attacks. The Emergency Management Subsystem represents an extremely broad group of call-taking, dispatch, command post, and operations centers. In addition to these public safety and emergency management centers, the Emergency Management Subsystem also represents private sector telematics service providers, service patrol dispatch systems, and security monitoring systems. Each of these systems has unique security vulnerabilities that must be considered in defining appropriate security services.

Systems represented by the Emergency Management Subsystem operate in environments ranging from tightly controlled, secure command centers through open field environments when command posts are established in the vicinity of a major incident or disaster. The command post environment, with its reliance on wireless communications and relative lack of physical and environmental protection, has different vulnerabilities than systems operating in a fixed center. The availability requirements for an individual center must be assessed in the context of the concept of operations for the region. For example, the availability requirements for a service patrol dispatch system may not be high because the dispatch operation may be moved to an emergency operations center in times of crisis. The emergency operations center would have much more stringent availability requirements in this scenario. Similarly, the sensitivity and value of the information handled by each specific system must be evaluated to determine appropriate security safeguards for integrity and confidentiality. While it is good practice for all systems, a rigorous evaluation of security objectives, threats, vulnerabilities, and countermeasures is particularly important for each system represented by the Emergency Management Subsystem.

B.1.6 Emergency Vehicle

The Emergency Vehicle Subsystem (EVS) is the communications lifeline that connects emergency personnel in the field with emergency dispatch, other emergency personnel, and other resources that support emergency response. The EVS handles potentially sensitive information, must "operate through" and be available in distressed environments, and is exposed to numerous threats including eavesdropping (disclosure), unauthorized access or control, and disruption of services. Although confidentiality is a concern, the most critical security objectives for EVS are availability and integrity - the services and information provided by EVS must be available and accurate so that incident response is not degraded. Although the EVS provides the same basic driver communications, tracking, and routing functions that are provided by the other fleet vehicle subsystems, these functions are frequently safety critical for this subsystem since they directly impact the ability to provide an effective response to emergencies, which in turn impacts public safety.

The EVS represents a wide range of vehicles including police cruisers, command vehicles, various types of fire apparatus, service patrol vehicles, ambulances, towing and recovery vehicles, and many different specialized response vehicles. This collection of vehicles may have very different security requirements, depending on the functions supported, the data that is stored, and the mission criticality of the services provided. For example, maintaining confidentiality of police vehicle locations is a public safety concern and frequently a key security objective. Tow vehicle locations are generally not a public safety concern, but tow truck operators may still want to prevent unauthorized vehicle location disclosure for business reasons. Finally, the current location of a service patrol vehicle may not be considered to be particularly sensitive.

There are also other variables that impact security that are independent of vehicle type. For example, initial EVS data services will supplement voice communications that frequently will continue to carry all mission critical information. The security requirements for these initial implementations might be less robust until the agency gains experience with the EVS data services and begins to rely on them for mission critical information. As the role of the data services evolves and expands, the security requirements and the systems themselves must be revised so that mission critical systems are available and reliable when they are needed most. The specific analysis of the security objectives, threats, vulnerabilities to those threats, and appropriate security services to address the vulnerabilities should be undertaken for systems associated with the EVS.

B.1.7 Emissions Management

The Emissions Management Subsystem processes vehicle emissions data and regional air quality data that are generally not sensitive to public disclosure. Also, while air quality is extremely important to everyone, the services provided by the Emissions Management Subsystem are generally not mission critical and could be lost or delayed for short periods of time without serious implications for public safety or operational efficiency of the transportation system. In most cases, normal precautions that are taken to protect data integrity will also suffice here since the threat of inadvertent or malicious tampering with data is not particularly high.

There are scenarios where the security associated with Emissions Management will be more significant. For example, data integrity and confidentiality are more significant if the specific emissions management system is identifying emissions/pollution violators and collecting personal information and evidence of infractions. This information is both sensitive and subject to tampering. In most cases, system availability will not be critical, but a specific system may require higher availability if the network of sensors and data collected are relied upon to detect and report dangerous levels of pollutants or other airborne materials in emergency situations.

B.1.8 Fleet and Freight Management

The Fleet and Freight Management Subsystem is responsible for submitting credential applications, enrolling in international goods movement programs and paying tax bills, which contain personal and financial data. Driver identification information, including biometric parameters, is managed by this subsystem and it contains sensitive personal information. Since knowing freight equipment locations and cargo contents, especially security sensitive HAZMAT could lead to unintended consequences like hijackings or terrorist acts, security measures should be in place to protect this information. In general, the Fleet and Freight Management Subsystem handles personal and business sensitive information, including financial data, that needs to have a relatively high degree of confidentiality in order to safeguard the information. In addition, it is important that the location and cargo content information is available. The integrity of the information is also important to prevent deceptive practices.

B.1.9 Information Service Provider

The Information Service Provider security considerations are related to the sensitivity of the requests being made for information as well as the sensitivity of the information being provided. Some ISPs may charge their clients for information and services, in which case security measures should be in place to protect the client's personal information including their credit information as well as unauthorized access to premium services. Information such as evacuation information and emergency alerts can jeopardize public safety if the information is unauthorized, inaccurate, or not delivered in a timely fashion. Traveler information that contains financial data or other highly sensitive information should have a relatively high degree of confidentiality in order to safeguard the information. In addition, it is important that traveler information is available in times of crisis. The integrity of the information is also important to prevent deceptive practices. Most traveler information will not require this level of safeguarding.

B.1.10 Maintenance and Construction Management

The security considerations for the Maintenance and Construction Management Subsystem relate to the physical security of transportation assets and maintenance personnel. This subsystem is involved in coordinating the response to certain incidents by dispatch, routing and allocating maintenance vehicles and other resources in coordination with other center subsystems. This subsystem collects and processes environmental sensor information from the roadside that might contribute to the detection, classification and response to security threats. In general, the Maintenance and Construction Management Subsystem's information security needs to have a relatively low degree of confidentiality in order to safeguard the information. In addition, it is important that the information is available and has integrity in order to prevent improper reporting of assets needed to support emergencies.

B.1.11 Maintenance and Construction Vehicle

The security considerations for the Maintenance and Construction Vehicle Subsystem relate to physical security of the vehicle, operators and the roadway on which the vehicle operates. The maintenance vehicles can be mobile environmental sensing platforms that could contribute to the detection, classification and response to security threats. Maintenance vehicles might be deployed as movable barriers in response to certain security threats. In general, the Maintenance and Construction Vehicle Subsystem's information security needs to have a relatively low degree of confidentiality in order to safeguard the information. In addition, it is important but not essential that the information is available and has integrity in order to prevent improper reporting of the vehicle's location and sensing capabilities.

B.1.12 Parking Management

The primary security consideration for the Parking Management Subsystem is related to the financial information collected from the customer vehicles and exchanged with center subsystems for electronic payment processing. Additional security sensitivity is for the personal information associated with electronic accounts used for parking payment. Parking lots may be capable of uniquely identifying each vehicle that enters and exits, for the purpose of computing the correct parking fee, and this information could also be used for security purposes. High profile parking lots may require special monitoring and classification of vehicles requiring a relatively higher degree of confidentiality, availability and integrity of the information than most parking lots.

B.1.13 Personal Information Access

Security considerations for Personal Information Access include the measures necessary to safeguard the personal and financial information that may be entered by individual users. Personal Information Access subsystem equipment is typically privately owned and operated, and includes the use of portable or handheld devices. Devices such as these are prone to theft and misuse. Information coming from these personal devices should be authenticated to verify that the requester is who they say they are and that the information they are given is limited to the information requested or to information that is available to the public. In general, the Personal Information Access Subsystem handles personal and financial information that needs a relatively low degree of confidentiality to safeguard the information. In addition, it is important but not essential that the information is available. The integrity of the information is also important in order to prevent improper financial transactions and accessibility to unauthorized information.

B.1.14 Remote Traveler Support

The Remote Traveler Support subsystem security considerations relate to the potential locations of the types of equipment included in this subsystem. Kiosks and other publicly accessible information access points can be target areas for criminal elements trying to rob or harm travelers. As such the RTS should include appropriate physical security measures including the placement in well-lit areas and the use of video and audio surveillance to secure the use of the equipment. Travelers may be using the RTS to request emergency services and measures should be in place to secure the information and ensure the availability and integrity of the system. Travelers may also be using the RTS to make reservations and trip plans that involve the transmission of personal and financial data. Those transactions should also be secured.

B.1.15 Roadway

The security considerations for the Roadway Subsystem (RS) are directly related to the types of field equipment that are included in a particular implementation. The RS performs a broad range of roadway network monitoring and control services and includes both safety-critical and non-safety critical systems.

Safety-critical systems include traffic signal systems, gates and barriers that control facility access, and future systems that may support automated vehicle control systems. Since improper operation of these systems can directly endanger motorists, security services should be established so that these systems operate with very high levels of integrity and availability and system operation degrades in a fail-safe manner. In contrast, the information associated with operation of these systems is not confidential and typically will not need special measures to protect it from disclosure.

Surveillance and environmental sensor systems provide information that may be safety critical if this information is used to monitor for incidents or dangerous road conditions. Although malicious tampering is possible, the more likely threats to sensor and surveillance information involve inadvertent loss or corruption of the provided information. Again, availability and integrity are the paramount security objectives. Although the surveillance and sensor data is generally not sensitive to disclosure, confidentially is important when CCTV cameras are zoomed in on a crash and other scenarios where individuals can be identified from the surveillance data.

The driver information systems included in the RS, such as dynamic message signs and highway advisory radio, are generally not considered to be safety-critical, but have their own set of security considerations. These systems are perhaps the most likely in the RS to be the target of unauthorized access attempts and must be protected against such attacks by emphasizing security services that enhance integrity. The availability requirements associated with DMS and HAR may increase as these systems are used increasingly in critical services like Amber Alert.

Other RS systems, including traffic detectors and probe beacons, do not have special security considerations since temporary loss or disruption of these systems generally won't impact public safety and these systems are unlikely to be subject to malicious attacks. Standard good-practice security considerations should be sufficient for most of these systems.

B.1.16 Security Monitoring

The Security Monitoring Subsystem (SMS) includes surveillance and sensor equipment used to provide enhanced security and safety for transportation facilities or infrastructure. The SMS handles information used to support safe operation of the transportation system and to support emergency response. The threat sensor, object detection and infrastructure integrity monitoring equipment represented by this subsystem perform safety critical functions. Since improper operation of these systems can directly endanger motorists and communities, security services should be established so 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.

Although malicious tampering is possible, the more likely threats to SMS sensor and surveillance information involve inadvertent loss or corruption of the provided information. Again, availability and integrity are the paramount security objectives. The surveillance and sensor data is not meant for public disclosure so confidentially is important. Limited processing of collected sensor and surveillance data is also included in this subsystem to support threat detection and classification. Physical security around the SMS sensors and surveillance equipment may be necessary to protect the equipment from usurpation and disruption.

B.1.17 Toll Administration

The primary security consideration for the Toll Administration Subsystem is related to the financial information collected from the field and exchanged between other agencies using common electronic payment media that needs to have a relatively high degree of confidentiality in order to safeguard the information. Additional security sensitivity is for the personal information associated with electronic accounts. In addition, it is important that the information is available to the Toll Administration subsystem in order to ensure that tolls are properly accounted for. The integrity of the information is also important to consider in order to prevent disruption of toll fee collection operations.

B.1.18 Toll Collection

The primary security consideration for the Toll Collection Subsystem relates to the financial information collected in the field that is sent to the Toll Administration Subsystem, and to any personal information associated with the financial transactions.

Electronic toll payment needs to have a relatively high degree of confidentiality in order to safeguard the information. Additional security sensitivity is for the personal information associated with electronic accounts. In addition, it is important that the information is available from the Toll Collection subsystem to the Toll Administration subsystem in order to ensure that tolls are properly accounted for. The integrity of the information is also important to consider in order to prevent disruption of toll fee collection operations.

B.1.19 Traffic Management

The Traffic Management Subsystem (TMS) represents centers that control freeway systems, rural and suburban highway systems, and urban and suburban traffic control systems. This includes safety critical control of traffic signals, dynamic message signs, gates and barriers, and other traffic control equipment. It also supports important coordination with other centers to adapt traffic management to address incidents and the special needs of other systems and agencies. The majority of the information handled by the TMS is not particularly sensitive; public disclosure of DMS messages, traffic signal control plans, and the bulk of the other information managed by the TMS is not a key concern.

The integrity of this information is more important since the principal threats are those that allow undetected errors or unauthorized control of field equipment. For example, errors that cause loss of control of traffic signals or malicious attacks that usurp control of a dynamic message sign. Both insider and outsider attacks must be considered in developing the overall security strategy for a traffic management center. Availability may also be important, depending on the role of the specific traffic management center in the region.

State, regional, and local traffic management centers are all represented by the TMS. In addition to traditional centers, the TMS also represents portable computers and other simple solutions that allow remote monitoring and control of field equipment. Each of these implementations may have different implications for security. For example, a regional traffic management center may take control from a local traffic management center during off-hours and under special circumstances. In these types of implementations, the security-related availability requirements could be much more stringent for the regional traffic management center and the associated remote control capability than they would be for the local traffic management center.

The functions performed by a specific TMC and the ability of the Roadway Subsystem to operate autonomously when the TMC is off-line are also factors that determine how critical availability is for a particular TMC. While confidentiality is not a special concern for most traffic management data, confidentiality may be important if the specific system supports speed enforcement, HOV occupancy enforcement, or other applications that identify specific vehicles and individuals and other information that must be protected from public disclosure.

B.1.20 Transit Management

The Transit Management Subsystem (TRMS) represents centers that control public transportation vehicle fleets, including buses and light and commuter rail, in rural, suburban, or urban settings. It provides operations (schedules, routes, fare structures), maintenance, customer information, planning and management functions for the transit property, and spans the central dispatch and garage management systems. Security considerations for the TRMS include safety critical control of the physical transit assets, operational security of the facilities that house the transit management center and the maintenance garage, and transit personnel security. The TRMS also supports coordination with other centers to adapt transit management to address incidents, event data, and the special needs of other systems and agencies, and to provide real-time information on current transit services. The majority of the information handled by the TRMS is not particularly sensitive; public disclosure of transit operational data, passenger loading, ridership, and vehicle maintenance data, and the bulk of the other information managed by the TRMS is not a key security concern.

The integrity of this information is more important since the principal threats are those that allow undetected errors or unauthorized control of physical transit assets, i.e., buses or light rail. For example, malicious attacks on the computer system that controls light rail would be a serious security concern. Both insider and outsider attacks must be considered in developing the overall security strategy for a transit management center. Security considerations at the Transit Management Center itself should include closing and locking outside doors, badge access to outside doors, at least password control when logging onto computers, a dispatcher in-house at all times service is operational, etc. Security considerations at the garage should include badge access to outside doors, password access when logging onto the bus (including transit vehicle operator authentication by the center).

From an information standpoint the primary security issues relate to financial transactions associated with electronic payment media or certain security sensitive operations, such as remote disabling of a transit vehicle during an incident such as a hijacking.

B.1.21 Transit Vehicle

The Transit Vehicle Subsystem (TRVS) is the communications path that connects transit personnel in the field with central dispatch at the transit management center. This subsystem provides the functions necessary to support the safe and efficient movement of passengers. Most of the information that is handled by the TRVS is not particularly sensitive except for financial transactions associated with electronic payment media, and the information flows used for operator authentication on the vehicle or remote vehicle disabling. Operator authentication is used to prevent unauthorized vehicle operation, and remote disabling is provided as one aspect of response to on-board threats.

The security considerations for the Transit Vehicle Subsystem relate to physical security of the vehicle, transit vehicle operators, and travelers using the vehicle. The TRVS is exposed to certain threats including unauthorized access or control (hijacking) and disruption of services. Other security objectives for TRVS are availability and integrity – the services and information provided by the TRVS must be available and accurate so that transit operations are not degraded. The basic transit vehicle operator communications, tracking, and routing functions provided by the TRVS are not particularly sensitive from a security standpoint. They do not directly affect public safety – disruption of service would be mainly an inconvenience.

The TRVS represents a wide range of vehicles including articulated and double-decked buses, paratransit vehicles, ferryboats, light and commuter rail, monorail vehicles, school buses, trolley buses, vans, tow trucks, shelter service trucks. This collection of vehicles may have different security requirements, depending on the functions supported, the data that is stored, and the services provided. Passenger carrying transit vehicles have additional security concerns beyond those vehicles that do not carry passengers, namely the physical security of the passengers, and the protection of financial or personal information relating to electronic fare payment systems. For example, threat sensors, surveillance, and alarms are used to identify threats on-board a vehicle, and there are confidentiality issues associated with all financial transactions. The primary security consideration for supervisory or support vehicles is the physical security of the vehicle and the vehicle operator.

There are also other variables that impact security that are independent of vehicle type. For example, as new systems are deployed on a bus, the transit vehicle operator must become familiar and comfortable with their usage. Until the operator is familiar with these systems, they may be vulnerable to attack (or the information that is stored and sent to the TRMS may be vulnerable) and security may be an issue. The specific analysis of the security objectives, threats, vulnerabilities to those threats, and appropriate security services to address the vulnerabilities should be undertaken for systems associated with the TRVS.

B.1.22 Vehicle

The primary security consideration for the Vehicle Subsystem relates to the security of the basic vehicle and the driver and passengers in the vehicle. A vehicle Mayday capability might allow the driver or passengers to provide center subsystems with information about security threats or incidents. Various safety systems in the vehicle might protect the occupants from some security hazards. The electronic toll and parking payment capabilities expose the financial information of the owner to certain risks of unauthorized disclosure. In general, the Vehicle Subsystem needs to have a relatively high degree of confidentiality in order to safeguard transmitted information. In addition, it is important that the information about the vehicle is available to the Commercial Vehicle Administration subsystem. The integrity of the information from the commercial vehicle is also important to prevent deceptive practices.

Appendix C

C.1 Architecture Flow Group Descriptions

In this appendix defines the architecture flow groups where architecture flows have been placed based on unique security considerations. In cases where an architecture flow could be allocated to multiple groups, the most appropriate security group was chosen. Each architecture flow group has been given typical security service, security objectives and security threat classifications of high, medium, low or minimal. Similar architecture flows are grouped together so that security services can be consistently applied.

C.1.1 Archived Data

The "Archived Data" architecture flows support data archival and retrieval. Archives may include a broad range of information with varied sensitivity. The security considerations for this group are for the general case for archives with nominal data sensitivity. Each specific archive must be evaluated so that appropriate security services can be identified, commensurate with the sensitivity and value of the information contained.

C.1.2 Business Sensitive

The "Business Sensitive" architecture flows carry information that could be deemed sensitive by a commercial firm. This information is critical to the businesses involved, and its accuracy is important to both the business and agencies that manage and monitor this information.

C.1.3 Emergency

The "Emergency" group includes architecture flows that support emergency response and related critical public safety activities. These flows have critical availability and integrity requirements.

C.1.4 Enforcement/Crash Reporting

The "Enforcement/Crash Reporting" architecture flows carry information about individual drivers that is used for crash reporting and enforcement applications. These flows carry sensitive information that can violate privacy principles if disclosed to unauthorized sources.

C.1.5 Financial/Personal

The "Financial/Personal" architecture flows can carry sensitive financial or personal information. The value of the information makes these flows subject to theft, fraud, and other disclosure threats.

C.1.6 Map Data

The "Map Data" architecture flows carry geospatial "map" information that is used in the operation of ITS.

C.1.7 Media

The "Media" architecture flows support distribution of information to the media. The loss or inaccuracy of this information can inconvenience the traveling public and potentially impact the reputation of the providing agency.

C.1.8 Not Applicable

The "Not Applicable" group includes architecture flows that do not carry information; for example, flows that represent the physical environment.

C.1.9 Operational Information

The "Operational Information" architecture flows carry information that is used to support operation of the transportation system. While not intended for general public distribution, this information has no special sensitivity. Transportation system operation does rely to some degree on the information's integrity and availability.

C.1.10 Operational Information – Safety

The "Operational Information – Safety" architecture flows carry information used to support operation of the transportation system that is safety critical; the loss of such information could impact public safety. The primary security considerations for these flows are ensuring the integrity and availability of the information.

C.1.11 Public

The "Public" group includes architecture flows that have no specific security sensitivity. These flows are not sensitive with respect to confidentiality, integrity, or availability.

C.1.12 Secure Human Interface

The "Secure Human Interface" architecture flows carry sensitive and safety critical data to and from operators and drivers (e.g., Mobile Data Terminal in a law enforcement vehicle).

C.1.13 System Control

The "System Control" architecture flows are used to control ITS systems. These flows should be protected so that only authorized individuals or systems can control these systems.

C.1.14 Traveler Information

The "Traveler Information" architecture flows carry traveler information, the loss of which can provide inconvenience to the traveling public and potentially impact the reputation of the providing agency.

C.1.15 Traveler Information – Safety

The "Traveler Information – Safety" architecture flows distribute information to the traveling public that is safety-critical. Information like evacuation information and emergency alerts can jeopardize public safety if the information is unauthorized, inaccurate, or not delivered in a timely fashion.

C.1.16 Weather/Environmental

The "Weather/Environmental" architecture flows carry weather and environmental information that is used for operational purposes. This is generally public information, but it must be accurate and available to support transportation system operation.