U.S. Department
of Transportation
Federal Highway
Administrahon

State of Maryland
Intelligent Transportation Systems
Security Requirements Recommendations

November 1997

Intelligent Transportation Systems
Joint Program Office

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-98-013		

4. Title and Subtitle	5. Report Date
STATE OF MARYLAND INTELLIGENT TRANSPORTATION SYSTEMS SECURITY REQUIREMENTS RECOMMENDATIONS	NOVEMBER, 1997
	6. Performing Organization Code
7. Author(s) James Ruby, Dan King, and Larry Gunshol	8. Performing Organization Report No.
9. Performing Organization Name and Address Computer Sciences Corporation Systems Engineering Division 7471 Candlewood Road Hanover, MD 21076	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTRS-57-95-C-0044
	13. Type of Report and Period Covered
12. Sponsoring Agency Name and Address Department of Transportation FHWA Intelligent Transportation Systems Joint Program Office 400 Seventh Street, S.W. - Room 3422 Washington, D.C. 20590	14. Sponsoring Agency Code HVH-1

15. Supplementary Notes

Bill Jones

16. Abstract

At the direction of the Volpe National Transportation Systems Center of the US Department of Transportation (US DOT), a two-phase study of the security vulnerability of Maryland Intelligent Transportation Systems (ITS) was conducted from July until November 1997. The Phase 1 report, State of Maryland Intelligent Transportation Systems Security Requirements Recommendations, developed specific security requirements for Maryland ITS. These reports continue the exploration of ITS security issues identified in the Intelligent Transportation Systems (ITS) Information Security Analysis report prepared for the US DOT Joint Program Office in May of 1997, Project Number 0996180%OA.

17. Key Words	18. Distribution Statement
Intelligent Transportation Systems, Security, Maryland	No restrictions. This document is available to the public from: The National Technical Information Service Springfield, VA 22161

19. Security Classif. (of this report)	20. Security Class (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	71	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Table of Contents

List of Exhibits

Preface

At the direction of the Volpe Center of Cambridge, Massachusetts, a two-phase study has been conducted of the security vulnerability of Maryland Intelligent Transportation Systems (ITS). This Phase 1 document, *State of Maryland Intelligent Transportation Systems Security Requirements Recommendations,* develops specific security requirements for Maryland ITS systems while the Phase 2 document, *State of Maryland Intelligent Transportation Systems Security Implementation Recommendations,* specifically focuses on candidate security countermeasures for Maryland ITS.

The study of the security vulnerability of Maryland ITS continues the exploration of ITS security issues initially identified in the *Intelligent Transportation Systems (ITS) Information Security Analysis* (Bibliography, Item 1) which was prepared for the U.S. Department of Transportation Joint Program Office (JPO). In that study, generic data flows were identified for ITS systems based on the National ITS Physical Model and these flows were assessed to identify the various security threats to ITS subsystems, their exchange of information, and their supporting communications infrastructure. This current study continues that work by analyzing the ITS data flows for a specific case-Maryland ITS-and identifying specific security measures which could be applied to protect those data flows.

Ms. Alisoun Moore, CIO of MDOT, was particularly helpful in identifying appropriate ITS contacts within MDOT and other Maryland modals from whom information could be obtained on current ITS programs and security practices. Mr. William S. Jones, Technical Director of the ITS JPO, U.S. Department of Transportation (US DOT), and Ms. Kelly Coyner, Acting Research and Special Programs Administrator (RSPA), US DOT, also supported the sponsorship and direction of the task. While their help is very much appreciated, we must caution that the views expressed herein are solely those of the authors.

This report was prepared under the direction of

Kevin F. Harnett, Project Manager
Volpe National Transportation Systems Center, US DOT
Kendall Square, DTS-78
Cambridge, MA 02142
(617) 494-2604, Fax (617) 494-2684, Email: Harnett@volpel.dot.gov

The Computer Sciences Corporation (CSC) Project Director for this work was Jim Ruby, Senior Consulting Engineer, with contributions by Larry Gunshol and Dan King, both of CSC.

Executive Summary

This Phase 1 document defines security requirements for Maryland Department of Transportation (MDOT) Intelligent Transportation Systems (ITS). It complements work already completed for the U.S. Department of Transportation Joint Program Office (JPO) and documented in *Intelligent Transportation Systems (ITS) Information Security Analysis* (Bibliography, Item 1). That document defined general ITS security requirements based on the National ITS Architecture.

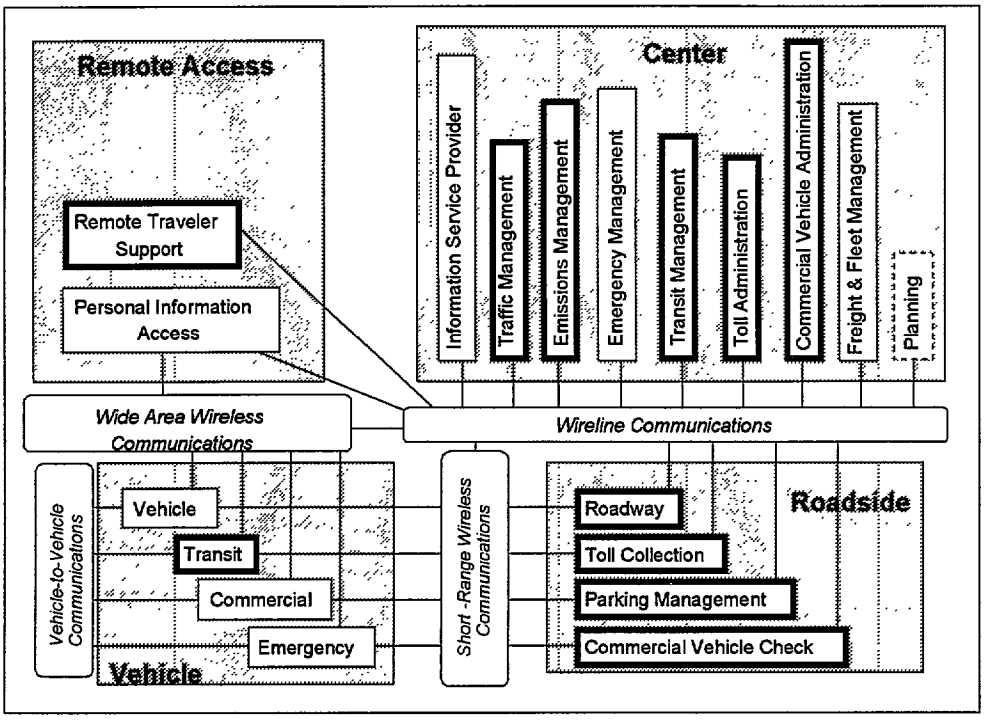
One of the key questions that remained unanswered at the completion of the original JPO study was whether or not generalized security requirements developed from the National ITS model could be successfully translated into specific requirements for an individual ITS network. This report offers some answers to that question as well as providing security requirements for MDOT's ITS.

Another relevant document is *ITS Information Security Awareness* scheduled for publication by the JPO in the fall of 1997. This latter document will be directed to senior level transportation managers and is intended to increase the awareness of information security.

The National ITS Physical Architecture and Intelligent Transportation Infrastructure (ITI)

The National ITS Physical Architecture model is shown in Exhibit ES-1. It is composed of four major systems and 19 subsystems that support ITS Functions. Those functions that are the responsibility of MDOT are outlined with "bold" borders.

Exhibit ES-1. National ITS Physical Architecture Model



The specific MDOT modals responsible for each of these functions is shown in Exhibit ES-2.

Exhibit ES-P. Map of MDOT Modals to National ITS Architecture Subsystems

	System										
	Center					Roadside				Vehicle	Remote Access
MDOT Modal	CVAS	EMMS	TAS	TMS	TRMS	CVCS	PMS	RS	TCS	TRVS	RTS
Maryland Aviation Administration (MAA)							■				
Maryland Transportation Authority (MdTA)		■	■	■				■	■		
Mass Transit Administration (MTA)					■					■	■
Motor Vehicle Administration (MVA)	■					■					
State Highway Administration (SHA)				■				■			

■ Responsible Organization

The systems and subsystems are not, however, ends in themselves. They support the Intelligent Transportation Infrastructure (ITI) which is generally considered to include the following functions:

- Traffic Signal Control
- Freeway Management
- Transit Management
- Incident Management
- Electronic Fare Payment
- Electronic Toll Collection
- Railroad Grade Crossing
- Emergency Management Services
- Regional Multimodal Traveler Information

In addition, commercial vehicle operations are now frequently included in this infrastructure. While the focus of this report is on individual ITS subsystems and data flows, it is the ITI supported by these subsystems which constitutes the real "business areas" of MDOT-the services MDOT provides to the citizens of Maryland.

The Problem

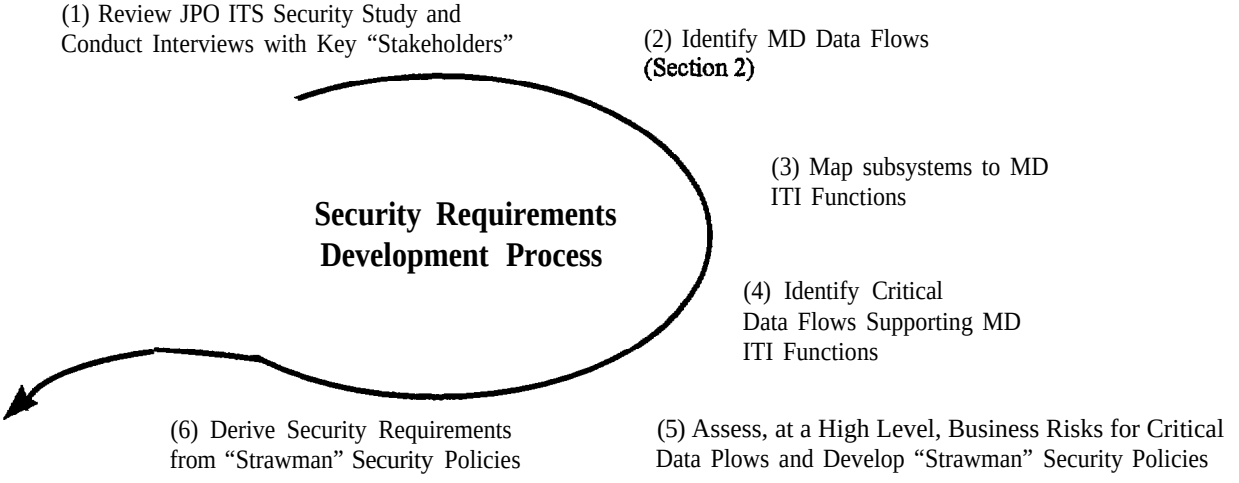
All of the ITI functions cited above are essential to the welfare of the citizens of Maryland. Unfortunately, as these functions have become more and more dependent on information processing for their control, maintenance, and operation they have also become more and more vulnerable to security attack. The **availability** of these ITS systems can be interrupted through accident or intentional sabotage thereby disrupting traffic and precluding toll and fare collection. The **confidentiality** of personal, financial, and commercial proprietary information contained in the systems can be violated and used for personal monetary gain or competitive advantage. The **integrity** of the information contained in the systems can be modified to support fraudulent

activities and the associated loss of tax, license, toll, and fare revenue to the state. Each of these security issues-availability, confidentiality, and integrity-will be examined for MDOT's ITS systems and the ITI functionality they support.

The Approach

The process followed in the examination of each of these issues is shown in Exhibit ES-3.

Exhibit ES-3. Security Requirements Development Process



Interviews were conducted with key MDOT "stakeholders" having responsibility for ITS to identify which data flows included in the national model existed for Maryland and to identify other data flows which existed in Maryland but were not included in the national model. The interviews were documented and the relevant portions shared with those interviewed to ensure accuracy. The final result of the interview process was the identification of a large number of data flows but without any indication as to which of those flows were the most critical to the support of the Maryland ITI.

To assist in the identification of the most critical data flows, each of the ITS subsystems included in the national model was "mapped" to the ITI function it supported, i.e., traffic signal control, freeway management, transit management, electronic fare payment, toll collection, commercial vehicle operations, etc. Those data flows that were essential to support these functions were then identified as critical.

With that information, a high level business security risk analysis was performed on critical data flows to develop "strawman" security policies on which to base recommended ITS security requirements. Business risk analysis compares the subjective cost of losing a resource relative to the subjective cost of ensuring its availability. Clearly, all threats cannot be protected against, so those that provide the greatest business risk must be identified, and countermeasures implemented.

The Results

Theresults of this process are specific security requirements for the MDOT ITS. Certain of those requirements apply to all four ITS systems and these general requirements are presented first followed by the same four system groupings used in the ITS model-Center, Roadside, Vehicle, and Remote Access (Traveler) systems. Requirements for each system can be summarized as follows:

General ITS Security Requirements

a) Devices utilized to provide ITS security must be based on open standards, conform to appropriate security standards where such standards exist, communicate utilizing international or U.S. standards based protocols, and employ commercial off-the-shelf (COTS) technology that has been subjected to due diligence whenever possible.

b) A formal, role-based access approval procedure for individual users should be implemented and enforced for each Center system and Center System data processing facility and should be used to adhere to a principle of "least privilege."

c) All custom software applications should successfully pass formal test procedures prior to installation in ITS.

d) ITS security requirements should be incorporated into planning for and the design of all new ITS and any invitation for bids or other solicitation for ITS or ITS components should include security as a weighted evaluation factor.

e) Configuration management must be exercised on all ITS software and hardware systems.

f) An MDOT ITS Security Officer should be appointed by the Secretary to ensure compliance with established ITS security standards and perform internal system audits. Further, consideration should be given to the establishment of an ITS Security Working Croup to support the State Data Security Committee.

g) A formal contingency/disaster recovery plan and procedures must be established for each ITS system and contingency/disaster recovery procedures should be tested on a periodic basis.

h) ITS operational data should be backed up as appropriate to their criticality and a copy stored off site consistent with contingency/disaster recovery plan procedures.

i) An information processing security training and awareness program must be implemented for ITS.

Center Systems

a) Center System application, communication, data, and file servers (sewers) should implement a role-based identification and authentication policy and mechanism sufficiently robust to protect system criticality.

b) Center System role-based access control mechanisms should be used to enforce a *least privilege* security policy.

c) Each user of Center System servers should be assigned a unique identifier to support *least privilege* access control processing.

d) Each user of Center System sewers should be assigned a unique personal authentication code, such as a password, to authenticate their unique identifier.

e) Each Center System *server* should implement an audit function appropriate to the criticality of the system.

f) Center System server remote access controllers should incorporate mechanisms to defeat masquerade of an authorized user by malicious attack.

g) Direct access to Center System *servers* from Intranets, Extranets, and the Internet should be inhibited.

h) An appropriate mechanism should be implemented to continuously validate the integrity of data entering a Central System.

i) An appropriate mechanism should be implemented to continuously authenticate the source of data entering a Central System.

j) A mechanism should be implemented to ensure non-repudiation of appropriate data entering a Central System.

k) A mechanism should be implemented for Central System sewers to guarantee the integrity and authenticity of data they provide to other systems.

l) A mechanism to uniquely identify individuals authorized unrestricted access to Center System data processing facilities should be implemented.

m) Communications between Center Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information to other ITS and terminator subsystems should utilize pair-wise encryption.

Roadside Systems

a) Communications between critical Roadside Systems and their respective Center System and other ITS and terminator subsystems should incorporate a sensor data integrity mechanism.

b) Communications between critical Roadside Systems and their respective Center System and other ITS and terminator subsystems should incorporate a sensor data authentication mechanism.

c) Communications between Roadside Systems that transfer credit card, personal identification number (PIN), an&or other sensitive information to their respective Center System and other ITS and terminator subsystems should utilize pair-wise encryption.

d) Communications between critical Roadside Systems and their respective Center System and other ITS and terminator subsystems should incorporate a data authentication mechanism.

e) Roadside System devices should include a mechanism to verify the integrity and authenticity of commands, program, and configuration data received.

f) Roadside System devices should include a mechanism to support identification and authentication of personnel utilizing the device craft/maintenance port.

Vehicle Systems

a) Vehicle System identification tokens (e.g., bar code tags) should include an anti-tamper mechanism to foil theft.

b) Vehicle System identification tokens (e.g., bar code tags) should include an authentication mechanism.

c) Vehicle System identification tokens (e.g., bar code tags) should include a non-repudiation mechanism.

d) Vehicle System identification tokens (e.g., bar code tags) should include an **integrity** mechanism.

e) Vehicle Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information should utilize pair-wise encryption.

f) Vehicle System transponder communications should incorporate a transponder data integrity mechanism.

g) Vehicle System data communications should incorporate a data integrity mechanism.

h) Critical Vehicle System transponder communications should incorporate a transponder data authentication mechanism.

i) Critical Vehicle System data communications should incorporate a data authentication mechanism.

j) Critical Vehicle System should include a mechanism to verify the integrity and authenticity of commands, program, and configuration data received.

k) Vehicle System devices should include a mechanism to support identification and authentication of personnel utilizing the device craft/maintenance port.

Remote Access Systems

a) Remote Access Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information should utilize pair-wise encryption.

b) Remote Access Systems should include a traveler identification and authentication mechanism for sensitive transactions.

c) Remote Access Systems should include a non-repudiation mechanism for sensitive transactions.

d) Remote Access Systems transactions should include a data authentication mechanism.

The development of the Maryland ITS security model is described in Section 2 of this report while the specific security requirements are discussed in Section 3. These requirements will serve as the basis for the subsequent development of specific security solutions for MDOT ITS systems that will be included in the Phase 2 report, *State of Maryland ITS Security Implementation Recommendations.*

Lessons Learned

As suggested at the beginning of this executive summary, one of the key questions which remained unanswered at the completion of the original JPO study was whether or not generalized security requirements developed from the National ITS model could be successfully translated into specific requirements for an individual ITS network. As this work has been conducted, some partial answers to that question have become apparent. There have been a few "lessons learned." These lessons are based only on the Maryland ITS but since Maryland is at the forefront of ITS development in the US, the lessons learned here are likely to apply to other states' efforts as well. These lessons include the following:

- While the goal is a fully integrated ITS structure, that is hardly the case today. Traffic management is handled by the State Highway Administration, some county governments, and the Maryland Transportation Authority; tolls by the Maryland Transportation Authority; fares

by the Mass Transit Administration and Maryland Aviation Administration; commercial vehicle operations currently reside in the Motor Vehicle Administration; etc. Each has developed systems, some centralized within the Motor Vehicle Administration Information Systems Center (ISC) and others decentralized as client/server systems, to meet their own requirements. Based on all information gathered during this study, there is no strategic plan for the integration (system integration, not organizational integration) of these ITS functions.

- Certain functions exist but are so dispersed that they cannot be specifically related to the National ITS Architecture model. By way of example, the Planning function included in the ITS model suggests a central point where statistics are collected and policies and directions are set for ITS within the state. Clearly, ITS planning does take place in Maryland but it is handled by individual modals within their sphere of interest. It does not currently take place within a single organizational entity.
- Many ITS subsystems cross organization boundaries which made it difficult to conform individual data flows to the model. Within the state, fares are collected by both the Maryland Aviation Administration for parking and the Mass Transit Administration for busses, Metro, Maryland Commuter Rail Passenger Service (MARC), etc. Traffic management within the State is handled by the State Highway Administration, but certain county governments such as Montgomery County also have extensive responsibilities in these areas. The databases for commercial vehicle operations under the Commercial Vehicle Information System and Networks (CVISN) project will reside not only on various Maryland systems but also within national clearinghouses maintained by the Federal Government. In short, actual data flows that must be protected are far more complex than suggested by the National model.
- Significant security issues can also be raised by the inclusion of new modals into systems that might otherwise be secure. For example, the CVISN system is being designed to include strong security measures. It is also likely that in time the Maryland Port Authority will interface with this system for the management of commercial vehicle traffic. However, the security measures in place within the Port Authority are less vigorous than those intended for CVISN. All systems that interface will have to be brought up to the same level of protection for security to be effective.
- It is more efficient to develop security requirements by examining the four major ITS systems as a whole rather than by focusing on the 19 individual subsystems. Each of the major systems has certain common characteristics that lead to similar security requirements. For example, those subsystems that comprise the Center system are generally mainframe or client/server systems located in MDOT facilities, controlled and operated by MDOT personnel, and connected by wireline technology. Roadside systems, on the other hand, are more accessible to the public and connected by a combination of wireline and wireless technology. Similar distinctions can be made with the other systems.
- The classification of threats into the three major categories of availability, confidentiality, and integrity is more than adequate for the development of requirements. While other studies have subdivided these threats into as many as six categories (denial of service, disclosure, manipulation, masquerading, replay, and repudiation) little was gained in the development of security requirements through the use of such narrow definitions.

While specific security requirements can be developed using the National ITS Physical Architecture as a guide, as this report demonstrates, doing so is more complex than suggested by the model and, to be as accurate as possible, requires the development of impact costs for potential security breaches and costs for the implementation of countermeasures.

1 Introduction

At the direction of the Volpe Center of Cambridge, Massachusetts, a two-phase study has been conducted of the security vulnerability of Maryland Intelligent Transportation Systems (ITS). This Phase 1 document, *State of Maryland Intelligent Transportation Systems Security Requirements Recommendations,* develops specific security requirements for Maryland ITS systems while the Phase 2 document, *State of Maryland Intelligent Transportation Systems Security Implementation Recommendations,* specifically focuses on candidate security countermeasures for Maryland ITS.

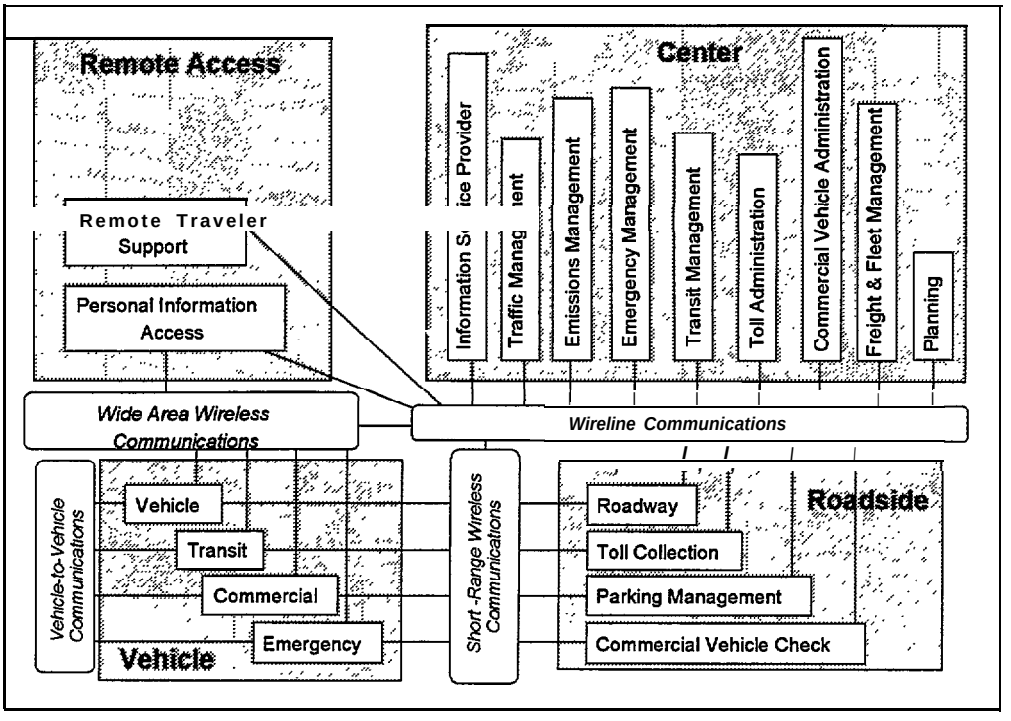
1.1 The National ITS Architecture

The National ITS Architecture provides a common conceptual model for the discussion of ITS related issues such as security. The architecture was developed over the past several years by the USDOT and ITS America with support from Lockheed Martin, Rockwell International, the Jet Propulsion Laboratory, and Mitretek Systems.

1.2 The ITS Physical Architecture Model

ITS architecture is the framework of interconnected subsystems that makes the collection, sharing, processing, and redistribution of ITS information possible. For the purposes of this report, the physical architecture model shown in Exhibit l-l best represents this architecture.

Exhibit 1-1. National ITS Architecture



The model consists of four major systems (indicated in bold text) and 19 separate subsystems. The four major systems indicate the locations where ITS functions are performed while the 19 subsystems represent the individual ITS functions. The lines shown between the various subsystems represent data flows between these systems. A brief description of these subsystems, extracted from the US DOT ITS web site, follows:

1.2.1 Center Subsystems

Center Subsystems deal with those functions normally assigned to public/private administrative, management, or planning agencies. The nine Center Subsystems are described below:

- Commercial Vehicle Administration - Sells credentials and administers taxes, keeps records of safety and credential check data, and participates in information exchange with other commercial vehicle administration subsystems and CVO Information Requesters,
- Fleet and Freight Management - Monitors and coordinates vehicle fleets including coordination with intermodal freight depots or shippers.
- Toll Administration - Provides general payment administration capabilities to support electronic assessment of tolls and other transportation usage fees.
- Transit Management - Collects operational data from transit vehicles and performs strategic and tactical planning for drivers and vehicles.
- Emergency Management - Coordinates response to incidents, including those involving hazardous materials (HAZMAT).
- Emissions Management - Collects and processes pollution data and provides demand management input to Traffic Management.
- Planning - Aids in optimal planning for ITS deployment. Collects and processes operational data from other Center subsystems, as well as the Parking Management Subsystem, and provides the results to Transportation Planners.
- Traffic Management - Processes traffic data and provides basic traffic and incident management services through the Roadside and other subsystems. The Traffic Management Subsystem may share traffic data with Information Service Providers. Different equipment packages provide a focus on surface streets or highways (freeways and interstates) or both. It also coordinates transit signal priority and emergency vehicle signal preemption.
- Information Service Provider - This subsystem may be deployed alone (to generally serve drivers and/or travelers) or be combined with Transit Management (to specifically benefit transit travelers), Traffic Management (to specifically benefit drivers and their passengers), Emergency Management (for emergency vehicle routing), Parking Management (for brokering parking reservations), and/or Commercial Vehicle Administration (for commercial vehicle routing) deployments. ISPs can collect and process transportation data from the aforementioned centers, and broadcast general information products (e.g., link times), or deliver personalized information products (e.g., personalized or optimized routing) in response to individual information requests. Because the ISP may know where certain vehicles are, it may use them as “probes” to help determine highway conditions, levels of congestion, and aid in the determination of travel or link times. This probe data may be shared with the Traffic Management Subsystem. The ISP is a key element of pre-trip travel

information, infrastructure based route guidance, brokering demand-responsive transit and ride matching, and other traveler information services.

1.2.2 Roadside Subsystems

These subsystems include functions that require convenient access to a roadside location for the deployment of sensors, signals, programmable signs, or other interfaces with travelers and vehicles of all types. The four Roadside Subsystems are described below:

- Roadway - Provides traffic management surveillance, signals, and signage for traveler information.
- Toll Collection - Interacts with vehicle toll tags to collect tolls and identify violators.
- Parking Management - Collects parking fees and manages parking lot occupancy/availability.
- Commercial Vehicle Check - Collects credential and safety data from vehicle tags, determines conformance to requirements, posts results to the driver (and in some safety exception cases, the carrier), and records the results for the Commercial Vehicle Administration Subsystem.

1.2.3 Vehicle Subsystems

These subsystems are installed in a vehicle. The four Vehicle Subsystems are described below:

- Vehicle - Functions that may be common across all vehicle types are located here (e.g. navigation, tolls, etc.) so that specific vehicle deployments may include aggregations of this subsystem with one of the other three specialized vehicle subsystem types. The Vehicle Subsystem includes the user services of the Advanced Vehicle Control and Safety Systems user services bundle.
- Transit Vehicle - Provides operational data to the Transit Management Center, receives transit network status, provides enroute traveler information to travelers, and provides passenger and driver security functions.
- Commercial Vehicle - Stores safety data, identification numbers (driver, vehicle, and carrier), last check event data, and supports in-vehicle signage for driver pass/pull-in messages.
- Emergency Vehicle - Provides vehicle and incident status to the Emergency Management Subsystem.

1.2.4 Remote Access Subsystems

These subsystems represent platforms for ITS functions of interest to travelers or carriers (e.g., commercial vehicle operators) in support of multimodal traveling. They may be fixed (e.g., kiosks or home/office computers) or portable (e.g., a palm-top computer), and may be accessed by the public (e.g., through kiosks) or by individuals (e.g., through cellular phones or personal computers). The two Traveler Subsystems are described below:

- Remote Traveler Support - Provides traveler information at public kiosks. This subsystem includes traveler security functions.
- Personal Information Access - Provides traveler information and supports emergency requests for travelers using personal computers/telecommunication equipment at the home, office, or while on travel.

1.3 The Mitretek Study

In May 1997, Mitretek prepared an *Intelligent Transportation Systems (ITS) Information Security Analysis* report under the sponsorship of the Federal Highway Administration. Federal officials envisioned CSC's current effort as the application of the information contained in that report to the Maryland ITS environment. Because of that linkage, CSC has tried to carry over the nomenclature and general approach to security that was contained in the Mitretek report. However, in a few cases CSC has departed from the terminology or security threat categories used by Mitretek. This is noted at appropriate places in the text. Because the Mitretek information was used as a point of beginning for CSC's work, the contents of the Mitretek report will be described briefly.

In addition to providing a general tutorial on information security, the Mitretek report takes the ITS systems, subsystems, and data flows contained in the National Physical ITS Model and "maps" these systems, subsystems, and individual data flows to specific security threat categories. This "mapping" is contained in a number of very useful tables contained in Appendix A to the Mitretek report.

The threat categories used in the report are briefly described in Exhibit l-2 along with a somewhat simpler approach used by CSC throughout this report. Rather than attempt to categorize specific threats, CSC believes that it is simpler to describe the security objectives, i.e., availability, confidentiality, and integrity, and discuss the threats to those objectives from whatever source. In fact, Mitretek used the same terminology CSC has used to discuss security objectives while including a fourth security objective-accountability. CSC does not consider accountability as a separate security objective but rather as a security safeguard implemented to assist in assuring any attempt to corrupt the integrity and confidentiality of the information is recorded.

CSC also believes that masquerading, replay, and repudiation are more correctly methods of attack, not specific categories of threats. Be this as it may, even though CSC chose to use security terminology slightly differently, CSC agrees with the conclusions Mitretek reached and its discussion of the generic security issues.

Exhibit 1-2. Mitretek and CSC Security Terminology

Mitretek Threat Categories	Threat Definitions	CSC security Objectives
Denial of Service	Any action that prevents any part of a system from functioning as intended.	Availability
Disclosure	The acquisition of sensitive personal or financial information through unauthorized channels.	Confidentiality
Manipulation	The modification of system information whether being processed, stored, or transmitted.	Integrity
Masquerading	The attempt by an unauthorized user or process to gain access to a system by posing as an authorized entity.	
Replay	The re-transmission of valid messages under invalid circumstances to produce unauthorized effects.	
Repudiation	The success&l denial of an action.	

In addition to the "mapping" of security threats to systems, subsystems, and individual data flows, the Mitretek report also contains discussions of the ITS Communications Infrastructure, Information Security Policy, and Information Security Mechanisms.

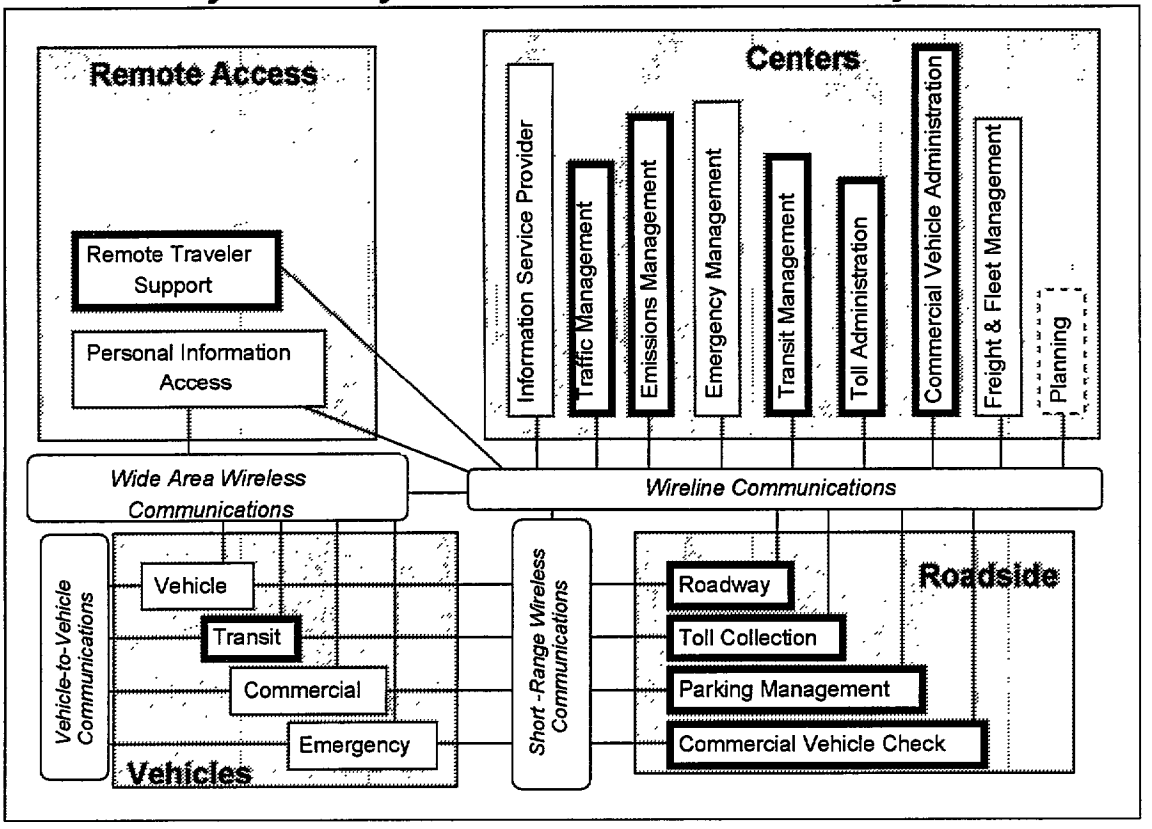
2 The ITS Security Model Applied to Maryland

The previous section described the National ITS Physical Architecture and its individual systems and subsystems. As one would expect, for most "real world" situations these "ideal" systems and subsystems might not exist or might be structured very differently from those shown in the model. The first step then to developing the security requirements for Maryland's ITS systems was to determine what ITS elements actually existed and their relationship to one another.

2.1 Maryland Data Flows

Interviews were conducted with key Maryland ITS stakeholders to compare the structure of Maryland's ITS systems to the National ITS Physical Architecture. As a result of those interviews, it was determined that all systems and all but one subsystem did exist but that some of the subsystems were the responsibility of commercial or trade organizations over which Maryland had no direct control. In Exhibit 2-1, those subsystems which are the responsibility of Maryland are outlined by bold lines while those which are the responsibility of others are not. All of the subsystems did exist in one form or another with the exception of the Planning Subsystem for which no equivalent could be found.

Exhibit 2-1. Maryland Subsystems within the National ITS Physical Architecture



In this report, only those systems that are the exclusive responsibility of Maryland, i.e., those shown in bold outline, will be discussed.

2.2 Maryland Subsystems

The MDOT Modals responsible for the national ITS architecture subsystems that are applicable to Maryland are identified in Exhibit 2-2. Based on the information provided by key stakeholders, each of the subsystems described in the National ITS Physical Architecture for which there is a Maryland equivalent are discussed below.

Exhibit 2-2. Map of MDOT Modals to National ITS Architecture Subsystems

	System										
	Center					Roadside				Vehicle	Remote Access
MDOT Modal	CVAS	EMMS	TAS	TMS	TRMS	CVCS	PMS	RS	TCS	TRVS	RTS
Maryland Aviation Administration (MAA)							■				
Maryland Transportation Authority (MdTA)		■	■	■				■	■		
Mass Transit Administration (MTA)					■					■	■
Motor Vehicle Administration (MVA)	■					■					
State Highway Administration (SHA)				■				■			

■ Responsible Organization

2.2.1 Commercial Vehicle Administration and Commercial Vehicle Check Subsystems (CVAS and CVCS)

The CVAS performs administrative functions supporting credentials, tax, and safety regulations while the CVCS operates at the roadside to enable credential checking and safety information collection. Within Maryland, the new Commercial Vehicle Information Systems and Networks program (CVISN) will subsume these functions.

Primarily states, multi-state associations, and their contractors are developing CVISN with partial funding by the U.S. Department of Transportation and the Federal Highway Administration. CVISN is a collection of existing and new state, federal and private information systems and communications networks that support commercial vehicle operations. The goal of the program is to bring the benefits of ITS to the motor carrier industry and to the Federal and state governments that monitor that industry.

CVISN will deliver new electronic services in the areas of safety, credentials administration, and electronic screening. Examples of these services include:

- Timely safety information to inspectors at roadside,
- Electronic credentialing,
- Exchange of registration and fuel tax information electronically, and
- Electronic screening of commercial vehicles at fixed and mobile sites while vehicles are in motion.

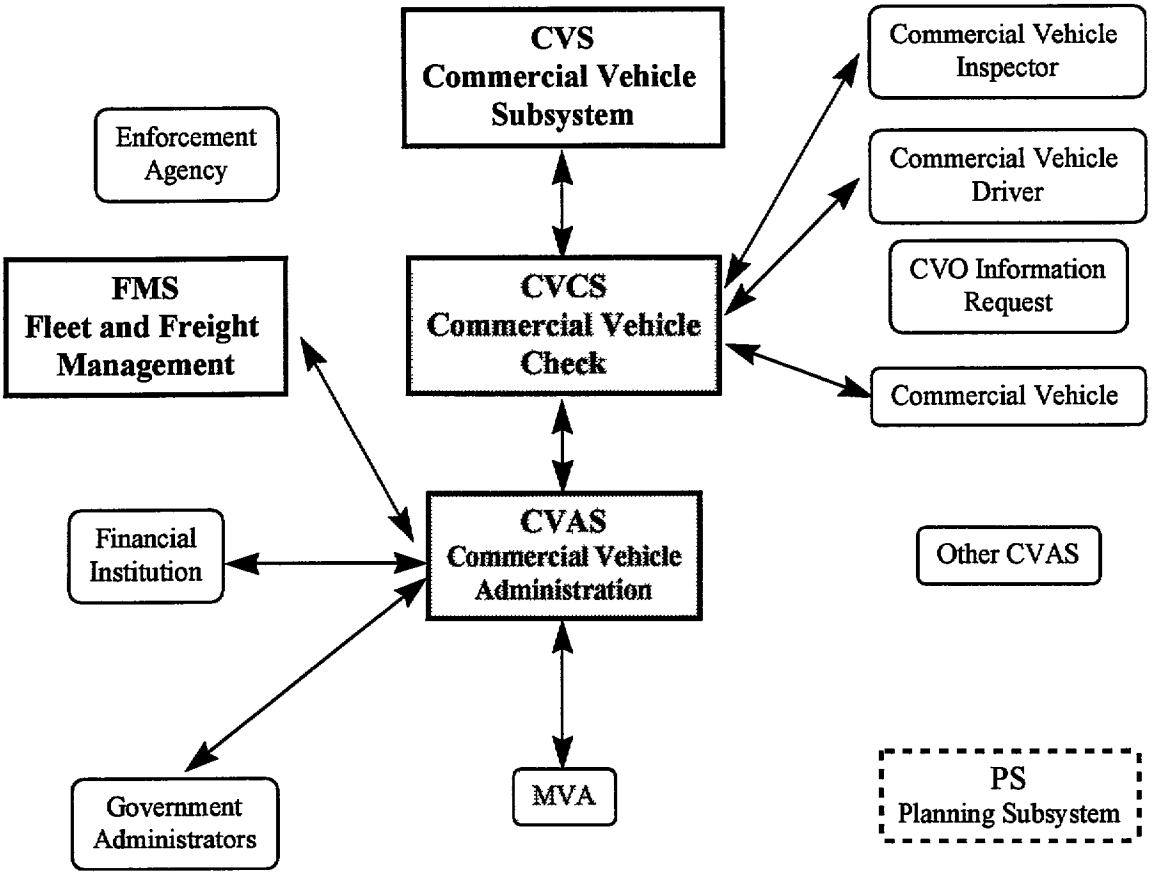
Maryland is a key state in the development of the CVISN system as it, together with Virginia, is a prototype state for the development of CVISN technology.

2.2.1.1 Diagram for CVAS and CVCS

Exhibit 2-3 describes the ITS physical architecture for commercial vehicle operations. Key elements of this model are the CVAS and CVCS systems whose databases reside in a number of locations including the Information Systems Center (ISC), contractor facilities, the Annapolis data center, the SHA LAN, State Police systems, the Public Services Commission, and Federal databases among others.

Maryland's major subsystems are shown in bold, rectangular boxes while subsystems which are part of the national ITS model but do not exist in Maryland are shown in dotted, rectangular boxes. Sources of data or data terminators are shown in rectangular boxes with rounded corners. Those subsystems over which MDOT has direct control are shaded. Data flows are shown by arrows indicating the direction of data flow. This same schema is used through this document.

Exhibit 2-3. Physical Architecture for CVAS and CVCS



The CVAS and CVCS systems in turn interface with several national and regional clearinghouse systems, which are the responsibility of IRP, Inc. and IFTA, Inc. The CVAS and CVCS systems interface with other state CVASs through Maryland's Commercial Vehicle Information Exchange Window (CVIEW) system, which connects to other jurisdictions via the national Safety and Fitness Electronic Records (SAFER) system. In time CVISN may be directly connected to similar systems in other jurisdictions.

In the Maryland situation, there are currently no direct links with enforcement agencies. Those agencies of Maryland responsible for roadside inspections will use currently existing channels to advise enforcement agencies of violations and not depend on the flow of information from the CVAS or CVCS systems to accomplish that end. There is also no data flow in response to CVO Information Requests (most frequently requests for safety information by insurance companies) because that information will be contained within the Federal clearinghouse databases,

Linkage between the CVAS system and financial institutions will be through existing mechanisms used by individual state agencies. That data flow will permit the electronic transfer of fines, license fees, and taxes.

The CVS and FMS will interface with the CVAS and CVCS as shown in the exhibit but the development of those interfaces is the responsibility of the commercial carriers and their trade organizations.

2.2.1.2 Data Flows

Exhibits 2-4 through 2-7 describe the individual data flows to and from the CVAS and CVCS (see Acronym list). These tables were extracted from the Mitretek Study but have been modified by striking through" those data flows or individual data elements which do not exist for Maryland.

For example, international border crossing data obviously does not apply to Maryland so that item was marked with a "strikethrough". Similarly, there is no intention to support the direct exchange of information with other CVASs and hence that line was eliminated from the table. Similar changes were made in the other tables as required to conform to Maryland's reality.

Exhibit 2-4. ITS Data Flow Security Assessment: From CVAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
cvas	credentials information	cvcs	w	x	x	~	x		
cvas	CVO database update	cvcs	w	x	x	x	x		
~~evas~~	~~international border crossing data~~	~~cvcs~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		
cvas	safety information	cvcs	w	x	x	x	x		
~~evas~~	~~activity reports~~	~~fms~~	~~w~~	~~x~~	~~x~~	~~x~~	~~x~~		
~~evas~~	~~compliance review report~~	~~fms~~	~~w~~	~~x~~	~~x~~	~~x~~	~~x~~		
cvas	electronic credentials	fms	w, u1t	x	x	x	x	x	x
~~evas~~	~~operational data~~	~~ps~~	~~w~~	~~x~~		~~~~	~~x~~		
cvas	payment request	x21	w	x		~	x	x	x
cvas	tax-credentials-fees request	x22	w	x	x	~	x		x
~~evas~~	~~credentials and safety information~~	~~x59~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		~~x~~
~~evas~~	~~CVAS information exchange~~	~~x59~~	~~w~~	~~x~~		~~~~	~~x~~		
~~evas~~	~~request for information on violators~~	~~x62~~	~~w~~	~~x~~		~~~~	~~x~~		
~~evas~~	~~violation notification~~	~~x62~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		
cvas	license request	x64	w	x		~	x		
~~evas~~	~~credentials & safety information response~~	~~x65~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		

Exhibit 2-5. ITS Data Flow Security Assessment: To CVAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
cvcs	citation and accident data	cvas	W	x	x	x	x		
cvcs	credentials information request	cvas	W	x	x	~	x		
cvcs	international border crossing data update	~~cvas~~	~~w~~	~~x~~	~~x~~	~~-~~	~~x~~		
cvcs	roadside log update	cvas	W	x	x	x	x		
cvcs	safety information request	cvas	W	x	x	~	x		
fms	credential application	.cvas	W	x	x	~	x		
fms	information request	cvas	w	x	x	~	x		
fms	tax filing, audit data	cvas	w	x	x	x	x	x	x
x21	transaction status	cvas	w	x		~	x	x	x
x22	regulations	cvas	w	x	x	~	x		
~~x59~~	~~credentials and safety information response~~	~~cvas~~	~~w~~	x	x	-	x		~~x~~
~~x59~~	~~CVAS information exchange~~	~~cvas~~	~~w~~	x			x		
~~x62~~	~~information on violators~~	~~cvas~~	~~w~~	x	x	-	x		
x64	registration	cvas	W	x	x	~	x		
~~x65~~	~~credentials and safety information request~~	~~cvas~~	~~w~~	x			x		

Exhibit 2-6. ITS Data Flow Security Assessment: From CVCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
cvcs	citation and accident data	cvas	w	x	x	x	x		
cvcs	credentials information request	cvas	w	x	x	~	x		
~~cvcs~~	~~international border crossing data update~~	~~cvas~~	~~w~~	~~x~~	~~x~~	~~-~~	~~x~~		
cvcs	roadside log update	cvas	w	x	x	x	x		
cvcs	safety information request	cvas	w	x	x	~	x		
~~cvcs~~	~~border clearance event record~~	~~cvs~~	~~u2~~	~~x~~	~~x~~	~~-~~	~~x~~	~~x~~	
~~cvcs~~	~~border clearance request~~	~~cvs~~	~~u2~~	~~x~~		~~-~~	~~x~~	~~x~~	
cvcs	clearance event record	cvs	u2	x	x	~	x	x	
cvcs	lock tag data request	cvs	u2	x		~	x	x	
cvcs	on-board safety request	cvs	u2	x	x	~	x	x	
cvcs	pass/pull-in	cvs	u2	x	x	x	x	x	
cvcs	safety inspection record	cvs	u2	x	x	x	x	x	
cvcs	screening request	cvs	u2	x		~	x	x	
cvcs	CVO Pull in Message	x06	H	x					
cvcs	CVO inspector information	x10	H	x					

Exhibit 2-7. ITS Data Flow Security Assessment: To CVCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
cvas	credentials information	cvcs	w	x	x	~	x		
cvas	CVO database update	cvcs	w	x	x	x	x		
~~evas~~	~~international border crossing data~~	~~evcs~~	~~w~~	~~x~~	~~x~~	~~-~~	~~x~~		
cvas	safety information	cvcs	w	x	x	x	x		
~~evs~~	~~border clearance data~~	~~evcs~~	~~u2~~	~~x~~	~~x~~	~~x~~	~~x~~	~~x~~	
cvs	lock tag data	cvcs	u2	x	x	x	x	x	
cvs	on board safety data	cvcs	u2	x	x	x	x	x	
cvs	screening data	cvcs	u2	x	x	x	x	x	
x08	CVO weight and presence	cvcs	P	x					
x10	CVC override mode	cvcs	H	x			x		
x10	CVO inspector input	cvcs	H	x			x		

2.2.1.3 Security Concerns

As noted earlier, one of the CVISN databases presently resides on the mainframe at the MVA. Hence, those security concerns expressed by MVA personnel (see section 2.2.7.3) apply to the CVISN system as well. However, there are certain security issues that are unique to the CVISN system.

Two concerns that been specifically noted by carriers to CVISN personnel follow:

- **Internet access by FMS.** Plans are to provide carriers with Internet access (via the FMS) to the CVAS. Carriers are very concerned about the security of the credentials, safety, tax, and financial information that must be provided as part of that process. However, these concerns are ameliorated by the fact that no remote log-on will be supported and no access to directory structures, etc. will be provided. Communications will be mediated through mailboxes.
- **CV Transponder Information.** Carriers are also concerned about the loss of transponder information which would provide locations, times, and driver information to competitors. They believe that competitors could use this information to develop operating costs, routing, and delivery times. It should be noted, however, that much of the same information could be obtained visually.

There are also security concerns that arise from the possible participation of other modals in the CVISN system. Although there are no current plans for the Maryland Port Administration (MPA) to participate in CVISN, it is a logical candidate to eventually join the CVISN system because of the movement of carrier traffic into and out of the port. At present, the MPA database that contains information on containers, cargo, authorized carriers, their drivers, etc. is located on the mainframe in the ISC at the MVA. As with other ISC systems, it is ID and password protected. However, multiple MPA personnel use identical log-on information and over 75 percent of the personnel having read/write access to the system are non-State employees who have not undergone background investigation. Personnel in this category include union longshoremen and contractor personnel. In addition, approximately 30 companies have dial-up

access to the mainframe although their access is limited to only that information they have provided. The security risks presented by this situation are well understood by those responsible for the operation of these systems but adequate resources (both personnel and financial resources) do not presently exist to address these issues. Although other modals such as the Maryland Aviation Administration were not interviewed, it is reasonable to assume that similar concerns will exist should they eventually join the CVISN system.

2.2.2 Parking Management Subsystem (PMS)

The Maryland Aviation Administration originated in 1929 when the state Aviation Commission was established. The State Aviation Administration replaced the Commission and became a unit of the Department of Transportation in 1970. The Administration was renamed in 1989 as the Maryland Aviation Administration. Under direction of the Maryland Aviation Commission since 1994, the Administration develops and operates airports and fosters and regulates aeronautical activity within the State.

Baltimore Washington International (BWI) Airport, the State's major air carrier facility, is operated by the Administration. This includes the operation of most parking lots at and in the vicinity of the airport. BWI Airport formerly was Friendship International Airport, which began operation in 1950. In 1972, the State was authorized to purchase Friendship International Airport from Baltimore City. The Airport was renamed BWI in 1973. The Administration also supervises the operation of the Martin State Airport in Baltimore County. Martin State Airport was purchased by the State in 1975.

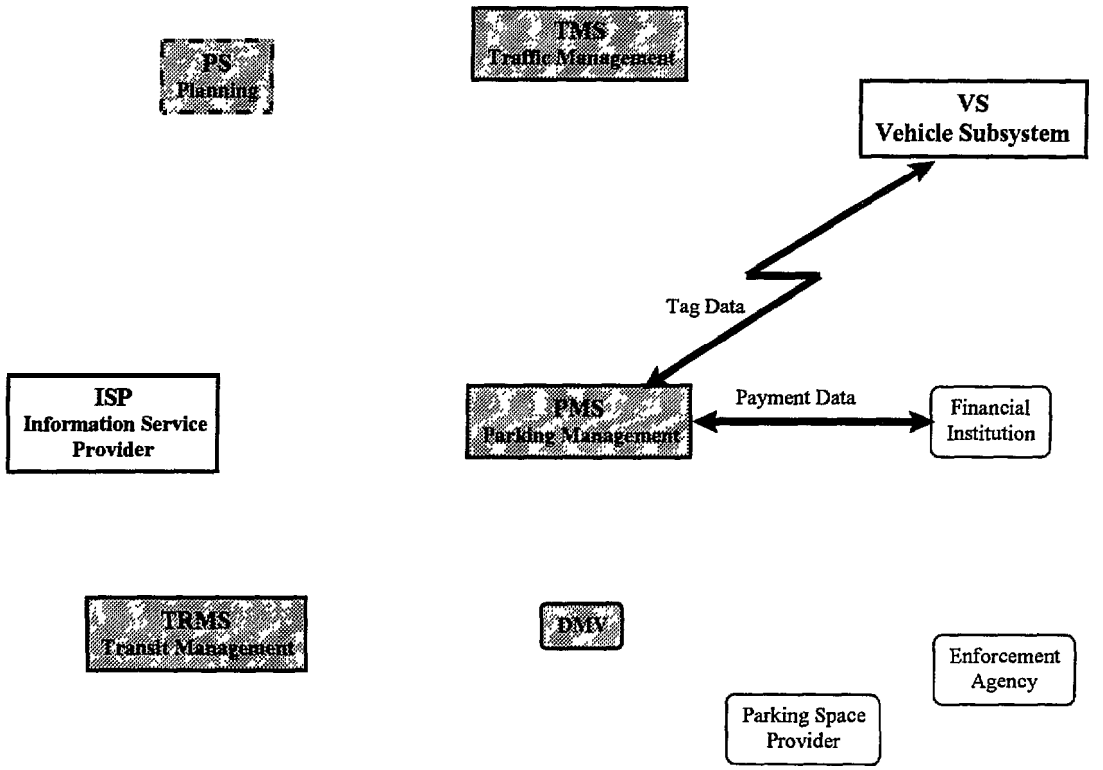
The Maryland Aviation Administration (MAA)-managed parking lots at BWI have been selected to develop the Maryland PMS model. In the Maryland model, a contractor operates and maintains the PMS central computer as an agent of the MAA. This computer is physically located in the Parking Administration Building at BWI. One other contractor staffs and operate the satellite parking facility, also an agent of the MAA.

The PMS contractor pays a guaranteed fee at the beginning of the month. At the end of the month, the contractor pays an additional fee that is based on the gross revenue collected during the month. The contractor keeps the remaining monthly revenue.

2.2.2.1 Diagram for PMS

Exhibit 2-8 represents the conceptual data flows between Maryland's PMS consistent with the National ITS Physical Architecture model. Current operational data flows involving the PMS are shown on the diagram. Most of the data flows are electronic. Several involve interfaces between a human user, operator, or vehicle driver and a subsystem.

Exhibit 2-8. Physical Architecture for PMS



2.2.2.2 Data Flows

Exhibit 2-9 and 2-10 describe the individual physical data flows involving the PMS. These tables were extracted from the Mitretek study. All of the data flows in the Mitretek study were discussed during an interview with the MAA. Most of the flows identified in the Mitretek study are not currently implemented in Maryland or planned for future implementation.

Exhibit 2-9. ITS Data Flow Security Assessment: From PMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
pms	parking availability	isp	w	x	x	~	x		
pms	parking lot reservation confirmation	isp	w	x	x	x	x	x	x
pms	operational data	ps	w	x		~	x		
pms	demand management price change response	tms	w	x		~	x		
pms	parking availability	tms	w	x		~	x		
pms	transit parking coordination	trms	w	x		~	x		
pms	request tag data	vs	u2	x	x	x	x	x	x
pms	tag update	vs	u2	x	x	x	x	x	x
pms	transaction status	x12	H	x					
pms	payment request	x21	w	x	x	x	x	x	x
pms	parking status	x36	H	x					
pms	parking availability	x37	w	x	x	x	x	x	x
pms	violation notification	x62	w	x	x	~	x		
pms	license request	x64	w	x		~	x		

Exhibit 2-10. ITS Data Flow Security Assessment: To PMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
isp	parking lot data request	pms	w	x	x	x	x	x	x
isp	parking reservations request	pms	w	x	x	~	x		
tms	demand management price change request	pms	w	x		~	x		
tms	parking instructions	pms	w	x		~	x		
trms	parking lot transit response	pms	w	x		~	x		
vs	tag data	pms	u2	x	x	x	x	x	x
x03	vehicle characteristics	pms	P	x					
x21	transaction status	pms	w	x	x	x	x	x	x
x36	parking instructions	pms	H	x			x		
x37	request for performance data	pms	w	x		~	x	x	x
x57	vehicle image	pms	P	x					
x64	vehicle characteristics	pms	w	x	x	~	x		

2.2.2.3 Security Concerns

The MAA supports cash and electronic payments. Limited access to the PMS central computer by MAA personnel is enabled via use of designated workstations, login IDs and passwords. Managers are able to audit the activities of each toll collector in real time, balancing the number of tickets with the cash received. Electronic payments via credit card are initiated by the toll collector who swipes the customer's card across the reader. The credit information is transferred by wire to the PMS central computer and then to an out-of-state financial institution. All wireline communications are secure. All databases are backed-up on a daily basis on two different physical media (tape and disk).

Shuttle busses that operate at BWI are tagged with transponders that are used for Automated Vehicle Identification (AVI). This feature allows management to track shuttle busses from the terminal to various lots and back to the terminal. The AVI stickers could be offered to commercial fleets in the future and support automatic monthly billing. There is a current physical limit of 24,000 tags per parking lot.

Countermeasures are in place to reduce the possibility of fraud. As previously mentioned, the number of tickets collected by an operator and the cash to be received is known to the auditors. The license tags of all vehicles remaining on the lots late at night are recorded on hand-held computers. As vehicles approach the tollbooths, the operators can type in the license tag numbers and automatically determine the approximate toll (accurate to a fraction of a day) to be charged. If a customer has swapped tickets with another person in order to pay less than they owe, this will be discovered.

2.2.3 Remote Traveler Support (RTS)

The Mass Transit Administration (MTA) is an agency of the State of Maryland, operating as a part of MDOT. The MTA originated as the Metropolitan Transit Authority in 1961. The Administration was created as part of the Department of Transportation in 1970. The Administration develops, constructs, and operates the Baltimore Metro subway system, the Central Light Rail Line, and the Maryland Commuter Rail Passenger Service (MARC).

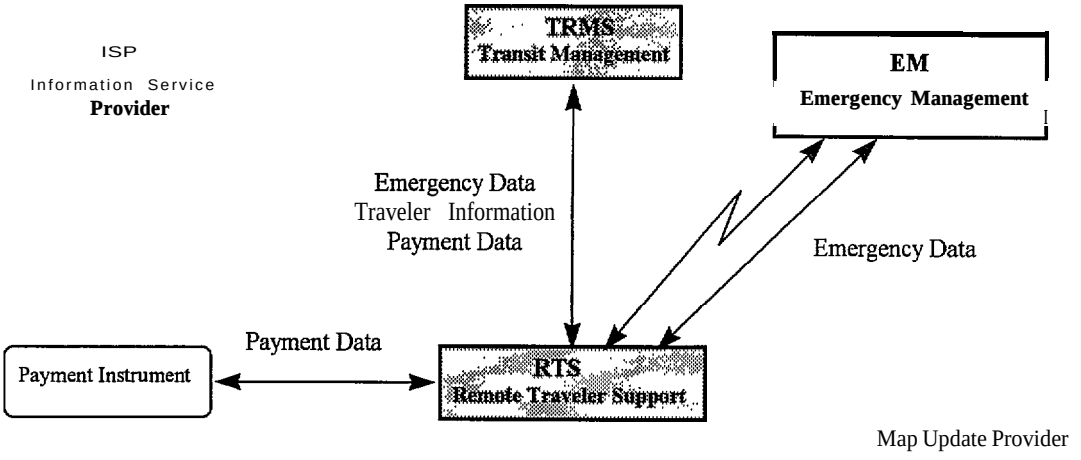
The MTA is responsible for public transportation-operating and maintaining the public bus, subway, and rail systems. The metropolitan area served encompasses Anne Arundel County, Baltimore City, and Baltimore County. Commuter bus service also links Howard and Harford Counties to Baltimore City, and southern Maryland to Washington, DC. The Administration also gives technical and financial assistance to develop or improve public transportation in small urban areas throughout the State

In the future, MTA Kiosks will be deployed and interface with the MTA Operations Centers through public switched telephone network (PSTN) auto dial lines. At this time, only MTA services will be available to the public. The MTA infrastructure and operations concepts for Kiosks have been selected to develop the Maryland RTS models. Security concerns are discussed in Section 2.2.3.3.

2.2.3.1 Diagram for RTS

Exhibit 2-l 1 represents conceptual data flows between Maryland's RTS. Most of the data flows are electronic. Several involve interfaces between a human user, operator, or vehicle driver and a subsystem.

Exhibit 2-11. Physical Architecture for RTS



2.2.3.2 Data Flows

Exhibits 2-12 and 2-l 3 describe the individual physical data flows involving the RTS. These tables were extracted from the Mitretek study. All of the data flows in the Mitretek study were evaluated based on an in-person interview with the MTA and follow up information obtained by telephone interviews. Some of the Mitretek flows were deleted based on MTA input and consistency with the plans of other organizations.

Exhibit 2-12. ITS Data Flow Security Assessment: From RTS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
rts	emergency notification	em	w,u1t	x	x	x	x		
~~rts~~	~~traveler information request~~	~~isp~~	~~w~~	~~x~~	~~x~~	~~x~~	~~x~~	~~x~~	~~x~~
~~rts~~	~~traveler selection~~	~~isp~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		
~~rts~~	~~trip request~~	~~isp~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		
~~rts~~	~~yellow pages request~~	~~isp~~	~~w~~	~~x~~		~~~~	~~x~~		
rts	emergency notification	trms	w	x	x	x	x		
rts	transit request	trms	w	x	x	x	x	x	x
rts	traveler information request	trms	w	x	x	x	x	x	x
~~rts~~	~~map update request~~	~~x23~~	~~w~~	~~x~~		~~~~	~~x~~		
rts	traveler information	x50	H	x					
rts	traveler interface updates	x56	H	x					
rts	request for payment	x61	s	x		~	x	x	x

Exhibit 2-13. ITS Data Flow Security Assessment: To RTS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
em	emergency acknowledge	rts	w,u1t	x		x	x		x
~~isp~~	~~broadcast information~~	~~rts~~	~~w,u1b~~	~~x~~		~~~~	~~x~~		
~~isp~~	~~traveler information~~	~~rts~~	~~w,u1t~~	~~x~~	~~x~~	~~x~~	~~x~~		~~x~~
~~isp~~	~~trip plan~~	~~rts~~	~~w~~	~~x~~	~~x~~	~~~~	~~x~~		
trms	emergency acknowledge	rts	w	x		x	x		
trms	transit and fare schedules	rts	w	x	x	~	x		x
trms	traveler information	rts	w	x	x	x	x	x	x
~~x23~~	~~map updates~~	~~rts~~	~~w~~	~~x~~		~~~~	~~x~~		
x50	traveler information request	rts	H	x					
x56	traveler information request	rts	H	x					
x61	payment	rts	s	x		x	x	x	x

2.2.3.3 Security Concerns

Concerns about future Kiosk and Internet public access are being addressed:

- Kiosks will have a touch screen, but no keyboard. A user will not have direct access to the modem bank. Input will be buffered (and checked) before transmission to the interface with the MTA Operations Center.
- For Internet access, the MTA will use the ISC firewall. Outgoing traffic only, e.g., file transfer protocol (FTP), will be allowed.

2.2.4 Toll Administration Subsystem and Toll Collection Subsystem (TAS and TCS)

The TAS provides general payment administration capabilities to support electronic assessment of tolls and other transportation usage fees while the TCS is the subsystem that supports toll collection operations. These systems fall within the purview of the Maryland Transportation Authority (MdTA).

MdTA is an agency of the State of Maryland, operating as a part of the Maryland Department of Transportation and as a public enterprise which develops, finances, operates and maintains a system of toll facilities and other transportation services for public use.

The MdTA is responsible for the operation and maintenance of the Fort McHenry Tunnel, the Baltimore Harbor Tunnel, the Francis Scott Key Bridge, the Thomas J. Hatem Memorial Bridge, the Harry W. Nice Memorial Bridge, the John F. Kennedy Memorial Highway, and the William Preston Lane Memorial Bridge (Bay Bridge). All MdTA maintenance, operations and capital improvements are funded through toll revenues. MdTA also maintains and operates certain ITS highway capabilities along the I-95 corridor from Baltimore east to the Delaware border and at the Oriole's Stadium in central Baltimore. The ITS devices include traffic counters, cameras, and

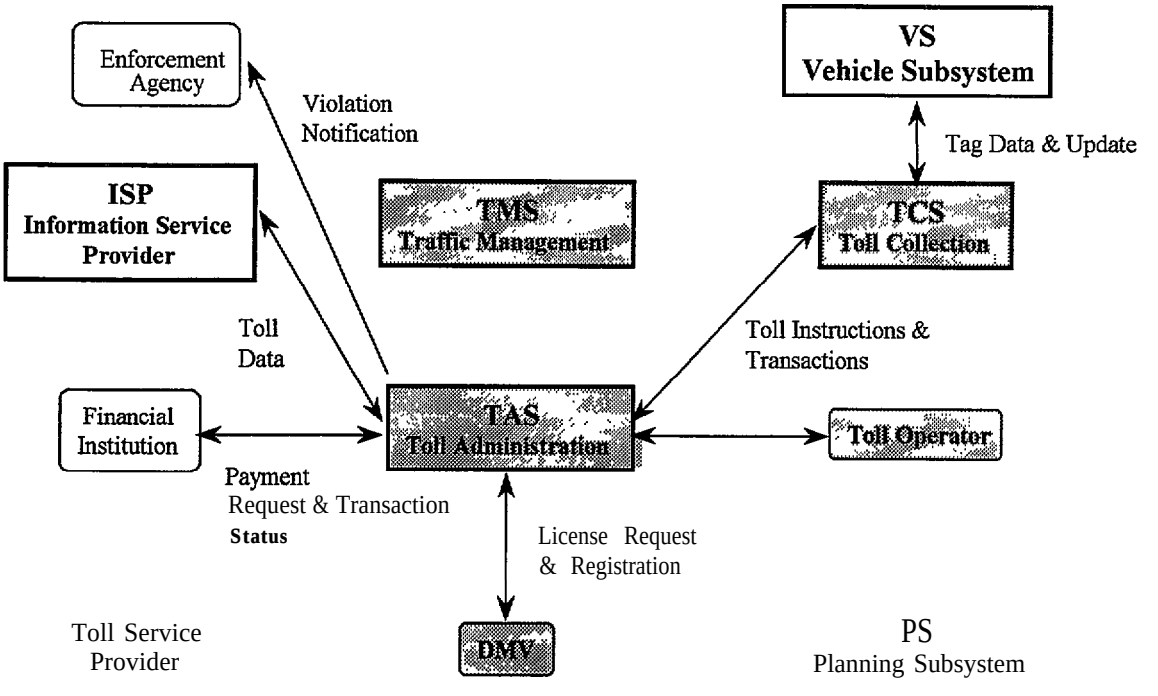
weather sensors. Only the toll functions of MdTA are discussed in this section. The MdTA ITS highway capabilities are discussed in Section 2.2.5.

A new, state-of-the-art electronic toll collection (ETC) system which performs TAS functions is now being designed and installed for MdTA by a commercial contractor. This contractor will also be responsible for the initial maintenance and operation of the system. The toll administration subsystem for Maryland will include not only this new electronic toll collection system but also a video enforcement system (VE) and a Service Center for the administration of customer accounts. The system will be maintained and operated by the contractor for a three-year period after which MdTA must decide whether future maintenance and operation will be performed by MdTA employees or by contract. The TCS will continue to be operated by MdTA employees.

2.2.4.1 Diagram for TAS and TCS

Exhibit 2-14 represents the conceptual data flows between Maryland toll subsystems consistent with the National ITS Physical Architecture model. In the Maryland model, a toll service provider as defined in the national architecture does not exist. Rather, the MdTA contractor effectively functions as the TAS operator and effects many although not all of the functions shown in the figure. In the operation of the new service center, the contractor will establish a stand-alone web site for data flows to and from the ISP and will establish dial-up or Integrated Services Digital Network (ISDN) lines with financial institutions for the debiting of tolls. All other data flows will interface directly with the TAS as shown on the diagram. Most of the data flows will be electronic although a few will involve human interface.

Exhibit 2-14. TAS and TCS Physical Architecture



2.2.4.2 Data Flows

Exhibits 2-l 5 through 2-18 describe the individual data flows to and from the TAS and TCS. As stated earlier, these tables were extracted from the Mitretek Study but have been modified by striking through those data flows or individual data elements that do not exist for Maryland.

There are currently no plans to provide operational data to the planning system or provide demand management and probe data to the traffic management system. For that reason, these data flows were eliminated from the tables. Also, toll transaction reports for Maryland will be provided to the toll operators electronically rather than by human interface and that Interconnect item was corrected in the tables. Violation information will be provided to the judiciary system for action but it is presently anticipated that this interface will be human rather than electronic. These and other appropriate changes were made in the tables.

Exhibit 2-15. ITS Data Flow Security Assessment: From TAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
tas	probe data	isp	w	x		~	x		
tas	toll data	isp	w	x	x	x	x	x	x
~~tas~~	~~operational data~~	~~ps~~	~~w~~	~~x~~		~~-~~	~~x~~		
tas	toll instructions	tcs	w	x	x	x	x	x	x
~~tas~~	~~demand management price change response~~	~~tms~~	~~w~~	~~x~~		~~-~~	~~x~~		
~~tas~~	~~probe data~~	~~tms~~	~~w~~	~~x~~		~~-~~	~~x~~		
tas	payment request	x21	w	x	x	x	x	x	x
tas	toll transaction reports	x43	~~H~~ w	x					
~~tas~~	~~toll revenues and summary reports~~	~~x44~~	~~w (? H)~~	~~x~~	~~x~~	~~x~~	~~x~~		
tas	violation notification	x62	~~w~~ H	x	x	~	x		
tas	license request	x64	w	x		~	x		

Exhibit 2-16. ITS Data Flow Security Assessment: To TAS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
isp	toll data request	tas	w	x	x	x	x	x	x
tcs	Toll Transactions	tas	w	x	x	x	x	x	x
~~tms~~	~~demand management price change request~~	~~tas~~	~~w~~	~~x~~		~~-~~	~~x~~		
x21	transaction status	tas	w	x	x	x	x	x	x
x43	toll operator requests	tas	~~H~~ w	x			x		
~~x44~~	~~toll fees~~	~~tas~~	~~H~~	~~x~~			~~x~~		
x64	registration	tas	w	x	x	~	x		

Exhibit 2-17. ITS Data Flow Security Assessment: From TCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
tcs	Toll Transactions	tas	w	x	x	x	x	x	x
tcs	request tag data	vs	u2	x		~	x	x	x
tcs	tag update	vs	u2	x	x	x	x	x	x
tcs	transaction status	x12	H	x					

Exhibit 2-18. ITS Data Flow Security Assessment: To TCS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
tas	toll instructions	tcs	w	x	x	x	x	x	x
vs	tag data	tcs	u2	x	x	x	x	x	x
x03	vehicle characteristics	tcs	P	x					
x57	vehicle image	tcs	P	x					

2.2.4.3 Security Concerns

In discussions with MdTA personnel, three areas of security vulnerability were suggested for further examination:

- The 900 MHz transponder signal between the VS and TCS subsystems (MdTA is a secondary user of this band)
- The interface between the TAS/TCS subsystems and the Office of Information Technology wide area network (WAN)
- The administrative and procedural controls that will govern the activities of those contractor personnel who will interface with the ISP and financial institutions

It should also be noted that the National Architecture requires that electronic financial transactions in which the TAS is an intermediary between the consumer and the financial infrastructure shall be cryptographically protected and authenticated to preserve privacy and ensure authenticity and auditability.

2.2.5 Traffic Management Subsystem (TMS), Emissions Management (EMMS), and Roadway Subsystem (RS)

The Maryland TMS is a composite of the SHA Statewide Operations Center (SOC), the Maryland Transportation Authority (MdTA) Traffic Control Centers (TCCs) at the Ft. McHenry Tunnel and Harbor Tunnel, the Montgomery County Traffic Operations Center (TOC), and traffic signal control centers in many other incorporated areas such as Annapolis City, Baltimore City,

and Baltimore County. A subset of the EMMS functions identified in the National ITS Architecture model is performed locally at both MdTA tunnel locations. No Maryland organization performs all of the EMMS functions defined in the National ITS Architecture model. The National ITS model for the RS is valid for Maryland with a major exception that there are no plans to deploy automated highway system (AHS) devices at this time.

2.2.5.1 Diagrams for TMS, EMMS, and RS

Exhibits 2-19 through 2-21 represent representative conceptual data flows between the TMS, EMMS, and RS, respectively. Most of the data flows are electronic. Several involve interfaces between a human user, operator, or vehicle driver and a subsystem.

Exhibit 2-19. TMS Physical Architecture

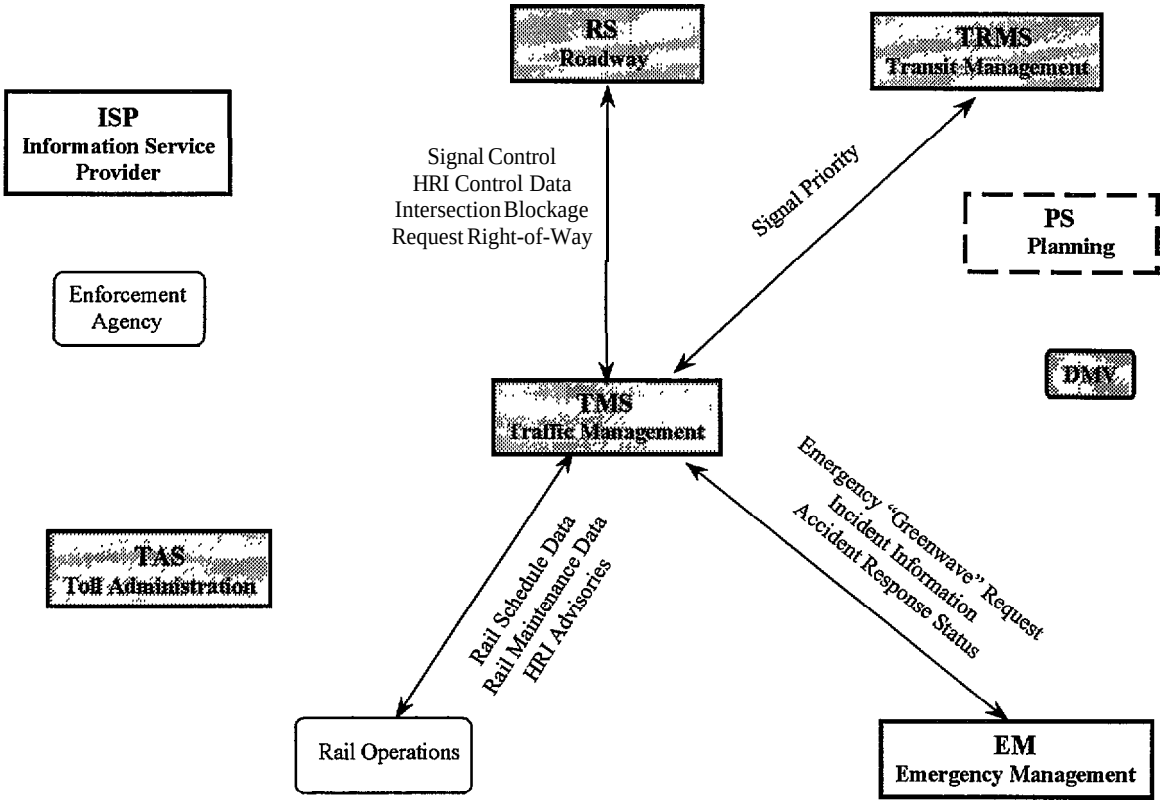
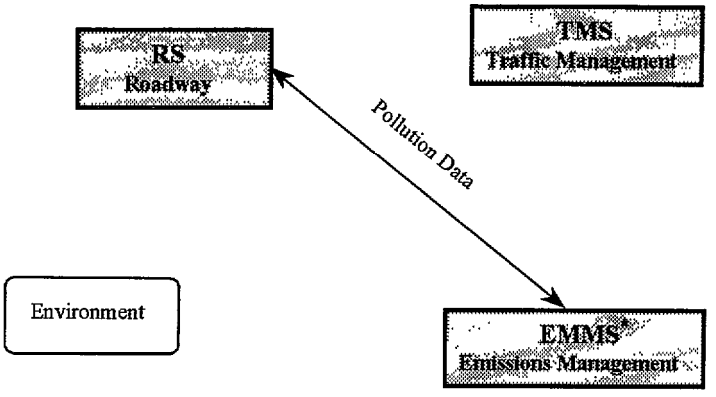
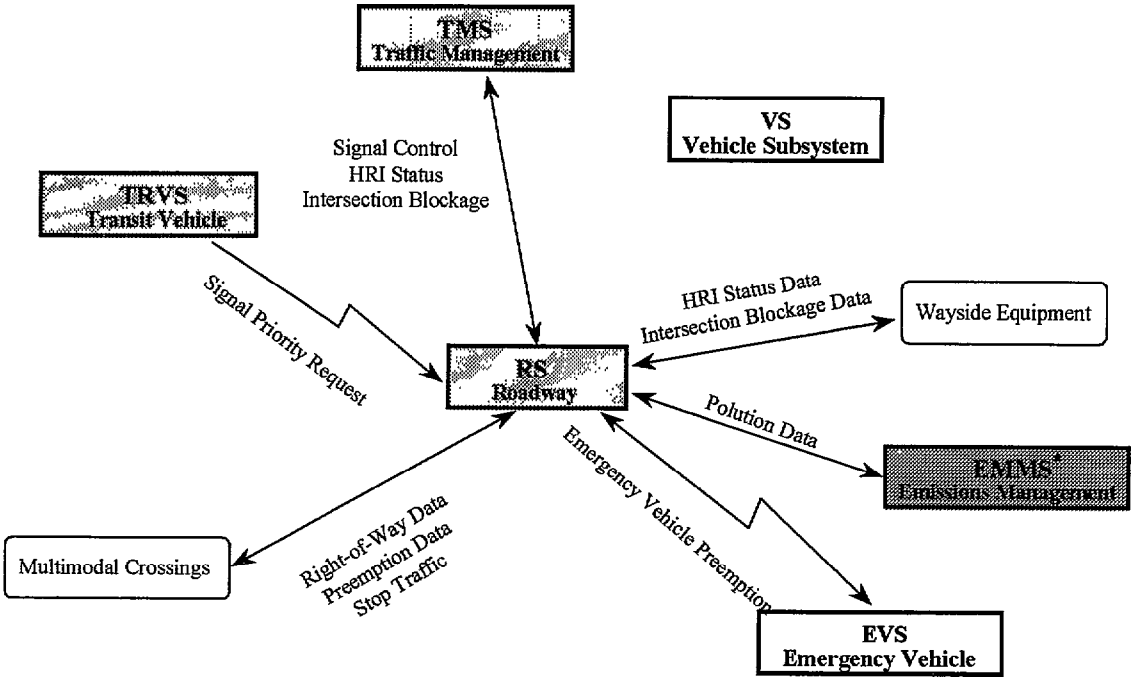


Exhibit 2-20. EMMS Physical Architecture Model



* Gne EMMS is collocated at the MdTA Ft. McHenry Tunnel TMS; one is collocated at the MdTA Harbor Tunnel TMS.

Exhibit 2-21. RS Physical Architecture Model



* One EMMS is collocated at the MdTA Ft. McHenry Tunnel TMS; one is collocated at the MdTA Harbor Tunnel TMS.

2.252 Data Flows

Exhibits 2-22 through 2-27 describe the individual physical data flows involving the TMS, EMMS, and RS. These tables were extracted from the Mitretek study. All of the data flows in the Mitretek study were discussed during interviews with the MdTA and SHA. Some of these flows were deleted based on the feedback from the MdTA and SHA. Several flows involving two-way wide area wireless communications were also added. These flows are shown in ***italics*** in the tables.

Exhibit 2-22. ITS Data Flow Assessment: From TMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
tms	incident information request	em	w	x		x	x		
tms	incident notification	em	w	x		x	x		
~~tms~~	~~pollution state data request~~	~~emms~~	~~w~~	~~x~~		~~~~	~~x~~		
tms	traffic information	isp	w	x		~	x		
~~tms~~	~~demand management price change request~~	~~pms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~tms~~	~~parking instructions~~	~~pms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~tms~~	~~operational data~~	~~ps~~	~~w~~	~~x~~		~~~~	~~x~~		
~~tms~~	~~AHS control information~~	~~rs~~	~~w~~	~~x~~		~~x~~	~~x~~		
tms	freeway control data	rs	w	x		x	x		
tms	hri control data	s	w	x		x	x		
tms	hri request	rs	w	x		~	x		
tms	signage data	rs	w	x		~	x		
tms	signal control data	rs	w	x		x	x		
tms	surveillance control	rs	w	x		~	x		
tms	surveillance *control*	*rs*	*u1t*	*x*					
~~tms~~	~~demand management price change request~~	~~tas~~	~~w~~	~~x~~		~~~~	~~x~~		
~~tms~~	~~demand management price change request~~	~~trms~~	~~w~~	~~x~~		~~~~	~~x~~		
tms	signal priority status	trms	w	x		~	x		
~~tms~~	~~traffic information~~	~~trms~~	~~w~~	~~x~~		~~~~	~~x~~		
tms	work schedule	x09	H	x					
tms	event confirmation	x19	w	x		~	x		x
tms	map update request	x23	w	x		~	x		
tms	TMC coord.	x35	w	x	x	x	x		
tms	traffic operations data	x46	H	x					
tms	violation notification	x62	w	x	x	~	x		
tms	license request	x64	w	x		~	x		
tms	hri advisories	x67	w	x		x	x		

Exhibit 2-23. ITS Data Flow Assessment: To TMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
em	emergency vehicle greenwave request	tms	w	x		x	x		
em	incident information	tms	w	x		x	x		
em	incident response status	tms	w	x		x	x		
~~emms~~	~~widearea statistical pollution information~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
isp	incident notification	tms	w	x		x	x		
isp	logged route plan	tms	w	x	x	x	x		
isp	request for traffic information	tms	w	x		~	x		
isp	road network use	tms	w	x	x	~	x		
~~pms~~	~~demand management price change response~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~pms~~	~~parking availability~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~ps~~	~~planning data~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~rs~~	~~AHS status~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
rs	fault reports	tms	w	x		~	x		
rs	freeway control status	tms	w	x		~	x		
rs	HOV data	tms	w	x		~	x		
rs	hri status	tms	w	x		x	x		
rs	incident data	tms	w	x	x	~	x		
rs	*incident data*	*tms*	*u1t*	*x*					
rs	intersection blockage notification	tms	w	x		x	x		
rs	local traffic flow	tms	w	x		~	x		
rs	request for right of Way	tms	w	x		~	x		
rs	signal control status	tms	w	x		~	x		
rs	signal priority request	tms	w	x		~	x		
rs	vehicle probe data	tms	w	x	x	~	x		
~~tas~~	~~demand management price change response~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~tas~~	~~probe data~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
~~trms~~	~~demand management price change response~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
trms	request for transit signal priority	tms	w	x		~	x		
trms	transit system data	tms	w	x		~	x		
x09	work zone status	tms	H	x			x		
x19	event plans	tms	w	x		~	x		
x23	map updates	tms	w	x		~	x		

Exhibit 2-23. ITS Data Flow Assessment: To TMS (Continued)

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
x35	TMC coord.	tms	w	x	x	x	x		
x46	traffic control	tms	H	x			x		
x58	weather information	tms	w	x		~	x		
x64	registration	tms	w	x	x	~	x		
x67	railroad advisories	tms	w	x		x	x		
x67	railroad schedules	tms	w	x		~	x		

Exhibif 2-24. ITS Dafa Flow Assessmenf; From EMMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
~~emms~~	~~operational data~~	~~ps~~	~~w~~	~~x~~		~	~~x~~		
~~emms~~	~~vehicle pollution criteria~~	~~rs~~	~~w~~	~~x~~		~	~~x~~		
~~emms~~	~~widearea statistical pollution information~~	~~tms~~	~~w~~	~~x~~		~	~~x~~		
~~emms~~	~~map update request~~	~~x23~~	~~w~~	~~x~~		~	~~x~~		
emms	pollution data display	x46	H	x					

Exhibit 2-25. ITS Data Flow Assessmenf: To EMMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
rs	pollution data	emms	w	x		~	x		
~~tms~~	~~pollution state data request~~	~~emms~~	~~w~~	~~x~~		~	~~x~~		
x18	pollution data	emms	P	x		~	x		
~~x23~~	~~map updates~~	~~emms~~	~~w~~	~~x~~		~	~~x~~		
x46	pollution data parameters	emms	H	x			x		

Exhibit 2-26. ITS Data Flow Security Assessment: From RS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
rs	pollution data	emms	w	x		~	x		
~~rs~~	~~AHS status~~	~~tms~~	~~w~~	~~x~~		~~~~	~~x~~		
rs	fault reports	tms	w	x		~	x		
rs	freeway control status	tms	w	x		~	x		
rs	HOV data	tms	w	x		~	x		
rs	hri status	tms	w	x		x	x		
rs	incident data	tms	w	x	x	~	x		
rs	*incident data*	*tms*	*u1t*	*x*					
rs	intersection blockage notification	tms	w	x		x	x		
rs	local traffic flow	tms	w	x		~	x		
rs	request for right of Way	tms	w	x		~	x		
rs	signal control status	tms	w	x		~	x		
rs	signal priority request	tms	w	x		~	x		
rs	vehicle probe data	tms	w	x	x	~	x		
~~rs~~	~~AHS control data~~	~~vs~~	~~u2~~	~~x~~		~~x~~	~~x~~	~~x~~	
rs	intersection status	vs	u2	x		x	x	x	
rs	request tag data	vs	u2	x		~	x	x	x
~~rs~~	~~vehicle signage data~~	~~vs~~	~~u2~~	~~x~~		~~~~	~~x~~	~~x~~	
rs	driver information	x12	H	x					
rs	grant right of way and/or stop traffic	x29	w	x		x	x		
rs	crossing permission	x38	H	x					
rs	hri status	x66	w	x		x	x		
rs	intersection blockage notification	x66	w	x		x	x		

Exhibit 2-27. ITS Data Flow Security Assessment: To RS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
~~emms~~	~~vehicle pollution criteria~~	~~rs~~	~~w~~	~~x~~		~~~~	~~x~~		
evs	emergency vehicle preemption request	rs	u2	x		~	x	x	
~~tms~~	~~AHS control information~~	~~rs~~	~~w~~	~~x~~		~~x~~	~~x~~		
tms	freeway control data	rs	w	x		x	x		
tms	hri control data	rs	w	x		x	x		
tms	hri request	rs	w	x		~	x		
tms	signage data	rs	w	x		~	x		
tms	signal control data	rs	w	x		x	x		
tms	surveillance control	rs	w	x		~	x		
tms	*surveillance control*	*rs*	*u1t*	*x*					
trvs	local signal priority request	rs	u2	x		~	x	x	
~~vs~~	~~ahs vehicle data~~	~~rs~~	~~u2~~	~~x~~		~~x~~	~~x~~		
vs	vehicle probe data	rs	u2	x	x	x	x		
x03	vehicle characteristics	rs	P	x					
x18	pollution data	rs	P	x					
x29	request for right of Way	rs	w	x		x	x		
x29	right of way preemption request	rs	w	x		x	x		
x38	crossing call	rs	H	x					
x41	weather conditions	rs	P	x					
x45	vehicle count	rs	P	x					
x66	arriving train information	rs	w	x		x	x		
x66	track status	rs	w	x		x	x		

2.2.5.3 Security Concerns

CHART workstation users are provided access by user ID and password. Once someone is logged onto the system, there is nothing to inhibit another individual from using the workstation if the initial user is not present. The MdTA logs (audits) all changes to controlled devices. If the user takes an inappropriate action, the user who logged on initially will be blamed.

The MdTA would prefer to enhance the system by implementing one of the functions currently installed on the criminal justice terminals. If there is no action for a system-specified time, e g., eight minutes, the user is automatically logged off and must log on again if needed.

MdTA has not encountered any misuse of fixed ITS assets. However, an inappropriate message was displayed on a portable variable message sign (VMS), and the offending person was never identified.

2.2.6 Transit Management Subsystem (TRMS) and Transit Vehicle Subsystem (TRVS)

The Mass Transit Administration (MTA) is described in Section 2.2.3. The MTA infrastructure and operations concepts have been selected to develop the Maryland TRMS and TRVS models. There are four MTA Operations Centers, one each for busses, Metro (subway), Light Rail, and MARC. CSX and AMTRAC supply most of the operational software systems at the MARC center. Two ongoing MTA ITS projects include the Automatic Vehicle Location and Monitoring (AVL/M) System, and the Transit Information Center Upgrade.

The AVL/M project entails the fleet wide installation of AVL/M equipment for bus and light rail. AVL is not being installed on MARC trains, primarily because the system resolution is not sufficient to determine if the train is on the correct track. AVL/M combines specialized equipment and new operational procedures to improve the supervision and dispatching of transit vehicles. Using upgraded radio communication and computer technology, operating supervisors are provided continuous reports of the status and location of transit vehicles. The equipment makes possible the automatic transmission of both routine and emergency information between operators and supervisors. AVL/M equipment has been installed on approximately l/3 of the fleet busses and light rail trains. Installation will be completed within the next 2 to 3 years.

AVL/M will produce cost savings through improved management and increased productivity, specifically in the area of supervision and optimization of schedules. Improved security will result from an immediate identification and location determination for vehicles requiring assistance. The availability of complete, up-to-date information on system performance will result in better planning, scheduling and routing. Customer service will be aided because of better information and a reduction in time necessary for responding to customer inquiries and complaints.

The Transit Information Center Upgrade project is being implemented in three phases to automate the access to transit information for customer service requests for all MTA services. In the first two phases the incoming telephone capabilities were upgraded; the interactive voice system capacity was doubled; MARC and Mobility information was incorporated; diagnostic and customer information management capabilities were installed; the Automatic Call Distribution System including remote access was improved and enhanced; the Customer Information Center was computerized; and AVL was integrated into the center with external systems for real-time travel information. Phase 3 is ongoing and incorporates a trunked radio system supporting two-way cellular, UHF, or VHF communications between the Operations Centers and the fleet vehicles. It also integrates the Transit Watch Information Network (TWIN).

The two-way radio system includes a microwave trunk and two receiver towers. The trunk infi-astructure links the intelligent fleet vehicles with the Operations Centers. TWIN includes a 4th generation database management system, data warehousing, and robust management reports for planning and scheduling, transit information, operations and maintenance, and administration. Phase 3 is scheduled for completion in December 1997. When all upgrades are completed, the Customer Information staff will be able to receive more phone calls and increase the speed and efficiency of providing transit schedule and route information to the public.

The MTA Operations Center was chosen to develop the Maryland TRMS model. The Vehicle Logic Unit (VLU) installed onboard the MTA vehicles was chosen to develop the Maryland TRVS model. Security concerns are discussed in Section 2.2.6.3.

2.2.6.1 Diagrams for TRMS and TRVS

Exhibits 2-28 and 2-29 represent conceptual data flows between Maryland's TRMS and between Maryland's TRVS, respectively, consistent with the National ITS Physical Architecture model. Most of the data flows are electronic. Several involve interfaces between a human user, operator, or vehicle driver and a subsystem.

Exhibit 2-28. Physical Architecture for TRMS

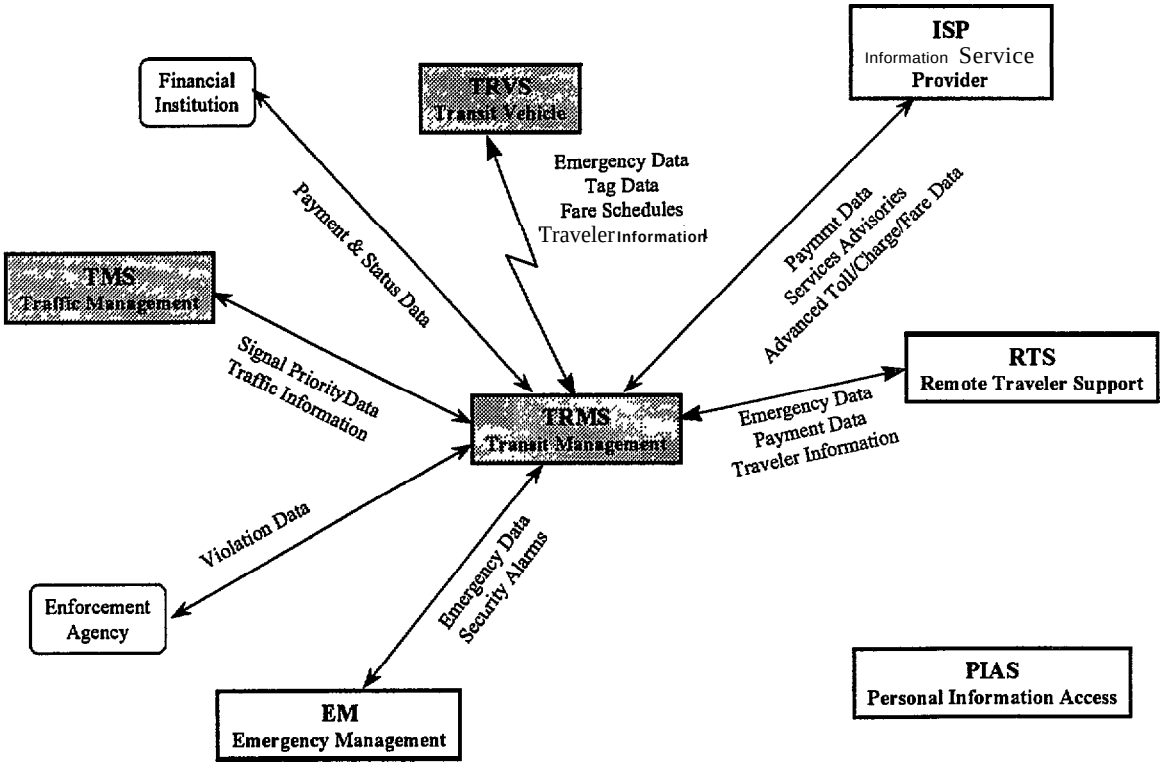
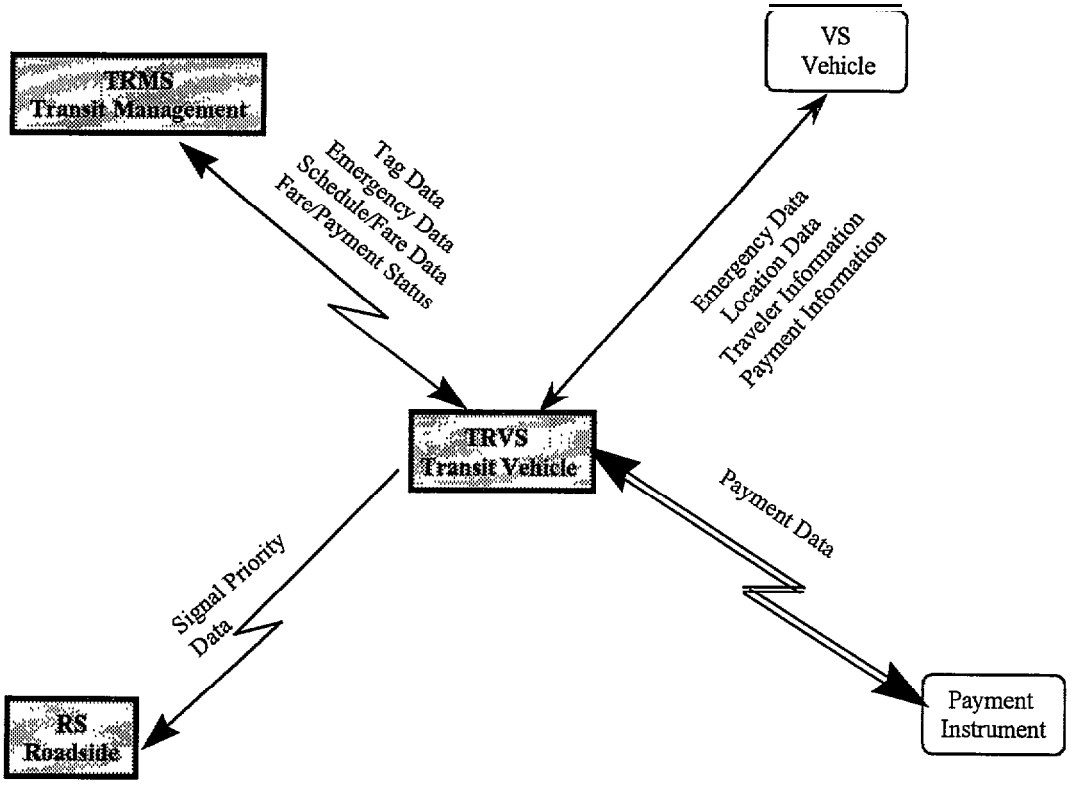


Exhibit 2-29. Physical Architecture for TRVS



2.2.6.2 Data Flows

Exhibits 2-30 through 2-33 describe the individual physical data flows involving the TRMS and TRVS. These tables were extracted from the Mitretek study. All of the data flows in the Mitretek study were discussed during an interview with the MTA. Some of the flows were deleted based on the feedback from the MTA.

Exhibit 230. ITS Data Flow Security Assessment: From TRMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
trms	security alarms	em	w	x		x	x		
trms	demand responsive transit plan	isp	w	x	x	~	x		
trms	transit and fare schedules	isp	w	x	x	x	x		
trms	transit request confirmation	isp	w	x	x	x	x	x	x
trms	demand responsive transit route	pias	w,u1t	x	x	~	x		
trms	parking lot transit response	pms	w	x		~	x		
~~trms~~	~~operational data~~	~~ps~~	~~w~~	~~x~~		~~~~	~~x~~		
trms	emergency acknowledge	rts	w	x		x	x		
trms	transit and fare schedules	rts	w	x	x	~	x		x
trms	traveler information	rts	w	x	x	x	x	x	x
trms	demand management price change response	tms	w	x		~	x		
trms	request for transit signal priority	tms	w	x		~	x		
trms	transit system data	tms	w	x		~	x		
trms	bad tag list	trvs	u1t	x	x	x	x		
trms	driver instructions	trvs	u1t	x	x	~	x		
trms	emergency acknowledge	trvs	u1t	x		x	x		
trms	request for vehicle measures	trvs	u1t,u2	x		~	x		
trms	schedules, fare info request	trvs	u1t	x	x	x	x	x	x
trms	traveler information	trvs	u1t	x	x	x	x		x
trms	intermodal information	x02	w	x		~	x		
trms	payment request	x21	w	x	x	x	x	x	x
trms	map update request	x23	w	x		~	x		
trms	TRMS coord	x33	w	x		~	x		
trms	camera control	x42	w	x		x	x		
trms	emergency acknowledge	x42	w	x		x	x		
trms	actual schedule and fare info	x47	H	x					
trms	transit operator display	x49	H	x					
trms	route assignment	x52	H	x					
trms	work schedule	x53	H	x					
trms	violation notification	x62	w	x	x	~	x		

Exhibit 2-31. ITS Data Flow Security Assessment: To TRMS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
em	transit emergency coordination data	trms	w	x		x	x		
isp	demand responsive transit request	trms	w	x	x	~	x		
isp	selected routes	trms	w	x	x	x	x	x	x
isp	transit information request	trms	w	x	x	x	x	x	x
pias	demand responsive transit request	trms	u1t	x	x	~	x		
pms	transit parking coordination	trms	w	x		~	x		
rts	emergency notification	trms	w	x	x	x	x		
rts	transit request	trms	w	x	x	x	x	x	x
rts	traveler information request	trms	w	x	x	x	x	x	x
tms	demand management price change request	trms	w	x		~	x		
tms	signal priority status	trms	w	x		~	x		
tms	traffic information	trms	w	x		~	x		
trvs	emergency notification	trms	u1t	x	x	x	x		
trvs	fare and payment status	trms	u1t,u2	x	x	x	x	x	x
trvs	request for bad tag list	trms	u1t,u2	x		~	x		
trvs	transit vehicle conditions	trms	u1t,u2	x	x	~	x		
trvs	transit vehicle passenger and use data	trms	u1t,u2	x		~	x		
trvs	traveler information request	trms	u1t	x	x	x	x	x	x
trvs	vehicle probe data	trms	u1t	x		~	x		
x02	intermodal information	trms	w	x		~	x		
x21	transaction status	trms	w	x	x	x	x	x	x
x23	map updates	trms	w	x		~	x		
x33	TRMS coord	trms	w	x		~	x		
x42	physical activities	trms	P	x		x	x		
x47	schedule Guidelines	trms	H	x			x		
x49	transit operator fare schedules	trms	H	x			x		
x53	maint Status	trms	H	x			x		

Exhibit 2-32. ITS Data Flow Security Assessment: From TRVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
trvs	local signal priority request	rs	u2	x			x	x	
trvs	emergency notification	trms	ult	x	x	x	x		
trvs	fare and payment status	trms	u1t,u2	x	x	x	x	x	x
trvs	request for bad tag list	trms	u1t,u2		x	~	x		
trvs	transit vehicle conditions	trms	u1t.u2	x	x	~	x		
trvs	transit vehicle passenger and use data	trms	u1t,u2	x		~	x		
trvs	traveler information request	trms	ult	x	x	x	x	x	x
trvs	vehicle probe data	trms	ult	x		~	x		
trvs	traveler advisory request	vs	w	x					
trvs	transit user fare status	x50	H	x					
trvs	transit user outputs	x50	H	x					
trvs	transit driver display	x52	H	x					
trvs	reauest for bavment	x61	s	x		~	x	x	x

Exhibit 2-33. ITS Data Flow Security Assessment: To TRVS

Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
				DoS	Dis	Man	Mas	Rpy	Rpd
trms	bad tag list	trvs	u1t	x	x	x	x		
trms	driver instructions	trvs	u1t	x	x	~	x		
trms	emergency acknowledge	trvs	u1t	x		x	x		
trms	request for vehicle measures	trvs	u1t,u2	x		~	x		
trms	schedules, fare info request	trvs	u1t	x	x	x	x	x	x
trms	traveler information	trvs	u1t	x	x	x	x		x
vs	vehicle location	trvs	w	x		~			
x50	emergency notification	trvs	H	x					
x50	transit user inputs	trvs	H	x					
x51	vehicle measures	trvs	w	x		~			
x52	transit driver inputs	trvs	H	x			x		
x61	payment	trvs	s	x		x	x	x	x

2.2.6.3 Security Concerns

MTA users access systems using ID and password. Passwords must be changed every 90 days. There is no strong authentication.

Concerns about future Kiosk and Internet access by the public are currently being addressed. These concerns are discussed in Section 2.2.3.3.

2.2.7 Motor Vehicle Administration (MVA) Terminator

Although not one of the 19 primary subsystems, the MVA, also referred to as the Department of Motor Vehicles (DMV), is uniquely important in Maryland not only because it is the primary user of data processing resources within MDOT but also because it manages the ISC on behalf of all other MDOT elements. Most ITS related databases are contained within the ISC and the ISC serves as the interface between MDOT systems and those Federal databases with which information is exchanged.

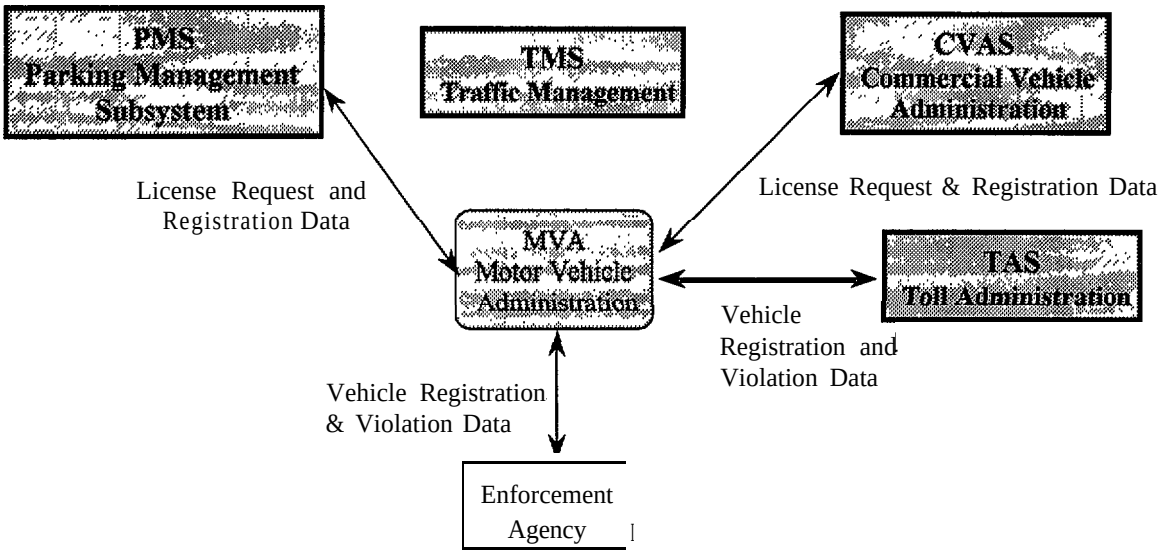
MVA is the state regulatory and licensing agency responsible for the varied activities affecting Maryland's motorists. The MVA is responsible for licensing drivers, registering and titling vehicles and administering motorcycle safety and automobile insurance programs. It also regulates vehicle sales through a dealer, salesman and manufacturer licensing program and manages the Vehicle Emissions Program.

As the primary user of data processing resources in MDOT, the MVA has also had responsibility for centralized data processing supporting other elements of MDOT. This support is provided through the ISC and includes broad responsibilities for the development and implementation of data security policies and procedures. However, MVA responsibilities in these areas are decreasing somewhat as many agencies, including the MVA itself, move to client/server systems which are generally managed by the individual MDOT components. All data processing operations are subject to broad security policies set by the State Data Security Committee within the Governor's Office.

2.2.7.1 Diagram for MVA

Exhibit 2-34 portrays the actual data flows between the MVA and other elements of the National ITS Physical Architecture model. There are existing MVA links with the American Association of Motor Vehicle Administrators (AAMVA) for the exchange of license and violation information throughout the U.S. and planned links with trucking companies as CVISN is implemented. CVISN in effect subsumes CVAS in the ITS physical model and, although CVAS is shown conceptually as an independent subsystem within the National ITS Physical Model, CVISN will in fact be organizationally a part of the MVA. On-line links also exist with the MAA for the exchange of license and violation information in support of the PMS. Links do not currently exist with any TMS nor are any planned. Links do exist with the MdTA, which operates the TAS for the exchange of license and violation data, and with enforcement agencies such as the police and courts.

Exhibit 2-34. Motor Vehicle Administration Physical Architecture



While the data flows shown above represent those contained within the National ITS Physical Architecture model, a number of other flows exist for the MVA which are not shown. These flows include data to/from:

- Health and Mental Hygiene for action against individuals failing to provide child support
- Insurance companies for violation information
- Car dealers for electronic titling
- Vehicle registration (a vendor will administer and collect fees for the MVA)
- Emission facilities (a vendor will administer this program for the MVA)

These flows are not included within the framework of the ITS Architecture Model

2.2.7.2 Data Flows

The data flows described above are shown in the Tables included elsewhere in this section only to the extent that the MVA (or DMV as it is referred to in the ITS Architecture Model) is a data Terminator. Although the details of other terminators are not provided in this study, an exception was made for the MVA because of its unique position as the major provider of data processing support within the MDOT and because of its role, up to the present, in the establishment and implementation of security policy with the MDOT.

2.2.7.3 Security Concerns

The primary security concerns for MVA systems are:

- **Unauthorized Access.** In all, approximately 6,000 personnel have access to MVA systems. Only user ID and password protect current systems with firewall protection for Internet access. State employees undergo background investigations although contractors (MVA vendors, insurance company personnel, etc.) do not. However, contractor personnel are

bonded and required to sign security agreements. Users other than MVA personnel also have "read only" access and any information they provide for input is reviewed before being written to the database.

- **Security System Management.** As mainframe systems migrate to new client/server systems and these systems come under the administrative and security control of a number of different MDOT components, it may be difficult to implement consistent security policies and procedures. Further, although currently undergoing reorganization to consolidate all physical and data security elements within the MVA, there is some question as to whether the new security office has sufficient numbers of personnel with the requisite data system security expertise.
- **Ineffective Auditing.** While extensive information is maintained on who attempted to access what system and when, few resources exist to analyze the data collected.
- **Disclosure of Sensitive Information.** The new vehicle registration system will require payment by credit card and those credit card numbers along with extensive personal information about individuals will reside in a single database.

All of these problems are recognized by the MVA and are being addressed to varying degree. However, each represents problems for existent and planned ITS subsystems and must be addressed by those subsystems.

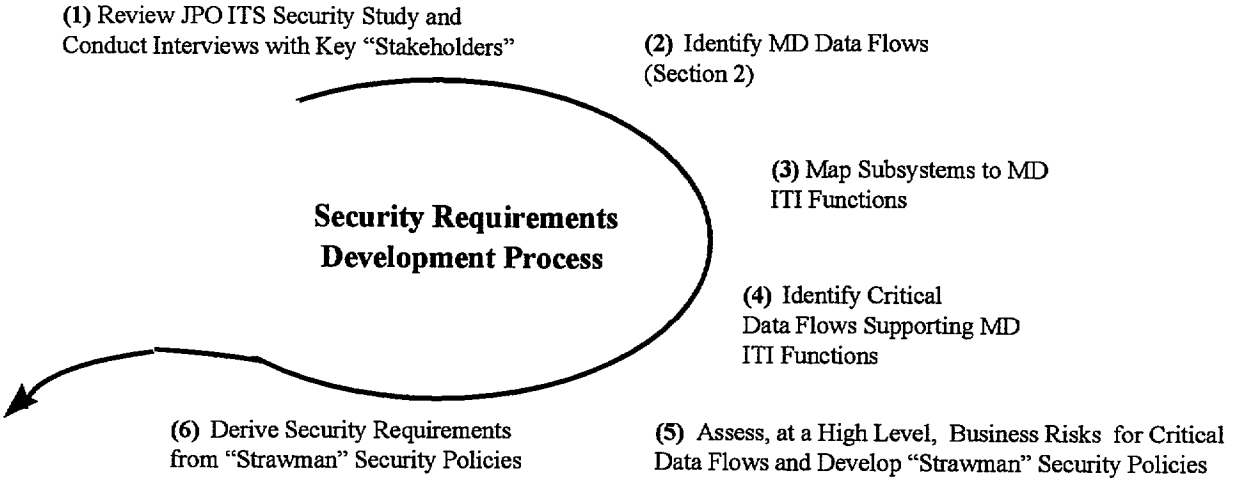
3 Maryland ITS Security Requirements

The specific data flows that apply for Maryland ITS systems were identified in Section 2 along with the general security threats that exist for each data flow as developed in the Mitretek study. However, these flows number in the hundreds and no distinction is made between those that are critical to the functioning of MDOT and those that are not. Furthermore, the business risk associated with countering common security threats (availability, confidentiality, integrity and, sometimes, authentication and non-repudiation) associated with the flows is not addressed. Business risk is normally addressed in terms of impact on operations and cost. Simply stated, what is the cost of losing or using a degraded resource relative to the cost of ensuring its full availability? Clearly, all threats to all resources cannot be protected against so those threats which present the greatest business risk to critical resources must be identified, security policies developed, and countermeasures implemented. This section describes the process used in the identification of critical systems, resources and data flows and identifies recommended security requirements that resulted from that process.

3.1 The Security Requirements Assessment Process

Security requirements for Maryland ITS systems were developed following the step-by-step process shown in Exhibit 3-1. Each step will be described in turn.

Exhibit 3-1. The Security Requirements Development Process



1. The first step in the process was to review the JPO Security Study and to interview key Maryland "stakeholders" to determine which ITS subsystems and data flows actually existed in Maryland.
2. Next these data flows were reflected in the tables included in Section 2 of this report.
3. Having done this, the key question still remained, "Which of these data flows are truly critical to the business of MDOT?" To answer that question, each ITS subsystems was mapped to

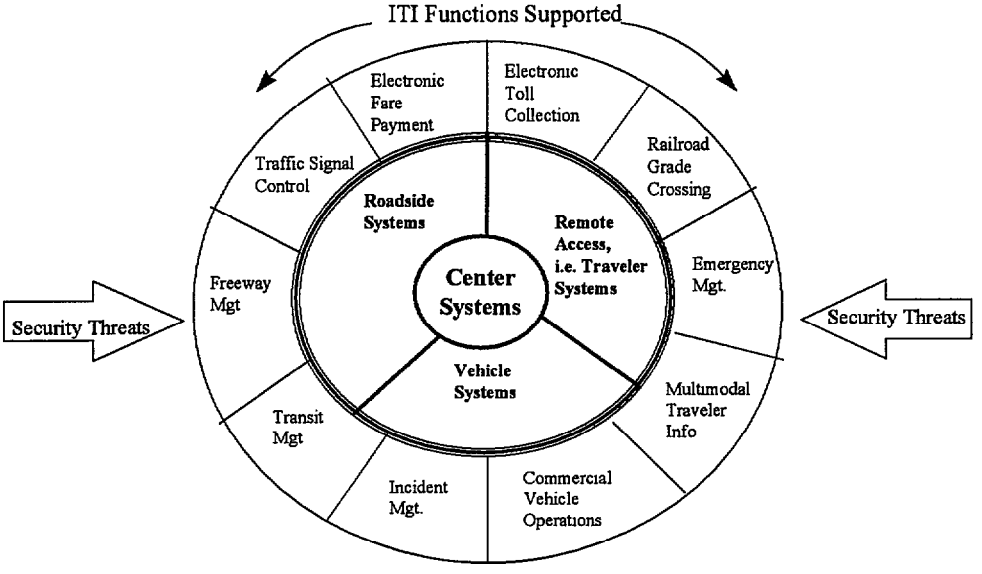
one of the following nine IT Infrastructure (ITI) functions described in the national ITS architecture:

- Traffic Signal Control
- Freeway Management
- Transit Management
- Incident Management
- Electronic Fare Payment
- Electronic Toll Collection
- Railroad Grade Crossings
- Emergency Management Services
- Regional Multi-modal Traveler

One other function that is not included in the National ITI but is important to Maryland-is Commercial Vehicle Operations (CVO), which was added. Each of the National ITS subsystems was then "mapped" to those Maryland ITI functions that are supported, as shown in Appendix A. The shaded areas in Appendix A identify those ITI functions or ITS subsystems that do exist for Maryland and are the responsibility of MDOT or the state.

4. With this mapping complete, it was then possible to identify which data flows were in fact critical, Simply put, if a particular data flow for a given subsystem is not essential to the accomplishment of a particular IT1 function, then it isn't a critical data flow requiring security protection. Another way of portraying this relationship is shown in Exhibit 3-2.

Exhibit 3-2. ITS Systems and the ITI Functions They Support



ITS systems are shown surrounded by the ITI functions they support. Unless a particular system or subsystem data flow is essential to the performance of an ITI function, then it isn't

considered critical. Using Appendix A as a guide, each individual data flow for the Center, Roadside, Remote Access, and Vehicle systems was reviewed and identified as being a critical flow or not. These critical flows are summarized in Appendix B.

5. Having identified the critical data flows, it was then possible, at a high level, to discuss these flows in terms of the business security risks they presented, i.e., what is the likely cost of providing security protection for certain data flows versus the cost of the damage which might result from a failure to do so.
6. From these discussions, "strawman" security policies evolved that in turn generated the specific security requirements included later in this report.

The business security risk discussions referred to above require further elaboration. Business security risk analyses are nothing more than cost-benefit comparisons in which the annualized cost of safeguards to defend against threats is compared with the expected annualized cost of loss. Typically, a business case to employ a safeguard should only be made if the cost of the safeguard is less than the cost of the loss. Classically, the expected loss can be computed as:

$$ALE = TV$$

where ALE is the annualized loss expectancy, T is the likelihood that a particular threat will be applied in any given year, and V is the dollar value of the asset threatened. Qualitative estimates of the importance of assets can also be used instead of monetary value, but some procedure must be used to determine the criticality of the asset. This, of course, means that qualitative estimates are more subjective and often represent management culture rather than true criticality.

So, the expected cost of a loss-expressed in monetary or qualitative terms-due to a security breach is predicated on the probability that a vulnerability, which is defined as a weakness that can be exploited by a threat, would be exploited to cause loss of an asset.

For example, if the computer responsible for monitoring vehicle emissions in a tunnel fails due to unreliable electrical service, people could be overcome by carbon monoxide poisoning while traveling through the tunnel because adequate warning was not available. Hence, the emissions monitoring computer would have a high criticality weight but a single emissions sensor may only have low criticality if there are many sensors in the tunnel. For this example, the necessity of a mitigating security requirement is a foregone conclusion.

For a second example, if the computer responsible for managing roadway VMS devices malfimctions, traffic advisory information could not be displayed throughout the traffic management system. While seemingly critical, this would not be as critical as malicious access to the computer by an unauthorized person that could result in an undetected display of traffic disrupting information causing an immense traffic jam. Hence, the former criticality may be weighted moderate but the latter moderately high.

Determining the probability that an ITS vulnerability could be exploited in the State of Maryland is beyond the scope of this report due to time limitations; all physical threads of each data flow would have to be examined and a loss history developed. However, the authors allocated the cost of loss in qualitative terms (criticality) based on analysis of the stakeholder interviews conducted.

3.2 General ITS Security Requirements

It should be noted that a few general security requirements apply to all four ITS systems. These requirements are administrative in nature and will be presented first followed by technical security requirements for the Center, Roadside, Vehicle, and Remote Access systems.

3.2.1 Recommended Security Requirements:

a) Devices utilized to provide ITS security must be based on open standards, conform to appropriate security standards where such standards exist, communicate utilizing international or U.S. standards-based protocols, and employ commercial off-the-shelf (COTS) technology that has been subjected to due diligence whenever possible.
b) A formal, role-based access approval procedure for individual users should be implemented and enforced for each Center system and Center System data processing facility and should be used to adhere to a principle of "least privilege."
c) All custom software applications should successfully pass formal test procedures prior to installation in ITS.
d) ITS security requirements should be incorporated into planning for and the design of all new ITS and any invitation for bids or other solicitation for ITS or ITS components should include security as a weighted evaluation factor.
e) Configuration management must be exercised on all ITS software and hardware systems.
f) An MDOT ITS Security Officer should be appointed by the Secretary to ensure compliance with established ITS security standards and perform internal system audits. Further, consideration should be given to the establishment of an ITS Security Working Croup to support the State Data Security Committee.
g) A formal contingency/disaster recovery plan and procedures must be established for each ITS system and contingency/disaster recovery procedures should be tested on a periodic basis.
h) ITS operational data should be backed up as appropriate to its criticality and a copy stored off site consistent with contingency/disaster recovery plan procedures.
i) An information processing security training and awareness program must be implemented for ITS.

3.3 Center Systems

Center subsystems are the "heart" of the ITS architecture. It is these systems which deal with all those functions normally assigned to public/private administrative, management, or planning agencies. Only those subsystems that are the direct responsibility of MDOT have been examined.

The MDOT ITS Centers consist of the following subsystems:

- Traffic Management
- Emissions Management
- Transit Management
- Toll Administration
- Commercial Vehicle Administration

Other center subsystems contained within the ITS National Physical Architecture include Information Service Provider, Emergency Management, Freight & Fleet Management, and Planning. Of these systems, the Planning subsystem does not exist in Maryland and the others are the responsibility of commercial or trade organizations that are not under the direct control of the State of Maryland. Maryland Center subsystems will interface with these latter systems but only as they are jointly developed with participation by Maryland, other states, the Federal Government, and commercial and trade organizations.

3.3.1 Recommended Security Requirements

a) Center System application, communication, data, and file servers *(servers)* should implement a role-based identification and authentication policy and mechanism sufficiently robust to protect system criticality.

b) Center System role-based access control mechanisms should be used to enforce a *least privilege* security policy.

c) Each user of Center System servers should be assigned a unique identifier to support *least privilege* access control processing.

d) Each user of Center System *servers* should be assigned a unique personal authentication code, such as a password, to authenticate his/her unique identifier.

e) Each Center System *server* should implement an audit function appropriate to the criticality of the system.

f) Center System *server* remote access controllers should incorporate mechanisms to defeat masquerade of an authorized user by malicious attack.

g) Direct access to Center System *servers* from Intranets, Extranets, and the Internet should be inhibited.

h) An appropriate mechanism should be implemented to continuously validate the integrity of data entering a Central System.

i) An appropriate mechanism should be implemented to continuously authenticate the source of data entering a Central System.

j) A mechanism should be implemented to ensure non-repudiation of appropriate data entering a Central System.

k) A mechanism should be implemented for Central System *servers* to guarantee the integrity and authenticity of data they provide to other systems.

1) A mechanism to uniquely identify individuals authorized unrestricted access to Center System data processing facilities should be implemented.

m) Communications between Center Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information to other ITS and terminator subsystems should utilize pair-wise encryption.

3.4 Roadside Systems

Roadside Systems are essential to the support of critical IT1 functions within Maryland. Traffic signal control, freeway management, electronic fare payment, electronic toll collection, and commercial vehicle operations are all supported by these systems. Those data flows considered critical to the performance of these IT1 functions are provided in Appendix B, Table B-2.

3.4.1 Roadway Subsystem (RS)

The RS includes the equipment distributed on and along the roadway, which monitors and controls traffic in Maryland. Equipment includes highway advisory radios, variable message signs, closed circuit television (CCTV) cameras, and video image processing systems for incident detection and verification, vehicle detectors, traffic signal, and grade crossing warning systems. The subsystem also provides the capability for emissions monitoring in the Harbor Tunnel and Ft. McHenry Tunnel, and environmental condition monitoring including weather sensors and pavement icing sensors.

3.4.2 Commercial Vehicle Check Subsystem (CVCS)

The CVCS is necessary to the support of commercial vehicle operations in Maryland. Although commercial vehicle operations are not currently considered an essential element of the IT1 in the national architecture, it is of growing importance within Maryland. Maryland is at the forefront of this technology which provides for automated checks and inspections of commercial vehicles at roadside, frequently while the vehicles remain in motion. The systems within the vehicles themselves are not the responsibility of Maryland but Maryland is responsible for CVCS systems that interface with the commercial vehicle and with the center subsystems that manage this activity. Collectively, these systems are known as the CVISN project in Maryland. As noted in Appendix B, Table B-2, connectivity between the roadside and center subsystems is provided exclusively by wireline communications while two-way, short-range wireless communications is used between the commercial vehicles and roadside systems.

3.4.3 Parking Management Subsystem (PMS)

As discussed in Section 2.2.2, the PMS model is based on the MAA-managed parking lots located at BWI Airport. In Maryland, a contractor operates and maintains the PMS central computer as an agent of the MAA. This computer is physically located in the Parking Administration Building at BWI. One other contractor staffs and operates the satellite parking facility, also an agent of the MAA.

The PMS supports cash and electronic payments via credit card and will support payment by vehicle transponders as discussed in Section 3.4.

3.4.4 Toll Collection Subsystem (TCS)

The TCS supports the toll collection infrastructure within the State. This infrastructure includes seven bridges and tunnels that are an important source of State revenue. The critical data flows for the TCS are shown in Appendix B, Table 2. The TCS interacts with vehicles to collect tolls and identify violators. Communications between the TCS and the central toll administration system is via wireline while communications with vehicle systems is via two-way, short-range wireless communications.

3.4.5 Recommended Security Requirements

a) Communications between critical Roadside Systems and their respective Center System and other ITS and terminator subsystems should incorporate a sensor data integrity mechanism.

b) Communications between critical Roadside Systems and their respective Center System and other ITS and terminator subsystems should incorporate a sensor data authentication mechanism.

c) Communications between Roadside Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information to their respective Center System and other ITS and terminator subsystems should utilize pair-wise encryption.

d) Communications between critical Roadside Systems and their respective Center System and other ITS and terminator subsystems should incorporate a data authentication mechanism.

e) Roadside System devices should include a mechanism to verity the integrity and authenticity of commands, program, and configuration data received.

f) Roadside System devices should include a mechanism to support identification and authentication of personnel utilizing the device craft/maintenance port.

3.5 Vehicle Systems

As mapped in Appendix B, Vehicle Systems are essential to the support of critical IT1 functions within Maryland. Emergency notification, transit vehicle operations, and electronic payment of parking fees and tolls are all supported by these systems. Those data flows considered to be critical to the performance of these IT1 functions are provided in Appendix B, Table B-3.

3.5.1 Commercial Vehicle Subsystem (CVS)

The CVS is being developed by the private sector. Interfaces between the CVS and the MDOT-supported CVCS are addressed in the security requirements for the CVCS (see Section 3.3)

3.5.2 Emergency Vehicle Subsystem (EVS)

The EVS is being developed by the private sector. No current or future interfaces between the EVS and MDOT-supported subsystems have been identified to date.

3.5.3 Transit Vehicle Subsystem (TRVS)

The Maryland TRVS is installed on Mass Transit Administration (MTA) vehicles. The MTA uses the term Vehicle Logical Unit (VLU) when referring to this device. The TRVS communicates with the onboard sensors via wireline, with the Roadside System via 2-way short-range wireless, and with Central Systems via 2-way wide area wireless telecommunications links. The 2-way wide area wireless system includes two receiver towers.

The security concerns for the TRVS include availability. Most of the TRVS ITS functions cannot be performed in the absence of the two-way wide area wireless network. If the communications network is down, travelers will be inconvenienced, but public safety will not be jeopardized. The cost of implementing and maintaining an independent backup network would be prohibitive.

3.5.4 Vehicle Subsystem (VS)

A critical Maryland VS is the onboard transponder which is used for electronic payment of parking fees and tolls at the PMS and TCS, respectively. These devices are developed by the

private sector. They normally take the form of small stickers that are typically installed on vehicle windshields.

3.5.5 Recommended Security Requirements

a) Vehicle System identification tokens (e.g., bar code tags) should include an anti-tamper mechanism to foil theft.

b) Vehicle System identification tokens (e.g., bar code tags) should include an authentication mechanism.

c) Vehicle System identification tokens (e.g., bar code tags) should include a non-repudiation mechanism.

d) Vehicle System identification tokens (e.g., bar code tags) should include an integrity mechanism.

e) Vehicle Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information should utilize pair-wise encryption.

f) Vehicle System transponder communications should incorporate a transponder data integrity mechanism.

g) Vehicle System data communications should incorporate a data integrity mechanism.

h) Critical Vehicle System transponder communications should incorporate a transponder data authentication mechanism.

i) Critical Vehicle System data communications should incorporate a data authentication mechanism.

j) Critical Vehicle System should include a mechanism to verify the integrity and authenticity of commands, program, and configuration data received.

k) Vehicle System devices should include a mechanism to support identification and authentication of personnel utilizing the device craft/maintenance port.

3.6 Remote Access Systems

As mapped in Appendix A, Remote Access Systems are essential to the support of critical IT1 functions within Maryland. Emergency notification and acknowledgment are supported by these systems. Those data flows considered to be critical to the performance of these IT1 functions are provided in Appendix B, Table B-4.

3.6.1 Personal Information Access Subsystem (PIAS)

PIAS platforms such as the hand-held personal digital assistant (PDA) are developed by the private sector for use in applications like traveler information dissemination. MDOT modals such as the Mass Transit Administration (MTA) are planning to establish traveler information bulletin boards in cyberspace and support read-only access by the public to this information. The public will be able to access information via the Internet and/or PSTN.

Regardless of the specific forms of interfaces made available to the public, safeguards must be in place to deny the availability of any and all protected MDOT resources, including databases, to PIAS users.

3.6.2 Remote Traveler Support Subsystem (RTS)

In the future, MTA Kiosks will be deployed and interface with the MTA Operations Centers through PSTN auto dial lines. At the present time, MTA services will be the only ones available to the public at the Kiosks.

Safeguards must be in place to deny the availability of any and all protected MDOT resources, including data bases, to Kiosk users.

3.6.3 Recommended Security Requirements

a) Remote Access Systems that transfer credit card, personal identification number (PIN), and/or other sensitive information should utilize pair-wise encryption.

b) Remote Access Systems should include a traveler identification and authentication mechanism for sensitive transactions.

c) Remote Access Systems should include a non-repudiation mechanism for sensitive transactions.

d) Remote Access Systems transactions should include a data authentication mechanism.

4 Conclusion

One of the key questions that remained unanswered at the completion of the original Mitretek study was whether or not generalized security requirements developed from the National ITS model could be successfully translated into specific requirements for an individual ITS network. As this work was conducted, some partial answers to that question have become apparent. There have been a few "lessons learned." These lessons are based only on the Maryland ITS but since Maryland is at the forefront of ITS development in the U.S., the lessons learned here are likely to apply to other states' efforts at well. These lessons include the following:

- While the goal is a fully integrated ITS structure, that is hardly the case today. Traffic management is handled by the State Highway Administration, some county governments, and the Maryland Transportation Authority; tolls by the Maryland Transportation Authority; fares by the Mass Transit Administration and Maryland Aviation Administration; commercial vehicle operations currently reside in the Motor Vehicle Administration; etc.. Each has developed systems, some centralized within the MVA ISC and others decentralized as client/server systems, to meet their own requirements. Based on the information gathered during this study, there is no strategic plan for the integration (system integration, not organizational integration) of these ITS functions.
- Certain functions exist but are so dispersed that they cannot be specifically related to the National ITS Architecture model. By way of example, the Planning function included in the ITS model suggests a central point where statistics are collected and policies and directions are set for ITS within the state. Clearly, ITS planning does take place in Maryland but it is handled by individual modals within their sphere of interest. It does not currently take place within a single organizational entity.
- Many ITS subsystems cross organization boundaries which made it difficult to conform individual data flows to the model. Within the state, fares are collected by both the Maryland Aviation Administration for parking and the Mass Transit Administration for busses, Metro, Maryland Commuter Rail Passenger Service (MARC), etc. Traffic management within the State is handled by the State Highway Administration, but certain county governments such as Montgomery County also have extensive responsibilities in these areas. The databases for commercial vehicle operations under the Commercial Vehicle Information System and Networks (CVISN) project will reside not only on various Maryland systems but also within national clearinghouses maintained by the Federal Government. In short, actual data flows that must be protected are far more complex than suggested by the National model.
- Significant security issues can also be raised by the inclusion of new modals into systems that might otherwise be secure. For example, the CVISN system is being designed to include strong security measures. It is also likely that in time the Maryland Port Authority will interface with this system for the management of commercial vehicle traffic. However, the security measures in place within the Port Authority are less vigorous than those intended for CVISN. All systems that interface will have to be brought up to the same level of protection for security to be effective.
- It is practically more efficient to develop security requirements by examining the four major ITS systems as a whole rather than by focusing on the 19 individual subsystems. Each of the major systems has certain common characteristics that lead to similar security requirements.

For example, those subsystems that comprise the Center system are generally mainframe or client/server systems located in MDOT facilities, controlled and operated by MDOT personnel, and connected by wireline technology. Roadside systems on the other hand are more accessible to the public and connected by a combination of wireline and wireless technology. Similar distinctions can be made with the other systems.

- The classification of threats into the three major categories of availability, confidentiality, and integrity is more than adequate for the development of requirements. While other studies have subdivided these threats into as many as six categories (denial of service, disclosure, manipulation, masquerading, replay, and repudiation) little was gained in the development of security requirements through the use of such narrow definitions.

While it is believed that this report has demonstrated that specific security requirements can be developed using the National ITS Physical Architecture as a guide, doing so is more complex than suggested by the model and, to be as accurate as possible, requires the development of impact costs for potential security breaches and costs for the implementation of countermeasures.

Appendix A

National ITS Subsystems Supporting MDOT's IT Infrastructure

Exhibit A - 1. National ITS Subsystems Supporting MDOT's IT Infrastructure

Note: The shaded subsystems and IT infrastructure are under the control of MDO

National ITS Element		***MDOT's IT Infrastructure***									
System	**Subsystem**	**Traffic Signal Control**	**Freeway Mgt.**	**Transit Mgt.**	**Incident Mgt.**	**Electronic Fare Payment**	**Electronic Toll Collection**	**Railroad Grade Crossing**	**Emergency Mgt.**	**Regional Multimodal Traveler Information**	**Commercial Vehicle Operations**
Center	Commercial Vehicle Administration (CVAS)										x
Center	Emergency Management (EM)								x		
Center	Emissions Management (EMMS)										
Center	Fleet and Freight Management (FMS)										x
Center	Information Service Provider (ISP)									x	
Center	Planning Subsystem (PS)										
Center	Toll Administration (TAS)						x				
Center	Traffic Management (TMS)	x	x		x			x			
Center	Transit Management (TRMS)			x		x					
Remote Access	Personal Information Access (PIAS)									x	
Remote Access	Remote Traveler Support (RTS)					x				x	
Roadside	Commercial Vehicle Check (CVCS)										x
Roadside	Parking Management (PMS)					x					
Roadside	Roadway Subsystem (RS)	x	x					x			
Roadside	Toll Collection (TCS)						x				
Vehicle	Commercial Vehicle Subsystem (CVS)										x
Vehicle	Emergency Vehicle Subsystem (EVS)								x		
Vehicle	Transit Vehicle Subsystem (TRVS)			x		x					
Vehicle	Vehicle (VS)						x				

Appendix B

MDOT ITS Threats

Exhibit B - 1. MDOT Central System Threats

Subsystem	Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES DoS	Dis	Man	Mas	Rpy	Rpd
MDOT Central to/from MDOT Central										
cvas	cvas	license request	x64 DMV	w	x		~	x		
cvas	x64 DMV	registration	cvas	w	x	x	~	x		
tms	tms	signal priority status	trms	w	x		~	x		
tms	tms	TMC coord.	x35 Other TM	w	x	x	x	x		
tms	trms	request for transit signal priority	tms	w	x		~	x		
tms	x35 Other TM	TMC coord.	tms	w	x	x	x	x		
trms	trms	request for transit signal priority	tms	w	x		~	x		
trms	trms	transit system data	tms	w	x		~	x		
trms	trms	TRMS coord	x33 Other TRM	w	x		~	x		
trms	tms	signal priority status	trms	w	x		~	x		
trms	tms	traffic information	trms	w	x		~	x		
trms	x33 Other TRM	TRMS coord	trms	w	x		~	x		
trms	tms	traffic information	trms	w	x		~	x		
trms	trms	transit system data	tms	w	x		~	x		
MDOT Central to/from Other Central										
cvas	cvas	electronic credentials	fms	w, u1t	x	x	x	x	x	x
cvas	fms	credential application	cvas	w	x	x	~	x		
cvas	fms	tax filing, audit data	cvas	w	x	x	x	x	x	x
tms	tms	incident information request	em	w	x		x	x		
tms	tms	incident notification	em	w	x		x	x		
tms	em	emergency vehicle greenwave req	tms	w	x		x	x		
tms	em	incident information	tms	w	x		x	x		
tms	em	incident response status	tms	w	x		x	x		
trms	trms	security alarms	em	w	x		x	x		
trms	em	transit emergency coordination dat	trms	w	x		x	x		
MDOT Central to/from Roadside										
cvas	cvas	credentials information	cvcs	w	x	x	~	x		
cvas	cvas	CVO database update	cvcs	w	x	x	x	x		
cvas	cvcs	credentials information request	cvas	w	x	x	~	x		
cvas	cvcs	roadside log update	cvas	w	x	x	x	x		
emms	rs	pollution data	emms	w	x		~	x		
tas	tcs	Toll Transactions	tas	w	x	x	x	x	x	x
tms	tms	freeway control data	rs	w	x		x	x		
tms	tms	hri control data	rs	w	x		x	x		
tms	tms	hri request	rs	w	x		~	x		
tms	tms	signal control data	rs	w	x		x	x		
tms	tms	surveillance control	rs	w	x		~	x		
tms	rs	HOV data	tms	w	x		~	x		
tms	rs	fault reports	tms	w	x		~	x		
tms	rs	freeway control status	tms	w	x		~	x		
tms	rs	hri status	tms	w	x		x	x		
tms	rs	incident data	tms	w	x	x	~	x		
tms	rs	intersection blockage notification	tms	w	x		x	x		
tms	rs	local traffic flow	tms	w	x		~	x		
tms	rs	request for right of Way	tms	w	x		~	x		
tms	rs	signal control status	tms	w	x		~	x		
tms	rs	signal priority request	tms	w	x		~	x		
MDOT Central to/from MDOT Vehicle										
trms	trms	emergency acknowledge	trvs	u1t	x		x	x		
trms	trvs	emergency notification	trms	u1t	x	x	x	x		
MDOT Central to/from Traveler										
trms	trms	emergency acknowledge	rts	w	x		x	x		
trms	trms	transit and fare schedules	rts	w	x	x	~	x		x
trms	trms	traveler information	rts	w	x	x	x	x	x	x
trms	rts	emergency notification	trms	w	x	x	x	x		
trms	rts	transit request	trms	w	x	x	x	x	x	x
trms	rts	traveler information request	trms	w	x	x	x	x	x	x

Note: "X" markings in the Threat Category Columns are in accordance with the Mitretek analysis.

Exhibit B - 1 (continued)

Subsystem	Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES DoS	Dis	Man	Mas	Rpy	Rpd
MDOT Central to/from Terminators										
cvas	cvas	payment request	x21 Financ'l Inst.	w	x		~	x	x	x
cvas	cvas	tax-credentials-fees request	x22 Govt. admin	w	x	x	~	x		x
cvas	x21 Financ'l Inst.	transaction status	cvas	w	x		~	x	x	x
tas	tas	payment request	x21 Financ'l Inst.	w	x	x	x	x	x	x
tms	tms	hri advisories	x67 Rail operations	w	x		x	x		
tms	x58 Weather serv'ce	weather information	tms	w	x		~	x		
tms	x67 Rail operations	railroad advisories	tms	w	x		x	x		
tms	x67 Rail operations	railroad schedules	tms	w	x		~	x		
trms	trms	payment request	x21 Financ'l Inst.	w	x	x	x	x	x	x
trms	trms	camera control	x42 Secure area env.	w	x		x	x		
trms	trms	emergency acknowledge	x42 Secure area env.	w	x		x	x		
trms	x21 Financ'l Inst.	transaction status	trms	w	x	x	x	x	x	x

Note: "X" markings in the Threat Category Columns are in accordance with the Mitretek analysis.

Exhibit B - 2. MDOT Roadside System Threats

Subsystem	Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
					DoS	Dis	Man	Mas	Rpy	Rpd
MDOT Roadside to/from MDOT Central										
cvcs	cvcs	credentials information reque	cvas	w	x	x	~	x		
cvcs	cvcs	roadside log update	cvas	w	x	x	x	x		
cvcs	cvas	credentials information	cvcs	w	x	x	~	x		
cvcs	cvas	CVO database update	cvcs	w	x	x	x	x		
rs	rs	pollution data	emms	w	x		~	x		
rs	rs	fault reports	tms	w	x		~	x		
rs	rs	freeway control status	tms	w	x		~	x		
rs	rs	hri status	tms	w	x		x	x		
rs	rs	incident data	tms	w	x	x	~	x		
rs	rs	intersection blockage notificat	tms	w	x		x	x		
rs	rs	local traffic flow	tms	w	x		~	x		
rs	rs	request for right of Way	tms	w	x		~	x		
rs	rs	signal control status	tms	w	x		~	x		
rs	rs	signal priority request	tms	w	x		~	x		
rs	tms	freeway control data	rs	w	x		x	x		
rs	tms	hri control data	rs	w	x		x	x		
rs	tms	hri request	rs	w	x		~	x		
rs	tms	signal control data	rs	w	x		x	x		
rs	tms	surveillance control	rs	w	x		~	x		
tcs	tcs	Toll Transactions	tas	w	x	x	x	x	x	x
rs	rs	HOV data	tms	w	x		~	x		
MDOT Roadside to/from Vehicle										
cvcs	cvcs	clearance event record	cvs	u2	x	x	~	x	x	
cvcs	cvcs	lock tag data request	cvs	u2	x		~	x	x	
cvcs	cvcs	pass/pull-in	cvs	u2	x	x	x	x	x	
cvcs	cvs	lock tag data	cvcs	u2	x	x	x	x	x	
pms	vs	tag data	pms	u2	x	x	x	x	x	x
rs	evs	emergency vehicle preemptio	rs	u2	x		~	x	x	
rs	trvs	local signal priority request	rs	u2	x		~	x	x	
tcs	tcs	request tag data	vs	u2	x		~	x	x	x
tcs	tcs	tag update	vs	u2	x	x	x	x	x	x
tcs	vs	tag data	tcs	u2	x	x	x	x	x	x
pms	pms	request tag data	vs	u2	x	x	x	x	x	x
pms	pms	tag update	vs	u2	x	x	x	x	x	x
MDOT Roadside to/from External										
pms	pms	payment request	x21 Financ'l Inst.	w	x	x	x	x	x	x
pms	x21 Financ'l Inst.	transaction status	pms	w	x	x	x	x	x	x
rs	rs	grant right of way and/or stop	x29 Multimodal cross'ngs	w	x		x	x		
rs	rs	hri status	x66 Wayside equipm't	w	x		x	x		
rs	rs	intersection blockage notificat	x66 Wayside equipm't	w	x		x	x		
rs	x29 Multimodal cross'ngs	request for right of Way	rs	w	x		x	x		
rs	x29 Multimodal cross'ngs	right of way preemption reque	rs	w	x		x	x		
rs	x66 Wayside equipm't	arriving train information	rs	w	x		x	x		
rs	x66 Wayside equipm't	track status	rs	w	x		x	x		

Note: "X" markings in the Threat Category Columns are in accordance with the Mitretek analysis.

Exhibit B - 3. MDOT Vehicle System Threats

Subsystem	Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
					DoS	Dis	Man	Mas	Rpy	Rpd
MDOT Vehicle to/from Central										
trvs	trvs	emergency notification	trms	u1t	x	x	x	x		
trvs	trms	emergency acknowledge	trvs	u1t	x		x	x		
Vehicle to/from Roadside										
trvs	trvs	local signal priority request	rs	u2	x		~	x	x	
vs	vs	tag data	pms	u2	x	x	x	x	x	x
vs	vs	tag data	tcs	u2	x	x	x	x	x	x
vs	pms	request tag data	vs	u2	x	x	x	x	x	x
vs	pms	tag update	vs	u2	x	x	x	x	x	x
vs	tcs	request tag data	vs	u2	x		~	x	x	x
vs	tcs	tag update	vs	u2	x	x	x	x	x	x
cvs	cvcs	lock tag data request	cvs	u2	x		~	x	x	
cvs	cvcs	clearance event record	cvs	u2	x	x	~	x	x	
cvs	cvs	lock tag data	cvcs	u2	x	x	x	x	x	
cvs	cvcs	pass/pull-in	cvs	u2	x	x	x	x	x	

Note: "X" markings in the Threat Category Columns are in accordance with the Mitretek analysis.

Exhibit B - 4. MDOT Traveler Information System Threats

Subsystem	Source	Physical Data Flow	Destination	Inter-connect	THREAT CATEGORIES					
					DoS	Dis	Man	Mas	Rpy	Rpd
MDOT traveler to/from Central										
rts	rts	emergency notification	em	w,u1t	x	x	x	x		
rts	rts	emergency notification	trms	w	x	x	x	x		
rts	em	emergency acknowledge	rts	w,u1t	x		x	x		x
rts	trms	emergency acknowledge	rts	w	x		x	x		
rts	rts	transit request	trms	w	x	x	x	x	x	x
rts	rts	traveler information reques	trms	w	x	x	x	x	x	x
rts	trms	transit and fare schedules	rts	w	x	x	~	x		x
rts	trms	traveler information	rts	w	x	x	x	x	x	x

Note: "X" markings in the Threat Category Columns are in accordance with the Mitretek analysis.

Acronym List

AHS	Automated Highway System
AVI	Automatic Vehicle Location
AVI	Automated Vehicle Identification
AVL/M	Automatic Vehicle Location and Monitoring
BWI	Baltimore Washington International
CHART	Chesapeake Highway Advisories (for) Routing Traffic
COTS	Commercial off-the-shelf
CVAS	Commercial Vehicle AdministrationSubsystem
CVCS	Commercial Vehicle Check Subsystem
CVISN	Commercial Vehicle Information Systems and Networks
CVO	Commercial Vehicle Operations
CVS	Commercial Vehicle Subsystem
DMV	Department of Motor Vehicles
EM	Emergency Management Subsystem
EMMS	Emissions Management Subsystem
ETC	Electronic Toll Collection
EVS	Emergency Vehicle Subsystem
FMS	Fleet and Freight Management Subsystem
FTP	File Transfer Protocol
H	Human Interface
HAZMAT	Hazardous materials
ISC	Information Systems Center
ISDN	Integrated Services Digital Network
ISP	Information Service Provider
ITI	Intelligent Transportation Infrastructure
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
LAN	Local area network
MAA	Maryland Aviation Administration
MARC	Maryland Commuter Rail Passenger Service

MDOT	Maryland Department of Transportation
MdTA	Maryland Transportation Authority
MPA	Maryland Port Administration
MTA	Mass Transit Administration
MVA	Motor Vehicle Administration
P	Physical
PDA	Personal Digital Assistant
PIAS	Personal Information Access Subsystem
PIN	Personal identification number
PMS	Parking Management Subsystem
PS	Planning Subsystem
PSTN	Public Switched Telephone Network
RS	Roadway Subsystem
RTS	Remote Traveler Subsystem
S	Payment Instrument
SHA	State Highway Administration
SOC	Statewide Operations Center
TAS	Toll Administration Subsystem
TCC	Traffic Control Center
TCS	Toll Collection Subsystem
TMS	Traffic Management Subsystem
TOC	Traffic Operations Center
TRMS	Transit Management Subsystem
TRVS	Transit Vehicle Subsystem
TWIN	Transit Watch Information Network
US DOT	United States Department of Transportation
U1t	2-way wide-area wireless
U1b	1-way wide-area wireless (broadcast)
U2	2-way short-range
VE	Video enforcement
VLU	Vehicle Logic Unit
VMS	Variable message sign
VS	Vehicle Subsystem

W	Wireline
WAN	Wide area network
x02	Intermodal Transportation Service Provider
x03	Basic vehicle
x06	Commercial vehicle driver
x08	Commercial Vehicle
x09	Construction and Maintenance
x10	CVO inspector
x12	Driver
x18	Environment
x19	Event Promoters
x21	Financial Institution
x22	Government Administrators
x23	Map Update Provider
x29	Multimodal Crossings
x33	Other TRM
x35	Other TM
x36	Parking Operator
x37	Parking service provider
x38	Pedestrians
x41	Roadway environment
x42	Secure area environment
x43	Toll operator
x44	Toll service provider
x45	Traffic
x46	Traffic operations personnel
x47	Transit fleet manager
x49	Transit system operators
x50	Transit user
x51	Transit vehicle
x52	Transit driver
x53	Transit maintenance personnel
x56	Traveler

x57	Vehicle characteristics
x58	Weather service
x59	Other CVAS
x61	Payment instrument
x62	Enforcement agency
x64	DMV
x65	CVO information requester
x66	Wayside equipment
x67	Rail operations

Bibliography

1. Biesecker, Keith; Jones, Kevin; Foreman, Elizabeth; and Staples, Barbara*Intelligent Transportation Systems (ITS) Information Security Analysis (DRAFT)* . Mitretek Systems Corporation for Federal Highway Administration, U.S. Department of Transportation (US DOT), Project Number 099618C4-0A, Contract Number DTFH61-95-C-00040. Washington, D.C., May 1997.
2. Booz·Allen & Hamilton,*Authentication Analysis (DRAFT).* Maryland Department of Transportation (MDOT), Information Systems Center,June 20, 1997.
3. Booz·Allen & Hamilton,*Firewall Analysis.* MDOT, Information Systems Center, October 1, 1996.
4. Booz·Allen & Hamilton,*Network Security Policy (DRAFT).* MDOT, Information Systems Center, GlenBurnie, MD, February 19, 1997
5. Booz·Allen & Hamilton.*Security Assessment Report.* MDOT, Motor Vehicle Administration, July 11, 1996.
6. Booz·Allen and Hamilton,*State of Maryland Network Study.* State of Maryland, 1997. http://www.dgs.state.md.us/~dgs/netstud.html.
7. Computer Sciences Corporation,*Intelligent Transportation Systems Telecommunications - Public or Private?* US DOT ITS Joint Program Office and MDOT, State Highway Administration, 1996.
8. Computer Sciences Corporation,*Maryland State Highway Administration CHART Telecommunications Analysis Summary Report.* MDOT, State Highway Administration, 1996.
9. Computer Sciences Corporation,*Maryland State Highway Administration Enterprise-Wide Network Study Report.* MDOT, State Highway Administration, 1995.
10. *Consolidated Transportation Program, 1997 State Report on Transportation FY 1997-FY 2002.* MDOT, Annapolis, MD, 1997.
11. *Electronic Toll Collection System & Related Services, Request for Proposals, Contract No. MA-661-000-006* . Maryland Transportation Authority, Baltimore, MD, 1995.
12. *Intelligent Transportation Systems, Building the ITI: Putting the National Architecture into Action.* US DOT, Washington, DC, 1997.
13. *ITS Architecture Browsing Site.* (The ITS National Architecture Development Program and the ITS Architecture Browsing Site is jointly developed by Lockheed Martin and Rockwell International and funded by a contract with the Federal Highway Administration (FHWA) Joint Program Office (JPO).) January 1997. http://www.rockwell.com/itsarch/.
14. Maryland State Data Security Committee*State Computerized Record System Security Requirements and Recommendations.* July 12, 1996.

15. *Maryland Transportation Plan, Implementation Report.* Maryland Department of Transportation, Annapolis, MD, 1997.

16. McGarigle, Bill. "Trucking into the Future," *ITS World*, May/June 1997.

17. *Standards and Procedures Manual, Administrative Volume, Security.* MDOT, Information Systems Center, October 9, 1996.

18. US DOT. *The National Architecture for ITS: A Framework for Integrated Transportation into the 21st Century.* (CD-ROM collection of a number of important ITS policy and architecture documents) Washington, DC, 1997.