



**U.S. Department of Transportation
John A. Volpe National Transportation Systems Center**

**State of Maryland
Intelligent Transportation Systems
Security Implementation
Recommendations**

**November 1, 1997
By
Computer Sciences Corporation**

1. Report No. FHWA-JPO-98-014		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle STATE OF MARYLAND INTELLIGENT TRANSPORTATION SYSTEMS SECURITY IMPLEMENTATION RECOMMENDATIONS			5. Report Date NOVEMBER, 1997		
			6. Performing Organization Code		
7. Author(s) James Ruby, Dan King, Larry Gunshol, and Gene Hilborn			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. (TRAVIS)		
			11. Contract or Grant No. DTRS-57-95-C-0044		
12. Sponsoring Agency Name and Address Department of Transportation FHWA intelligent Transportation Systems Joint Program Office 400 Seventh Street, S.W. - Room 8422 Washington, D.C. 20590			13. Type of Report and Period Covered		
			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 from the US DOT Joint Program Office in May of 1997, Project Number 099618C4-0A					
17. Key Words Intelligent Transportation Systems, Security, Maryland			18. Distribution Statement No restrictions. This document is available to the public from: The National Technical Information Service Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 76	22. Price

Table of Contents

Executive Summary	vii
1 Introduction	1
1.1 The Problem	1
1.2 Maryland Subsystems and Modals.....	2
1.3 Critical Data Flows	3
1.4 Process for the development of Maryland Security Implementation Recommendations	3
2 Maryland Security Policy in Support of ITS.....	5
2.1 “Strawman” ITS Security Policies.....	5
2.2 Existent Security Policies Which Impact ITS	6
2.3 Comparison with “Strawman” Security Policies.....	7
2.4 Recommended Policy Additions.....	8
3 Mapping of State of Maryland Critical Data Flows to ITS Security Requirements.....	11
3.1 General ITS Security Requirements.....	11
3.2 Center System Requirements	12
3.3 Roadside System	14
3.4 Vehicle System	15
3.5 Remote Access System.....	16
4 Discussion of Candidate Security Countermeasures for Maryland ITS Security Requirements	19
4.1 Protective Countermeasures.....	19
4.2 Access Control.....	20
4.3 User Authorizations	23
4.4 User I&A.....	24
4.5 User Accountability	25
4.6 Communication Security	26
4.7 Network Entity I&A.....	27

5 Recommendations for the Implementation of Specific Security Countermeasures for Maryland ITS.....	30
5.1 Recommended Security Countermeasures for ITS Subsystems.....	30
5.1.1 Center System	32
5.1.2 Remote Access (Traveler) System.....	33
5.1.3 Roadside System.....	33
5.1.4 Vehicle System.....	34
5.2 Funded ITS Projects Mapped to Maryland Subsystems and Countermeasures	36
6 Barriers to Implementation	38
6.1 Policy.....	38
6.2 Organizational.....	38
6.3 Technical	38
6.4 Resources	39
7 Conclusions and Recommendations.....	40

List of Exhibits

1-1. National ITS Physical Architecture Model.....	2
1-2. Map of MDOT Modals to National ITS Architecture Subsystems	3
1-3. Process for Development of Implementation Recommendations.....	3
2-1. "Strawman" Security Policies for ITS.....	5
2-2. Comparison of “Strawman” and Maryland/MDOT Security Policies	7
2-3. Recommended Policy Additions	8
3-1. Mapping of Central System Requirements to Critical Data Flows.....	13
3-2 Mapping of Roadside System Requirements to Critical Data Flows	15
3-3. Mapping of Vehicle System Requirements to Critical Data Flows	16
3-4. Mapping of Remote Access System Requirements to Critical Data Flows.....	17
4-1. Protection Requirements and Candidate Countermeasures	20
5-1. Specific Countermeasures for Maryland ITS.....	31

Appendix - Funded Maryland ITS Projects Mapped to Maryland Subsystems

Acronym List

Bibliography

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). The Phase 1 document, *State of Maryland Intelligent Transportation Systems Security Requirements Recommendations*, developed specific security requirements for Maryland ITS systems while this 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 that could be applied to protect those data flows.

Ms. Alisoun Moore, Chief Information Officer (CIO) of Maryland Department of Transportation (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@volpe1.dot.gov

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

Executive Summary

ITS Security Implementation Recommendations

The Phase 1 document, *State of Maryland Intelligent Transportation Systems Security Requirements Recommendations*, November 1, 1997, contains specific security requirements for MDOT ITS. This Phase 2 document, *State of Maryland Intelligent Transportation System Security Implementation Recommendations*, provides:

- A description of “strawman” security policies applicable to all ITS systems (Section 2.1), a comparison of these “strawman” policies to existent Maryland security policies, and recommendations for additional security policies to strengthen Maryland ITS (Sections 2.3 and 2.4),
- A “mapping” of Maryland Critical Data Flows to ITS security requirements (Section 3),
- Candidate security countermeasures for ITS (Section 4) and specific recommendations for Maryland ITS (Section 5.1),
- A “mapping” of funded Maryland ITS projects to Maryland systems and subsystems (Section 5.2),
- A description of barriers to the implementation of the recommended countermeasures (Section 6), and
- Recommendations for an approach to the design for security systems for ITS (Section 7).

Strawman Security Policies

In Phase 1 of this study, “strawman” security policies were developed based on a high-level discussion of the associated business risks for Maryland critical ITS data flows, i.e., what is the likely cost of providing security protection for certain data flows versus the cost of the damage that might result from a failure to do so. In Phase 2, these “strawman” policies are compared to existent Maryland security policies to identify security “gaps” that might result in the protection of Maryland ITS. While most Maryland security policies were found to provide protection for ITS as well as existent data processing and communications systems (Section 2.3, page 7), the following additions to Maryland security policy are recommended to strengthen the protection of ITS in Maryland.

Recommended Security Policy Additions

- All originations, additions, deletions, and other accesses to sensitive/critical information by system users should require prior authorization and should ensure the accountability of each user.
- All automated transactions between distributed subsystems must be based on accurate mutual identification and authentication of the transacting subsystems.
- Equally rigorous information and telecommunications security technology must be extended from the ITS center systems to ITS remote access, vehicle, and roadside systems.
- 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.
- ITS security requirements should be incorporated into planning for and the design of all new ITS and any solicitation for ITS should include security as a weighted evaluation factor.
- An MDOT ITS Security Officer should be appointed by the Maryland Secretary of Transportation 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 Group to support the State Data Security Committee.
- An information processing security training and awareness program must be implemented for ITS.

Each of these recommendations is intended to strengthen the policy foundation on which more detailed ITS requirements and countermeasures rest.

Security Requirements and Data Flows

From the broad policies cited above, specific security requirements were derived for Maryland ITS. These security requirements were provided in the Phase 1 report but in this Phase 2 report they are mapped to critical Maryland data flows. The reason for this mapping is to ensure that the derived security requirements encompass each and every critical data flow. Mapping these critical data flows in this fashion provides a high level of confidence that countermeasures developed in response to specific security requirements will indeed protect the critical flows associated with those same requirements.

Candidate Security Countermeasures for ITS

Section 4, Exhibit 4-1, page 20 of this report provides a table describing alternative security countermeasures for ITS. These security countermeasures are organized into six general areas of protection. Briefly, these protection categories are:

- **Access control** to limit the users' access to information,
- **User authorization** to establish individual user access,

- **User identification and authentication (I&A)** to ensure that users are who they say they are,
- **User accountability** to ensure that the actions of a user can be audited and cannot be denied,
- **Communication security** to protect information from unauthorized origination, viewing/copying, modification, and deletion, and
- **Network entity** identification and authentication to ensure that, just as with individual users, communicating systems/networks are in fact the systems/networks portrayed.

The candidate countermeasures that are capable of providing protection in each of these protection categories are described in detail in Section 4. The purpose of each is, of course, to ensure that the overall objective of ITS availability, confidentiality, integrity, and authenticity is met.

Security Countermeasures Recommended for Maryland ITS

Which countermeasures are appropriate to meet the security needs of Maryland ITS? Ultimately, that is the question that has to be answered. The answer depends on such factors as the legacy applications and complete subsystems to be retained; MDOT funding availability; the impact on other systems sharing the same physical network or platforms; and security product availability and cost at the time a detailed design and implementation are performed. All of these factors are beyond the scope of this present effort. However, what can be done is to identify those countermeasures that are appropriate to Maryland ITS and from which a final choice can be made when an actual ITS security design is accomplished.

Exhibit ES-1 (also included as Exhibit 5-1, page 30), identifies those countermeasures that are applicable to Maryland ITS for each ITS system—center, remote access, roadside, and vehicle. Center systems include traffic management, emissions management, transit management, toll administration, and commercial vehicle administration subsystems. Remote access or traveler systems represent platforms (kiosks, home/office computers, etc.) for ITS functions of interest to travelers or commercial bus operators in support of multimodal traveling. Roadside systems include functions that require convenient access to a roadside location for the deployment of sensors, signals, programmable signs, toll collection, commercial vehicle checks, and other interfaces with travelers and vehicles of all types. Vehicle subsystems are installed in public, personal and commercial vehicles for the purposes of navigation, advanced vehicle control, toll collection, commercial vehicle status, and, in transit vehicles, to provide operational data, network status, and enroute traveler information.

Exhibit ES-1. Specific Countermeasures for Maryland ITS

Type of Protection Requirement	Candidate Mechanism Types	Maryland ITS Systems				Other
		Center System	Remote Access System	Roadside System	Vehicle System	External System
1. Access Control	a. External physical/admin controls only	No	Yes	Yes	Yes	
	b. Platform-O/S access control mechanism.	Yes		Yes		
	c. Appliqué access control mechanism.	Yes		No		
	d. Appl-specific access control mechanism	Yes		Yes		
2. User Authorization	e. External physical/admin records only	No	Yes	Yes	Yes	
	f. Platform-operating system user account establishment and access privilege entry	Yes		Yes		
	g. Appliqué access control mechanism account establishment and access privilege entry	Yes		No		
	h. Application-specific access control mechanism account establishment and access privilege entry	Yes		Yes		
3. User I&A	i. None	No		No		
	j. External	No	Yes	Yes		
	k. Identifier & Fixed password	Yes		Yes		
	l. Identifier & Dynamic password	Yes		Yes	Yes	
	m. [Identifier &] Biometric data	Yes		No		
	n. Shared secret-challenge response	Yes		Yes		
	o. User token device + shared secret	Yes		No		
	p. User token device + digital signature	Yes		No		
	q. Integrated with other crypto protections	Yes	Yes	No	Yes	
4. User Accountability	r. None	No		No		
	s. External logging (e.g., paper records)	No	Yes	Yes	Yes	
	t. Native platform O/S system audit trail	Yes		Yes		
	u. Appliqué audit trail mechanism	Yes		No		
	v. Appl-specific accountability mechanisms	Yes		Yes		
5. Comm Security	w. Physical isolation	No	No	No	No	
	x. Enclave-level net screening mechanism	No	No	No	No	No
	y. Data link level encr/error det, node-node	Yes	Yes	Yes	Yes	No
	z. End-to-end encr/error-detection bet pltfms	Yes	Yes	Yes	Yes	Yes
	aa. End-to-end encr/error-detection bet apps	Yes	Yes	Yes	Yes	Yes
6. Network Entity I&A	bb. None/Anonymous peer system	No	No	No	No	No
	cc. None/Physical isolation	No	No	No	No	No
	dd. Shared secret exchanged in the clear	Yes	Yes	Yes	Yes	Yes
	ee. Shared secret-based response	Yes	Yes	Yes	Yes	Yes
	ff. Digital signature of challenge/time/etc.	Yes	Yes	Yes	Yes	Yes
	gg. Integrated with other cryptographic protections	Yes	Yes	Yes	Yes	Yes

A detailed discussion of these countermeasures as they apply to Maryland ITS is contained in Section 5 of this report.

Mapping of Funded Maryland ITS Projects to Maryland ITS Systems and Countermeasures

The usefulness of the previous table extends beyond the identification of security countermeasures for Maryland ITS. It can also be used to determine which countermeasures are appropriate for specific Maryland ITS projects.

The Appendix to this report contains a description of all known Maryland ITS projects including, in Exhibit A-1, a table mapping these projects to ITS systems and subsystems. With this information, one can identify the ITS system types for each Maryland project and then, using the table provided above, identify the appropriate countermeasures for that project. By way of example, a Maryland project to “Upgrade Transit Information Center” is identified in Exhibit A-1 as both a Center system and Remote Access system project. Using Exhibit 5-1, the Center and Remote Access columns identify those countermeasures applicable to this Maryland project.

In the design and implementation of the project, each of the security countermeasures identified above should be considered for implementation. This consideration should be structured within the framework of a business risk analysis, i.e., what is the cost of providing this countermeasure versus the cost of the damage that might result from a failure to do so. As a final step in the design process, any security countermeasures designed into a project should be mapped against the data flows for that project to ensure that each and every critical data flow is in fact protected.

Barriers to Implementation

In the end, effective ITS security is a function of the quality of MDOT ITS management and personnel and the sufficiency of funds made available for implementation. The telecommunications networks supporting ITS must be managed; systems to ensure availability, confidentiality, and integrity must be installed; auditing programs must be put in place; and qualified security personnel must be made available to review the information obtained. **Failure to do so is likely to result in significant tax, license, toll, and fare revenue losses to the state; loss of competitive information to commercial vehicle operators with attendant loss of trust; and, more importantly, a loss of MDOT’s reputation as a leader in ITS implementation and management.**

In the implementation of ITS security, MDOT may not have to rely on its resources alone. There is considerable interest at the Federal level in the security of ITS and the possibility for joint, innovative approaches to ITS security would appear to exist.

Conclusions and Recommendations

In the conduct of this study of the security vulnerabilities of Maryland ITS systems, both Phases 1 and 2, a number of conclusions were reached as to the usefulness of data flow information from the national ITS physical model and the most effective approach to actually designing countermeasures for ITS systems. Specific findings include the following.

- Data flow information from the national ITS physical model is useful in conceptualizing ITS system and subsystem relationships and is helpful in the development of broad security policies affecting ITS.
- The security policies developed as part of this study (Section 2.1) should be applicable to all state ITS.
- Critical data flows applicable to a particular state are useful in the development of specific ITS security requirements for that state based on a high-level business risk analysis of those flows.
- The mapping of critical data flows to specific ITS security requirements (Section 3) ensures that each and every critical data flow is protected by a required security mechanism.
- The candidate security countermeasures identified as part of this study (Section 4) are applicable to all state ITS although the specific recommendations contained in Section 5 (Exhibit 5-1) must be tailored to individual state needs.
- The mapping of individual state ITS projects (Section 5) to specific ITS systems and subsystems combined with the use of Exhibit 5-1 provides a useful way to identify which countermeasures are applicable to specific ITS projects.
- In the design and implementation of a specific ITS project, each of the security countermeasures identified for that project should be considered for implementation. This consideration should be structured within the framework of (1) does it meet an identified security requirement and (2) what is the cost of providing this countermeasure versus the cost of the damage that might result from a failure to do so.
- As a final step in the design process, all security countermeasures designed into a project should be mapped against the data flows for that project to ensure that each and every critical data flow is in fact protected.

Complementing these conclusions, a number of recommendations are made throughout this report. Specific additions to existent Maryland security policy are recommended in Section 2.4, Exhibit 2-3, and recommendations for security countermeasures applicable to Maryland ITS are made in Section 5.1, Exhibit 5-1, page 30.

While most of these recommendations address specific issues, there is one additional recommendation concerning communications protocols that deserves special note. Standards-based communication protocols, such as the evolving IP version 6 (next generation IP), offer built-in support for authentication and other network security mechanisms. The new National Transportation Communications for ITS Protocol (NTCIP) is another evolving protocol for the transmission of data and messages between ITS devices that should evolve to include embedded security mechanisms. We strongly recommend that MDOT follow these developments closely

because the use of new communications protocols such as those described would effectively solve many, but not all, of the identification and authentication issues discussed in this report.

Finally, we suggest that current and planned Maryland ITS projects be “tested” against the “strawman” security policies enumerated in Exhibit 2-1 and the candidate security countermeasures described for each ITS system category in Exhibit 5-1. This is a relatively simple step that can be accomplished by Maryland ITS project personnel with a small expenditure of time and money. **In those cases where security policies or countermeasures are not met, corrective action is essential if Maryland revenue sources and citizen confidence in MDOT are to be maintained.**

1 Introduction

At the direction of the Volpe Center of Cambridge, MA, a two-phase study has been conducted of the security vulnerability of Maryland Intelligent Transportation Systems (ITS). The overall purpose of the study is to analyze the National ITS Architecture and to recommend security requirements and candidate countermeasures for derived State of Maryland Department of Transportation (MDOT) ITS data flows. This study supplements the *ITS Vulnerability Study* being conducted jointly by the Presidential Commission on Critical Infrastructure Protection (PCCIP) and by the Intelligent Transportation System Joint Program Office (JPO) of the United States Department of Transportation.

The first phase in this study, *State of Maryland Intelligent Transportation Systems Security Requirements Recommendations*, November 1, 1997, contained specific security requirements for MDOT ITS. This Phase 2 document, *State of Maryland Intelligent Transportation System Security Implementation Recommendations*, describes the “strawman” security policies from which these requirements were derived, compares those “strawman” security policies with existent State of Maryland and MDOT security policies to identify policy “gaps,” verifies that derived security requirements cover all critical data flows, recommends specific security countermeasures to strengthen the security of Maryland’s ITS, and finally suggests an approach for the design of security countermeasures for ITS.

1.1 The Problem

ITS systems benefit the citizens of Maryland in a variety of ways including but not limited to:

- 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
- Commercial Vehicle Operations

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. Finally, the **authenticity** of the information can be modified to fraudulently repudiate financial transactions involving credit card numbers which would result in financial loss to the issuing institution.

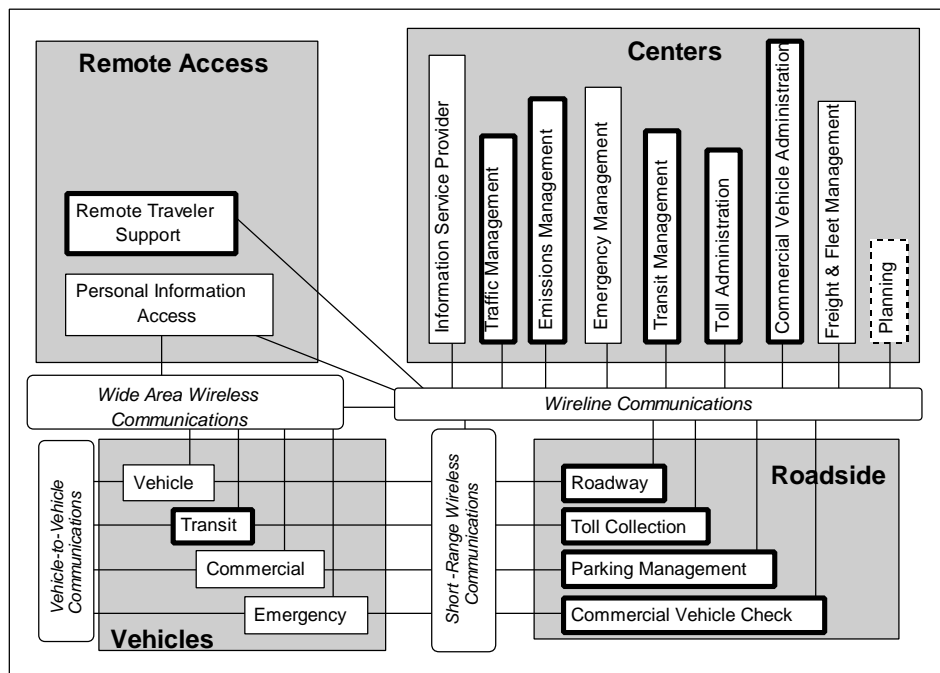
1.2 Maryland Subsystems and Modals

The National ITS Physical Architecture model is shown in Exhibit 1-1. This architecture provides a common frame of reference for the discussion of ITS issues including ITS security.

The ITS architecture is composed of four major systems and 19 subsystems which support ITS functions. The lines shown between the various subsystems represent data flows between the systems and subsystems.

Those ITS functions which are the responsibility of MDOT are outlined with “bold” borders in Exhibit 1-1.


Exhibit 1-1. National ITS Physical Architecture Model



All subsystems do not exist in every ITS and, even where they do exist, they may not all be the direct responsibility of a single entity. In the case of Maryland, only 11 subsystems are the direct responsibility of the State and it is these subsystems that are discussed in this document. It should also be noted that a one-for-one correlation between the National model and MDOT organizational elements does not exist. Some MDOT departments have responsibility for multiple ITS subsystems and some ITS subsystems are the responsibility of multiple MDOT departments. This correlation is clearly shown in Exhibit 1-2.

Exhibit 1-2. Map of MDOT Modals to National ITS Architecture Subsystems

MDOT Modal	System											
	Center					Roadside				Vehicle	Remote	
	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

Notwithstanding these differences, the National architecture still serves as a useful device for the discussion of ITS related security issues.

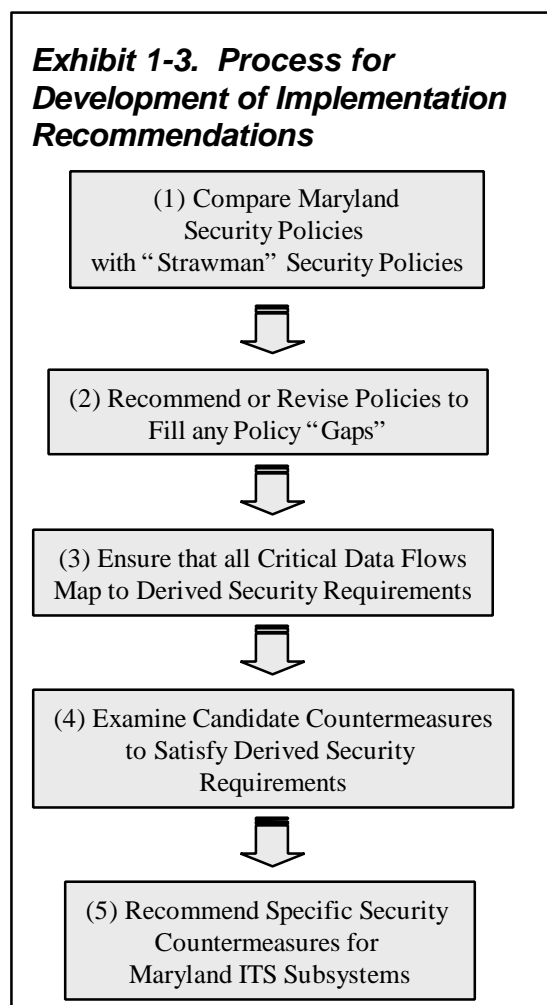
1.3 Critical Data Flows

In Phase 1 of this study, a number of critical data flows were identified. These flows are described in more detail in Section 3 of this report. A critical data flow is one that is so important to the performance of an ITS function that in the absence of that flow the function cannot be successfully performed. Because a given ITS function cannot be accomplished in the absence of these flows, it is these flows that are the focus of attention for the implementation of security measures and any recommended security measures, to be effective, must adequately protect these critical data flows.

1.4 Process for the Development of Maryland Security Implementation Recommendations

The process shown in Exhibit 1-3 and described below was followed in the identification of specific security countermeasures for MDOT ITS.

- (1) Maryland and MDOT security policies were compared to the “strawman” security policies that were used to develop derived security requirements for MDOT ITS (see Section 3 of this report). The purpose of this comparison was to identify any security “gaps” or areas for improvement in existing policies and practices.
- (2) New policies or revisions were recommended to correct any identified policy gaps.



- (3) Critical data flows identified in Phase 1 of this study were mapped to derived security requirements to ensure that these requirements encompassed each and every critical data flow. Mapping these critical data flows in this fashion ensures that solutions developed to satisfy derived security requirements also encompass each and every critical data flow.
- (4) Having ascertained that the derived security requirements cover all critical data flows, candidate countermeasures were examined which would fulfill derived ITS security requirements.
- (5) From these candidates, specific security countermeasures for Maryland ITS were recommended.

2 Maryland and MDOT Security Policies in Support of ITS

Prior to addressing specific security requirements it is useful to examine the “strawman” security policies from which they evolved. How do these “strawman” security policies compare with existent Maryland and MDOT security policies? Do any policy “gaps” exist and, if so, what must be done to correct them?

2.1 “Strawman” ITS Security Policies

In Phase 1 critical data flows were discussed in terms of their associated business security risks, i.e., what is the relative cost of providing security protection for these data flows versus the cost of the damage which might result from a failure to do so.

From these business risk discussions, the following fifteen “strawman” security policies were developed for Maryland ITS.

Exhibit 2-1. "Strawman" Security Policies for ITS

1. Physical and technical security protection must be provided for all MDOT Intelligent Transportation Systems to ensure appropriate availability, confidentiality, integrity, and authenticity of the information contained in or transferred between these systems.
2. Sensitive and/or critical information (e.g., personal, financial, safety, and system security management information) must be afforded especially high quality protection against unauthorized origination, viewing/copying, modification, and deletion.
3. All originations, additions, deletions, and other accesses to sensitive/critical information by system users should require individual user prior authorization, and should ensure individual user accountability.
4. All automated transactions between distributed subsystems must be based on accurate, mutual identification and authentication of the transacting subsystems.
5. All center data processing systems supporting ITS should employ state-of-the-art information and telecommunications security technology, consistent with budgetary constraints.
6. Equally rigorous information and telecommunications security technology must be extended from the ITS center systems to ITS remote access (traveler), vehicle, and roadside systems.
7. 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.
8. 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.”
9. All custom software applications should successfully pass formal test procedures prior to installation in ITS.
10. 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.

11. Configuration management must be exercised on all ITS software and hardware systems.
12. A 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 Group to support the State Data Security Committee.
13. 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.
14. 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.
15. An information processing security training and awareness program must be implemented for ITS.

From these “strawman” policies, specific security requirements for the primary ITS systems—central, roadside, vehicle, and remote access—were identified and are described in Section 3 of this report.

2.2 Existent Security Policies Which Impact ITS

ITS systems are not specifically addressed by current MDOT security policies although there is extensive documentation addressing the security of MDOT data processing systems. Since many of these data processing systems are integral to the performance of the ITS function, the security policies affecting these systems would be applicable to ITS systems as well.

Existent Maryland and MDOT security policies that affect data processing systems supporting the ITS function are described in the following documents:

- *State Computerized Record System Security Requirements and Recommendations*, Revised by the State Data Security Committee, July 12, 1996.
- *FMIS Security Policy for Access to Third-Party Networks*, August 15, 1995.
- *Internet Security and the FMIS Network*, August 1995, prepared by KPMG Peat Marwick LLP Strategic Services Consulting.
- *Maryland Department of Transportation Information Systems Center Standards and Procedures Manual Administrative Volume*, October 9, 1996.
- *Maryland Department of Transportation Information Systems Center Network Security Policy (DRAFT)*, February 19, 1997, prepared for MDOT by Booz-Allen & Hamilton, Inc.

This latter document is included, even though not yet approved for implementation, simply because it is believed to reflect current security thinking within MDOT.

2.3 Comparison with “Strawman” Security Policies

A comparison was made between the “strawman” security policies and the Maryland security documentation cited above. The results are provided below.

Exhibit 2-1. Comparison of “Strawman” and Maryland/MDOT Security Policies

“Strawman” Security Policy	MDOT Security Policies
1. Physical and technical security protection must be provided for all MDOT Intelligent Transportation Systems to ensure appropriate availability, confidentiality, integrity, and authenticity of the information contained in or transferred between these systems.	✓
2. Sensitive and/or critical information (e.g., personal, financial, safety, and system security management information) must be afforded especially high quality protection against unauthorized origination, viewing/copying, modification, and deletion.	✓
3. All originations, additions, deletions, and other accesses to sensitive/critical information by system users should require individual user prior authorization, and should ensure individual user accountability.	↯
4. All automated transactions between distributed subsystems must be based on accurate, mutual identification and authentication of the transacting subsystems.	X
5. All <u>center</u> data processing systems supporting ITS should employ state-of-the-art information and telecommunications security technology, consistent with budgetary constraints.	✓
6. Equally rigorous information and telecommunications security technology must be extended from the ITS <u>center</u> systems to ITS <u>remote access, vehicle, and roadside</u> systems.	X
7. 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 US standards based protocols, and employ commercial-off-the-shelf (COTS) technology that has been subjected to due diligence whenever possible.	↯
8. 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.”	✓
9. All custom software applications should successfully pass formal test procedures prior to installation in ITS.	✓
10. ITS security requirements should be incorporated into planning for and the design of all new ITS and any solicitation for ITS should include security as a weighted evaluation factor.	↯
11. Configuration management must be exercised on all ITS software and hardware systems.	✓
12. 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 Group to support the State Data Security Committee.	X
13. 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.	✓
14. 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.	✓
15. An information processing security training and awareness program must be implemented for ITS.	X

✓ = covered, ↯ = partially covered, X = not covered

This comparison suggests that there are indeed areas addressed in the “strawman” security policy that do not appear to be adequately covered by current Maryland and MDOT security policy or only partially covered. This is to be expected because Maryland and MDOT security policies were written for mainframe and client/server systems, usually installed in state facilities and

operated by state employees, not ITS systems which are distant and more geographically disbursed and vulnerable.

2.4 Recommended Policy Additions

While existing security policies are adequate in most respects, we recommend that they be strengthened in the areas identified in Exhibit 2-3.

Exhibit 2-1. Recommended Policy Additions

- All originations, additions, deletions, and other accesses to sensitive/critical information by system users should require prior authorization and should ensure the accountability of each user.
- All automated transactions between distributed subsystems must be based on accurate mutual identification and authentication of the transacting subsystems.
- Equally rigorous information and telecommunications security technology must be extended from the ITS center systems to ITS remote access, vehicle, and roadside systems.
- 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.
- ITS security requirements should be incorporated into planning for and the design of all new ITS and any solicitation for ITS should include security as a weighted evaluation factor.
- An MDOT ITS Security Officer should be appointed by the Maryland Secretary of Transportation 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 Group to support the State Data Security Committee.
- An information processing security training and awareness program must be implemented for ITS.

In the following paragraphs, each of these recommendations will be examined in more detail:

- All originations, additions, deletions, and other accesses to sensitive/critical information by system users should require prior authorization and should ensure the accountability of each user.

It is clear from Maryland and MDOT policies that systems should incorporate the ability to check users' authorizations every time a new system or resource is accessed. Our recommendation goes further in that it implies that (a) sensitive or critical information in these systems should be clearly identified, (b) for such identified information, each individual must have authorizations that specify their authorized access (e.g., originations, additions, deletions, changes, etc.), and (c) there is an audit trail (for those systems with sensitive/critical information) of individual access actions. This level of detailed enforcement and audit is needed to ensure that individuals scope of action is properly limited to what is authorized, and individuals can be held accountable for misuse of their authorizations and for attempts to exceed their authorizations.

- All automated transactions between distributed subsystems must be based on accurate mutual identification and authentication of the transacting subsystems.

Most information transfer between subsystems occur over networks common to multiple subsystems under diverse management, and even with the public networks, such that connectivity is not constrained by the communication network to be between only authorized subsystems. Consequently the mere self-asserted identity of a network entity is not sufficient to prevent fraud, disruption, and other improper access to these systems. Consequently there must be a means to protect these systems against these threats by strong, mutual identification and authentication.

- Equally rigorous information and telecommunications security technology must be extended from the ITS center systems to ITS remote access, vehicle, and roadside systems.

Current policies clearly define the security requirements of center systems but say little about the need to specifically extend that security to ITS remote access, vehicle, and roadside systems. ITS now expands the security envelope to include sensors and devices located along roadways, in vehicles, and at remote locations supporting travelers. With this expansion, new security problems arise. Some roadside locations make possible direct public access to the devices and systems. Other ITS devices are located in commercial vehicles, e.g., CVISN, or at locations that are not controlled by “cleared” state employees. Many more involve telecommunications technologies such as wireless that has not traditionally been employed in mainframe or client/server environments. All of these changes present vulnerabilities that must be specifically addressed with the same vigor as that applied to existing MDOT data processing systems and centers.

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

In the implementation of ITS security, it is critical that it be based on open standards, cite appropriate security standards, utilize standard telecommunications protocols, and employ COTS security technology whenever possible. This is clearly the direction in the design and implementation of all information systems including ITS and should be clearly stated as a matter of policy.

- ITS security requirements should be incorporated into planning for and the design of all new ITS and any solicitation for ITS should include security as a weighted evaluation factor.

ITS with its roadside, vehicle, and remote access subsystems are more vulnerable than other types of information systems which are located exclusively within data processing centers or at locations under the total control of state employees. Because of these vulnerabilities, security is a much more critical issue which must be incorporated into the total life cycle of ITS. By that we mean that security issues must considered at every stage of project development from inception to maintenance and operation to final disposal. State security policy states that security must be

considered in the design and development of each computerized record system. But is this enough? Even more emphasis could be placed on this requirement by making security a specific, weighted evaluation factor in the contract award process.

- An MDOT ITS Security Officer should be appointed by the Maryland Secretary of Transportation 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 Group to support the State Data Security Committee.
- An information processing security training and awareness program must be implemented for ITS.

Finally, because of the continued growth of ITS and its inherent vulnerabilities, greater emphasis should be placed on security for ITS within the state's security structure. This might be accomplished by the appointment of an MDOT Security Officer to manage ITS development and implementation, the establishment of an ITS Security Working Group to support the State Data Security Committee, and the establishment of a formal ITS information processing and security awareness program.

3 Mapping of State of Maryland Critical Data Flows to ITS Security Requirements

This section “maps” the critical data flows documented in the Phase 1 Report, Appendix B, to the ITS security requirements documented in Section 3 of the Phase 1 Report. Mapping these security requirements in this manner ensures that each and every critical data flow is encompassed by a security requirement. Then, when a countermeasure is identified to fulfill one or more security requirements, there is a high level of assurance that the associated critical data flows are, in fact, protected by that countermeasure. Notwithstanding this high level of assurance, it is still necessary, once the final “suite” of countermeasures has been identified, to yet again examine each data flow to ensure that each and every critical data flow will be protected.

Before “mapping” the critical data flows to specific security requirements it should be noted that there are a few general security requirements that apply to all four ITS systems—not individual data flows. These requirements are administrative in nature and correspond to security policies numbered 7 through 15 in the previous section of this report. These policies will be presented first followed by technical security requirements for the Center, Roadside, Vehicle, and Remote Access systems.

3.1 General ITS Security Requirements

Those general ITS security requirements that apply to all ITS subsystems and not just to individual data flows follow:

- 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 Group 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.

3.2 Center System Requirements

Those Center System technical security requirements documented in the Phase 1 Report, Section 3.2, are duplicated below. It should be noted that as was the case with the administrative security requirements described above, some of the technical requirements provided below apply to the system or subsystem as a whole, not an individual data flow. Hence, while every data flow is identified with an individual requirement, the opposite is not always true.

- 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 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 Center System.
- i) An appropriate mechanism should be implemented to continuously authenticate the source of data entering a Center System.
- j) A mechanism should be implemented to ensure non-repudiation of appropriate data entering a Center System.
- k) A mechanism should be implemented for Center System *servers* 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.

Exhibit 3-1 maps these Center System security requirements to the critical Center System data flows documented in Phase 1, Appendix B, Exhibit B-1. (See Acronym List.)

Exhibit 3-1. Mapping of Central System Requirements to Critical Data Flows

ID	Subsystem	Source	Physical Data Flow	Destination	Inter-connect	Requirement(s) Mapped
MDOT Central to/from MDOT Center						
C1	cvas	cvas	license request	x64 DMV	w	h,k
C2	cvas	x64 DMV	registration	cvas	w	h,k
C3	tms	tms	signal priority status	tms	w	h,k
C4	tms	tms	TMC coord.	x35 Other TM	w	h,k
C5	tms	tms	request for transit signal priority	tms	w	h,k
C6	tms	x35 Other TM	TMC coord.	tms	w	h,k
C7	tms	tms	request for transit signal priority	tms	w	h,k
C8	tms	tms	transit system data	tms	w	h,k
C9	tms	tms	TRMS coord	x33 Other TRM	w	h,k
C10	tms	tms	signal priority status	tms	w	h,k
C11	tms	tms	traffic information	tms	w	h,k
C12	tms	x33 Other TRM	TRMS coord	tms	w	h,k
C13	tms	tms	traffic information	tms	w	h,k
C14	tms	tms	transit system data	tms	w	h,k
MDOT Central to/from Other Center						
C101	cvas	cvas	electronic credentials	fms	w, u1t	i,k,m
C102	cvas	fms	credential application	cvas	w	i,j
C103	cvas	fms	tax filing, audit data	cvas	w	h,i,i,m
C104	tms	tms	incident information request	em	w	k
C105	tms	tms	incident notification	em	w	k
C106	tms	em	emergency vehicle greenwave request	tms	w	h,i
C107	tms	em	incident information	tms	w	h,i
C108	tms	em	incident response status	tms	w	h,i
C109	tms	tms	security alarms	em	w	k
C110	tms	em	transit emergency coordination data	tms	w	h,i
MDOT Center to/from Roadside						
C201	cvas	cvas	credentials information	cvcs	w	k
C202	cvas	cvas	CVO database update	cvcs	w	k
C203	cvas	cvcs	credentials information request	cvas	w	h,i
C204	cvas	cvcs	roadside log update	cvas	w	h,i
C205	emms	rs	pollution data	emms	w	h,i
C206	tas	tcs	Toll Transactions	tas	w	h,i,i
C207	tms	tms	freeway control data	rs	w	k
C207	tms	tms	hri control data	rs	w	k
C209	tms	tms	hri request	rs	w	k
C210	tms	tms	signal control data	rs	w	k
C211	tms	tms	surveillance control	rs	w	k
C212	tms	rs	HOV data	tms	w	h,i
C213	tms	rs	fault reports	tms	w	h,i
C214	tms	rs	freeway control status	tms	w	h,i
C215	tms	rs	hri status	tms	w	h,i
C216	tms	rs	incident data	tms	w	h,i
C216	tms	rs	intersection blockage notification	tms	w	h,i
C218	tms	rs	local traffic flow	tms	w	h,i
C219	tms	rs	request for right of Way	tms	w	h,i
C220	tms	rs	signal control status	tms	w	h,i
C221	tms	rs	signal priority request	tms	w	h,i
MDOT Center to/from MDOT Vehicle						
C301	tms	tms	emergency acknowledge	trvs	u1t	k
C302	tms	trvs	emergency notification	tms	u1t	i

Exhibit 3-1. (Continued)

ID	Subsystem	Source	Physical Data Flow	Destination	Inter-connect	Requirement(s) Mapped
MDOT Center to/from Remote Access						
C401	trms	trms	emergency acknowledge	rts	w	k
C402	trms	trms	transit and fare schedules	rts	w	k
C403	trms	trms	traveler information	rts	w	k
C404	trms	rts	emergency notification	trms	w	h,i
C405	trms	rts	transit request	trms	w	h,i
C406	trms	rts	traveler information request	trms	w	h,i
MDOT Center to/from Terminators						
C501	cvas	cvas	payment request	x21 Financ'l Inst.	w	i,j,m
C502	cvas	cvas	tax-credentials-fees request	x22 Govt. admin	w	j,k,m
C503	cvas	x21 Financ'l Inst.	transaction status	cvas	w	h,i,j,m
C504	tas	tas	payment request	x21 Financ'l Inst.	w	i,k,m
C505	tms	tms	hri advisories	x67 Rail operations	w	k
C506	tms	x58 Weather service	weather information	tms	w	h,i
C507	tms	x67 Rail operations	railroad advisories	tms	w	h,i
C508	tms	x67 Rail operations	railroad schedules	tms	w	h,i
C509	trms	trms	payment request	x21 Financ'l Inst.	w	k,n
C510	trms	trms	camera control	x42 Secure area env.	w	k
C511	trms	trms	emergency acknowledge	x42 Secure area env.	w	k
C512	trms	x21 Financ'l Inst.	transaction status	trms	w	h,i,m

3.3 Roadside System

The recommended Roadside System security requirements documented in the Phase 1 Report, Section 3.3 are duplicated below.

- 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 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.

Exhibit 3-2 maps the Roadside System security requirements to the critical Roadside System data flows documented in the Phase 1 Report, Appendix B, Exhibit B-2.

Exhibit 3-1. Mapping of Roadside System Requirements to Critical Data Flows

ID	Subsystem	Source	Physical Data Flow	Destination	Inter-connect	Requirement(s) Mapped
MDOT Roadside to/from MDOT Central						
R1	cvcs	cvcs	credentials information request	cvcs	w	c
R2	cvcs	cvcs	roadside log update	cvcs	w	c
R3	cvcs	cvcs	credentials information	cvcs	w	c
R4	cvcs	cvcs	CVO database update	cvcs	w	c
R5	rs	rs	pollution data	emms	w	a,b
R6	rs	rs	fault reports	tms	w	a,b
R7	rs	rs	freeway control status	tms	w	a,b
R8	rs	rs	hri status	tms	w	a,b
R9	rs	rs	incident data	tms	w	a,b
R10	rs	rs	intersection blockage notification	tms	w	a,b
R11	rs	rs	local traffic flow	tms	w	a,b
R12	rs	rs	request for right of Way	tms	w	a,b
R13	rs	rs	signal control status	tms	w	a,b
R14	rs	rs	signal priority request	tms	w	a,b
R15	rs	tms	freeway control data	rs	w	e
R16	rs	tms	hri control data	rs	w	e
R17	rs	tms	hri request	rs	w	e
R18	rs	tms	signal control data	rs	w	e
R19	rs	tms	surveillance control	rs	w	e
R20	tcs	tcs	Toll Transactions	tas	w	d
R21	rs	rs	HOV data	tms	w	a,b
MDOT Roadside to/from Vehicle						
R101	cvcs	cvcs	clearance event record	cvcs	u2	d
R102	cvcs	cvcs	lock tag data request	cvcs	u2	d
R103	cvcs	cvcs	pass/pull-in	cvcs	u2	d
R104	cvcs	cvcs	lock tag data	cvcs	u2	e
R105	pms	vs	tag data	pms	u2	e
R106	rs	evs	emergency vehicle preemption request	rs	u2	e
R107	rs	trvs	local signal priority request	rs	u2	e
R108	tcs	tcs	request tag data	vs	u2	e
R109	tcs	tcs	tag update	vs	u2	d
R110	tcs	vs	tag data	tcs	u2	e
R111	pms	pms	request tag data	vs	u2	d
R112	pms	pms	tag update	vs	u2	d
MDOT Roadside to/from Terminator						
R201	pms	pms	payment request	x21 Financ'l Inst.	w	c
R202	pms	x21 Financ'l Inst.	transaction status	pms	w	c
R203	rs	rs	grant right of way and/or stop traffic	x29 Multimodal cross'ngs	w	e
R204	rs	rs	hri status	x66 Wayside equipm't	w	a,b,e
R205	rs	rs	intersection blockage notification	x66 Wayside equipm't	w	a,b,e
R206	rs	x29 Multimodal cross'ngs	request for right of Way	rs	w	e
R207	rs	x29 Multimodal cross'ngs	right of way preemption request	rs	w	e
R208	rs	x66 Wayside equipm't	arriving train information	rs	w	a,b
R209	rs	x66 Wayside equipm't	track status	rs	w	a,b
R210	rs	x99 Device maintainer	Maintain device	rs	w	f

3.4 Vehicle System

The recommended Vehicle System security requirements documented in the Phase 1 Report, Section 3.4 are duplicated below.

- 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.

Exhibit 3-3 maps the Vehicle System security requirements to the critical Vehicle System data flows documented in the Phase 1 Report, Appendix B, Exhibit B-3.

Exhibit 3-1. Mapping of Vehicle System Requirements to Critical Data Flows

ID	Subsystem	Source	Physical Data Flow	Destination	Inter-connect	Requirement(s) Mapped
MDOT Vehicle to/from Central						
V1	trvs	trvs	emergency notification	trms	u1t	g,i
V2	trvs	trms	emergency acknowledge	trvs	u1t	g,i
Vehicle to/from Roadside						
V101	trvs	trvs	local signal priority request	rs	u2	g,i
V102	vs	vs	tag data	pms	u2	a,b,c,d,e,f,g,h,i
V103	vs	vs	tag data	tcs	u2	a,b,c,d,e,f,g,h,i
V104	vs	pms	request tag data	vs	u2	j
V105	vs	pms	tag update	vs	u2	i
V106	vs	tcs	request tag data	vs	u2	i
V107	vs	tcs	tag update	vs	u2	i
V108	cvs	cvcs	lock tag data request	cvs	u2	i
V109	cvs	cvcs	clearance event record	cvs	u2	i
V110	cvs	cvs	lock tag data	cvcs	u2	i
V111	cvs	cvcs	pass/pull-in	cvs	u2	i
MDOT Vehicle to/from Terminator						
V201	trvs	x53 Transit Maintenance Personnel	Maintain vehicle system	trvs	w	k

3.5 Remote Access System

The recommended Remote Access System security requirements documented in the Phase 1 Report, Section 3.5 are duplicated below.

- 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.

Exhibit 3-4 maps the Remote Access System security requirements to the critical Remote Access System data flows documented in the Phase 1 Report, Appendix B, Exhibit B-4.

Exhibit 3-1. Mapping of Remote Access System Requirements to Critical Data Flows

ID	Subsystem	Source	Physical Data Flow	Destination	Inter-connect	Requirement(s) Mapped
MDOT Remote Access to/from Central						
RA1	rts	rts	emergency notification	em	w,u1t	d
RA2	rts	rts	emergency notification	trms	w	d
RA3	rts	em	emergency acknowledge	rts	w,u1t	d
RA4	rts	trms	emergency acknowledge	rts	w	d
RA5	rts	rts	transit request	trms	w	a,b,c
RA6	rts	rts	traveler information request	trms	w	a,b,c
RA7	rts	trms	transit and fare schedules	rts	w	a,b,c
RA8	rts	trms	traveler information	rts	w	a,b,c

4 Discussion of Candidate Security Countermeasures for Maryland ITS Security Requirements

4.1 Protective Countermeasures

For purposes of developing candidate protective countermeasures to be applied to each of the MDOT Intelligent Transportation Systems subsystems and critical data flows between them, Exhibit 4-1 organizes protection requirements into six categories and, corresponding to each, a set of generic candidate countermeasures. The exhibit displays these protection requirement categories and a corresponding set of countermeasures for each. The subsequent paragraphs discuss each of these candidate countermeasures, give illustrative examples, and establish the technical framework for specific recommendations for each MDOT system in Section 5 of this report.

Exhibit 4-1. Protection Requirements and Candidate Countermeasures

Type of Protection Requirement	Candidate Mechanism Types
1. Access Control: Limits access of users to information objects in systems to established user authorizations.	<ul style="list-style-type: none"> a. External physical/administrative controls only b. Platform-operating system access control mechanism c. Appliqué access control mechanism d. Application-specific access control mechanism
2. User Authorization: Establishes individual user access authorizations in systems.	<ul style="list-style-type: none"> e. External physical/administrative records only f. Platform-operating system user account establishment and access privilege entry g. Appliqué access control mechanism account establishment and access privilege entry h. Application-specific access control mechanism account establishment and access privilege entry
3. User I&A: Ensures identification & authentication of users of system.	<ul style="list-style-type: none"> i. None j. External k. Identifier & Fixed password l. Identifier & Dynamic password m. [Identifier &] Biometric data n. Shared secret-challenge response o. User token device + shared secret p. User token device + digital signing q. Integrated with other cryptographic protections
4. User Accountability: Ensures individual user accountability for access to information in systems.	<ul style="list-style-type: none"> r. None s. External logging (e.g., paper records) t. Native platform/operating system audit trail mechanism u. Appliqué audit trail mechanism v. Application-specific accountability mechanisms
5. Communication Security: Protects information communicated between systems against unauthorized origination, viewing/copying, modification, and deletion.	<ul style="list-style-type: none"> w. Physical isolation x. Enclave-level network screening mechanisms (firewalls) y. Data link level encryption & error detection mechanism between network nodes z. End-to-end encryption/error-detection between platforms aa. End-to-end encryption/error-detection between applications
6. Network Entity I&A: Ensures identification & authentication between communicating systems.	<ul style="list-style-type: none"> bb. None/Anonymous peer system cc. None/Physical isolation dd. Shared secret exchanged in the clear ee. Shared secret-based response ff. Digital signing of challenge/nonce gg. Integrated with other cryptographic protections

4.2 Access Control

The purpose of access controls are to limit the access of users to information objects or other resources in systems to those specified in pre-established user authorizations. Accordingly, an access control mechanism can be regarded as a countermeasure to unlimited user access. The

following paragraphs describe a range of access control mechanisms from weak and simple to very strong.

a. External physical/administrative controls only. When a system has no effective internal mechanism to control access, the only possible controls are external, i.e., administratively and physically controlling user access. This level of access control is satisfactory only when a user with physical access is authorized full access to all information in the system. An example of this type of subsystem is a palmtop PC or laptop that might be used by roadside inspectors. Access control to this device is by physical possession and the system is not required to distinguish the access privileges of different users.

b. Platform-operating system access control mechanism. Many contemporary platform operating systems provide information object access control mechanisms that distinguish between the authorizations of individual users. Access control requirements can be fully satisfied by a native platform-operating system, however, only when the information objects for which access control is required are those provided to applications by the operating system, such as files, memory segments, input/output (I/O) channels, etc. For other kinds of information objects, such as those created by applications, additional measures are required.

A widely recognized minimum satisfactory level of platform access control functionality and assurance provides the “controlled access protection” specified as the C2 class in the Trusted Computer System Evaluation Criteria (TCSEC). An equivalent profile has been defined for future evaluations under the Common Criteria. Operating systems that have been evaluated as meeting the requirements of the C2 class are as follows:

- Data General Corporation AOS/VS II, Release 3.01
- Data General Corporation AOS/VS II, Release 3.10
- Digital Equipment Corporation OpenVMS VAX Version 6.0
- Digital Equipment Corporation OpenVMS VAX Version 6.1
- Digital Equipment Corporation OpenVMS VAX and Alpha Version 6.1
- IBM AS/400 with OS/400 V2R3M0
- IBM AS/400 with OS/400 V3R0M5
- Microsoft Corporation Windows NT, Version 3.5
- Tandem Computers Inc. Guardian-90 w/Safeguard S00.01

Additional systems are added to this list from time to time upon completion of their evaluations.

The principal limitation of the access control mechanisms C2 class systems is that the access control mechanism is “discretionary.” The “owner” of an information object has the discretion to set its access permissions. However, once another user or user’s program is given permission to read the object, it is free to make *copies*, and the copying user’s program is then the “owner” of those copies and therefore has the discretion to give access to any other users or their programs. Prevention of this effective “permission passing” can be achieved only by additional access control mechanism, such as controlling the allowed applications to those which are trusted not to make copies, or going to an operation that supports a mandatory access control policy based on labeled information objects and subjects. Systems which have been evaluated as meeting the B1 TCSEC evaluation criteria (“labeled security protection”) are as follows:

- Amdahl Corporation UTS/MLS, Version 2.1.5+
- Digital Equipment Corporation SEVMS VAX Version 6.0
- Digital Equipment Corporation SEVMS VAX Version 6.1
- Digital Equipment Corporation SEVMS VAX and Alpha Version 6.1
- Digital Equipment Corporation ULTRIX MLS+ Version 2.1 on VAX Station 3100
- Harris Computer Systems Corporation CX/SX 6.1.1
- Harris Computer Systems Corporation CX/SX 6.2.1
- Hewlett Packard Corporation HP-UX BLS release 8.04
- Hewlett Packard Corporation HP-UX BLS release 9.0.9+
- Silicon Graphics Inc. Trusted IRIX/B release 4.0.5EPL
- Unisys Corporation OS 1100 Security Release I
- Unisys Corporation OS 1100/2200 Release SB3R6
- Unisys Corporation OS 1100/2200 Release SB3R8
- Unisys Corporation OS 1100/2200 Release SB4R2
- Unisys Corporation OS 1100/2200 Release SB4R7

A few operating systems (not listed here) have been evaluated as meeting the even higher B2 and B3 criteria.

c. Appliqué access control mechanism. “Appliqué access control mechanisms” refer to additional trusted software mechanisms that are applied in addition to the operating system to provide additional access control granularity refinements and other security services. These appliqués are special trusted applications which provide security and other functional services to other (usually less trusted) applications or parts of applications.

The principal example of such a trusted appliqué in wide use is a trusted database management system (DBMS). A trusted DBMS can provide fine-grain access control to database information objects that are not known to the operating system. Some examples of database management systems known to provide good appliqué access control mechanisms include:

- Informix Software, Incorporated INFORMIX-OnLine/Secure 4.1,
- Informix Software, Incorporated INFORMIX-OnLine/Secure 5.0,
- Oracle Corporation Oracle7, and
- Sybase, Inc. SQL Server version 11.0.6.

Some appliqués have been developed to provide a degree of access control and other security services to platforms with little or no security built into the operating system. Two of these have been evaluated as providing minimal protection to PC systems are as follows:

- Fischer International Watchdog PC Data Security, Version 7.0.2
- Okiok Data Ltd. RAC/M and RAC/M II version 3.3

The Fisher Watchdog product adds Identification and Authentication (I&A), Discretionary Access Control (DAC), Audit (AUD), and Object Reuse (OR) features to the DOS operating system.

The Okiok RAC/M product allows multiple users to share a single PC in a controlled manner by providing for access restrictions. There are no required limits on the type of software that can be run on the PC by a user. RAC/M can be used in two main types of applications: to ensure that only authorized users access the PC; and to ensure that in addition to controlling access to the PC, specific users can be prevented from accessing specific data.

DCE (Distributed Computing Environment) is an open standards appliqué that provides general security services, including discretionary access control services to distributed applications, such that robust security services based on cryptographic and other mechanisms are available to applications without the application developers in a standard way.

d. Application-specific access control mechanism. Application-specific access control mechanisms are those that are integral to specific applications. For example, within an application that performs financial transactions, such as authorizing purchases, moving funds, etc., individuals could have different transaction amount authority. Certain high value transactions or the control of what authorizations individuals have could require multiple-user concurrence. Because of their specificity, they are not part of general-purpose products or standards. Nevertheless application-specific access controls should be subject to varying levels of design rigor, design documentation, configuration control, and vulnerability analysis and testing, depending on the sensitivity/value/criticality level of information or function involved. Toll collection and accounting systems are good examples of systems in which application-specific access control mechanisms are typically employed. Because of the relatively high cost of such scrutiny, application-specific access controls for highly sensitive applications should be minimized in favor of pre-evaluated COTS products.

4.3 User Authorizations

The purpose of a user authorization is to clearly pre-establish individual user access authorizations to a system or information objects/resources in it. These authorizations for a user form the basis of access controls that limit that user's accesses. In the following, we describe a range of user authorization mechanisms. They support the basic access control mechanisms that are described in Section 4.2.

e. External physical/administrative record only. When access is granted to a system on the basis of physical access controls, user authorization takes the form of an external record and issuance of such physical control devices as pertain, e.g., keys to doors or equipment locks.

f. Native platform/operating system user account establishment and access privilege entry. All operating systems meeting controlled access protection or higher standards, must provide a mechanism for an authorized administrator to enter/change individual user authorization data, and must protect that data itself from unauthorized access. Typically certain storage areas and other resources are assigned ownership to the user, and the user is given access to such other system resources as are required by the user's job or role, where the user performs multiple role. It is important to assign only the minimum accesses for each role in accordance with the

functional requirements of that role (principle of least privilege). In many cases, the notion of groups and access control lists is supported, which simplifies the assignments for large user populations.

g. Appliqué access control mechanism account establishment and access privilege entry.

As with operating systems, each generic appliqué access control mechanism includes with it a supporting facility to administer access authorizations for individual users (and in many cases, groups). Generally, before a user can gain access to the information objects recognized by the appliqué, a user account must be established on the underlying operating system platform. With some distributed appliqués, such as DCE, it is not necessary for the distributed user to have an identity or account on every server platform from which they receive services. In this case it is possible to manage the user accounts and privileges in a central way within the appliqué.

h. Application-specific access control mechanism account establishment and access privilege entry.

While it is possible for application-specific access control mechanisms to establish user identities and access authorizations independently of the underlying platform operating system, it is usually more successful to build on that underlying facility to simplify administration and utilize operating system identification and authentication mechanisms.

4.4 User I&A

Identification and authentication of users is the basis of applying access control and accountability to individual users. Identification is a nominal or an asserted identity by a claimant to a verifier. Authentication is the verification, based on additional evidence of the truth of the claimed identity. Strong I&A is a countermeasure to fraud and misuse based on impersonation of a user either to exploit the privileges of that user, avoid true accountability for actions, or both. While I&A is generally a built-in function of each of the access control mechanisms discussed in Section 4.2, the issue is complicated by the need to authenticate users operating remotely from the system that is ultimately controlling access. For the typical evaluated operating system, the evaluation is valid only for a local access configuration. For remote access supplemental I&A mechanisms should be considered.

i. None. No user I&A is applicable only when anonymous guest access is appropriate, e.g., to view public information or deposit anonymous suggestions/tips. In this special case, all users are treated equally, so no individual identity based access controls or accountability is required.

j. External. External I&A is applicable where access is controlled externally/physically and I&A is part of an external system, e.g. guards checking picture badges, possession of a key to a lock, etc.

k. Identifier & Fixed password. This is the basic method that is native to virtually all the generic access control mechanisms discussed in Section 4.2. It is by comparison of a shared secret in the verifying system's database with that given by the claimant that identity is authenticated. While almost universal, it is considered to be minimal, since it is based only on a single factor (something you know). Passwords can be easily compromised by being guessed, written down, or otherwise stored. Even with the best of password practices, (long, hard-to-guess, not written down, etc.), fixed passwords are highly vulnerable to being observed

(“sniffed”) in network traffic in remote access use, unless all network traffic is encrypted or otherwise protected.

l. Identifier & Dynamic password. By “dynamic password” we mean one that changes on each use, by some computation or lookup done by a remote user or user’s local software. The computation is based on a secret that both the claimant and verifier have, but it is not passed between them. This method is a strong countermeasure to the network observability of fixed passwords, but is still a single-factor (the shared secret) method.

m. [Identifier &] Biometric data. Still in relatively rare use, biometric technology for identifying and authenticating a user relies on a user-unique characteristic such as fingerprint, iris, voiceprint, etc. While apparently stronger than passwords, it is a single-factor method (something you are) that also suffers from reliability problems. The biggest weakness for biometrics alone is that for remote access, the biometric data is effectively a fixed password that can be observed on the network and played back to impersonate the user.

n. Shared secret-challenge response. This is a variation of dynamic passwords, where the verifier issues an unpredictable challenge, and the other computes and returns a function of the challenge based on a shared secret, such that the secret or future response cannot be computed from the challenges or responses.

o. User token device + shared secret. A user token device is a small (credit card size, key chain device, etc.) device that embeds the secret and the computation of a dynamic password or response to challenge in the device. When used along with another secret identifier (PIN) that is passed with the response to the verifying system, such a token can provide strong, two-factor (something you have and know) authentication.

p. User token device + digital signing. A token device that responds to a dynamic challenge with a digital signature (based on public key cryptography) can also provide strong two-factor authentication (provided the user must use a secret PIN to activate the token). It is considered better than the shared secret token, because no secret is shared.

q. Integrated with other cryptographic protections. Strong user I&A can be included or integral with other client-server cryptographic protection mechanisms. In Kerberos (standard Internet authentication protocol) and DCE, for example, identity of a remote client/user is established between the client and an authentication server by a form of the “identifier and dynamic password” method described above. The authentication server issues cryptographic “tickets” to the client used to authenticate the client to other servers. Some Kerberos and DCE products use provide for a supplemental token-based feature in the initial authentication. In message-based transaction applications, digital signatures of messages and signed receipts can strongly authenticate message origin and bind it to contents.

4.5 User Accountability

The purpose of user accountability is to ensure that individual users can be held accountable for access to information in systems or for specific transactions in those systems, and for attempts to exceed their permitted scope of activity.

r. None. No individual user accountability is applicable only when anonymous guest access is appropriate and intended, e.g., to view public information or deposit anonymous suggestions/tips.

s. External logging. When external I&A is applicable, accountability can only be for access at the level of access to an entire system. The minimum level accountability is the record of the initial grant of access. If more timely accountability is required (e.g., when a list of users use a sensitive system at different times), then such external mechanisms as signed usage logs can be kept.

t. Native platform/operating system audit trail mechanism. When access control is applied by an operating system that provides controlled access protection to sensitive or critical information, it should incorporate an audit trail mechanism that can log all individual user and information object access attempts and outcomes. All operating systems that are evaluated at the C2 or higher level (as described in Section 4.2) will have this capability.

u. Appliqué audit trail mechanism. When access control is applied by an appliqué system to sensitive or critical information, as described in Section 4.2, such a system should include an audit trail mechanism similar to that provided by a C2 operating system or better. All of the appliqué examples in Section 4.2 have such capabilities.

v. Application-specific accountability mechanisms. When access control is applied to application level objects by a trusted application to sensitive or critical information, the application should incorporate an audit trail mechanism similar to that provided by a C2 operating system or better.

4.6 Communication Security

The purpose of communication security mechanisms is to protect information communicated between systems against unauthorized origination, viewing/copying, modification, and deletion. Threats can come from passive eavesdropping (network sniffing) or active false origination, data modification and message or data deletion.

w. Physical Isolation. Where all communicating systems are within a physically secured facility (enclave), communications within the enclave may not have any specific communication countermeasures applied. This is based on an assumption of trust of all the systems in the enclave. If any of these systems becomes corrupted or misused, or if there is surreptitious external connectivity to the local network, then all communications and systems within the facility are vulnerable to attack via that connection.

x. Enclave-level network screening mechanisms (firewalls). When additional connectivity beyond the protected confines of the enclave is required, e.g., to traveling users or Internet services, then a boundary protection device or “firewall” is often employed to limit connectivity in and out to only the services/protocols/remote points that are desired. Because of the vulnerability of this arrangement to impersonation of allowed end-points, and to interception or modification of data outside the firewall, it is important for sensitive/critical data or services to employ countermeasures of strong I&A (of remote end-point system and/or user), and cryptographic services to protect the data on the external network. A number of firewall products

can provide these services, with a variety of strong I&A mechanisms as described in Section 4.4. For example, *SmartWall*, from V-One, is an application-level gateway that combines smartcard and encryption technology to create remote client token or software cryptographic I&A and firewall-to-firewall session encryption. The *CyberGuard Firewall*, from Cyber-Guard Corporation, provides filtering, token authentication, and encrypted virtual private network services on a B1-evaluated platform.

y. Data link level encryption & error detection mechanism between network nodes. Data link level encryption is where encryption is applied to physical point-to-point links or to virtual point-to-point data transfers over shared media networks (e.g., over an Ethernet LAN). This encryption is typically done only in hardware devices external to the end systems. This technique is effective against threats based on uncontrolled physical access to the transmission media, (e.g., outside a protected facility). Normal error-detection/correction protocol functions at higher layers will detect manipulation attempts at the encrypted data link layer. If none of the systems connected by link encryption has any connectivity outside the protected set, the situation is equivalent to a virtual equivalent of the physically isolated facility, even though the systems may be geographically remote. The residual vulnerability is, like that of a physically isolated set of connected systems, the data is exposed in all connected systems, including those that serve only to relay/route data and do not need to understand its contents. Data link level encryption also provides no end-to-end authentication. Other mechanisms must be employed to achieve end-to-end authentication, such as shared-secret-based authentication.

z. End-to-end encryption/error-detection between platforms. End-to-End encryption between platforms is where encryption is applied at the network protocol level, either by an end system's network software, or by a hardware unit external to the end system. End-to-end encryption between platforms provides an additional countermeasure the exposure of data to non-end-point systems on the network, and can provide end-to-end protection of integrity and authenticity. The residual vulnerabilities are within the two end-points of a protected connection.

aa. End-to-end encryption/error-detection between applications. End-to-end encryption between applications moves the encryption mechanism one level higher than between platforms - specifically to the communicating applications. This placement defends against some attacks against the communications within end platforms. This countermeasure is most important when end systems are multiple user systems and the internal access controls are weak. The disadvantage is that it places a burden of trust within the applications and on their designers. Whenever possible, it is best to avoid application-specific design of end-to-end encryption, and use instead a form of generic, end-to-end security services such as the General Security Service Application Programming Interface (GSS-API) provided by Kerberos and DCE products.

4.7 Network Entity I&A

The purpose of network entity identification and authentication is to ensure that communicating systems are transacting with accurately known remote end-points. Note that Internet Protocol (IP) Version 6 is a new network communications standard that supports authentication and other security mechanisms. For example, IP v.6 supports Community of Interest (COI) and authentication of peer network entities. Note also that the National Transportation Communications for ITS Protocol (NTCIP) is an evolving standard for transmitting data and

messages between electronic roadway devices used in ITS. Although the standard does not currently include user authentication mechanisms, it could be cost-beneficial to the ITS community to expand NTCIP to include these mechanisms. Indeed, adding an authentication mechanism to NTCIP would resolve most roadside device security concerns.

bb. None/Anonymous peer system. When no individual user accountability is applicable because the remote end system function is to support the client of some anonymous guest access, end point identification can be by assertion and serves no security function. Its only function is to support communications functionality.

cc. Non/Physical Isolation. Where all communicating systems are within a physically secured facility (enclave), communications within the enclave do not have any specific communication countermeasures applied (based on an assumption of trust of all the systems in the enclave). End point identification may be by simple assertion, with no authentication. If any of these systems becomes corrupted or misused, or if there is surreptitious external connectivity to the local network, then all communications and systems within the facility are vulnerable to attack via that connection.

dd. Shared secret exchanged in the clear. The principles and vulnerabilities of shared secret exchange for network entities is the same that of user fixed password authentication. Because such mechanisms are not part of standard communication protocols, they tend to be applied at the application level, and can be one-way or two-way. They are vulnerable to observation and re-use of the fixed shared secrets (“passwords”) by an attacker. When this method is used only to establish a connection, it does not bind subsequent data passed over the connection to the initial authentication. The data may still be fraudulently modified.

ee. Hidden shared secret-based exchanges. Hidden shared secret-based network authentication is similar to user identity/dynamic password and user identity/challenge-response user I&A mechanisms. One or both ends computes and sends some information that is a function of a shared secret (and other variables) to the other. Hidden shared secret-based exchanges are not vulnerable to observation as are shared secrets passed in the clear. Moreover, if the computed function of the shared secret is also a function of a block of data which it accompanies, it is strongly bound to the data, thus protecting it from both fraudulent origination or modification. This is the principle of the manipulation detection codes or message authentication codes used in such standards as ANSI X9.9, X9.19, FIPS PUB 113, and ISO 8730, 8731 - all based on using the FIPS PUB 46-2 Data Encryption Algorithm in conjunction with its key as the shared secret; and RFC 1828 which is based on keyed-use of the MD5 (RFC 1321) hash algorithm. Hidden shared secret exchange authentication provides strong authentication, but not non-repudiation of the origin of the data bound to the authenticating information.

ff. Digital signing of challenge/nonce. A digitally signed response to a random challenge or non-repeating nonce not only strongly authenticates the remote end point, but when bound to data, provides non-repudiation of origin. A digital signature based on a public key algorithm such as the Digital Signature Standard (FIPS 186) or the commercial de facto standard PKCS #1, based on the MD5 hash code and the RSA public key algorithm. These standards are typically applied at the application level, e.g., electronic messaging systems.

gg. Integrated with other cryptographic protections. Strong end point entity authentication may also be integrated with end-to-end encryption between applications, such electronic messaging systems (e.g., Privacy Enhanced Mail, Pretty Good Privacy, etc.) or as an integral part of generic appliqué services such as in Kerberos and DCE products.

5 Recommendations for the Implementation of Specific Security Countermeasures for Maryland ITS

5.1 Recommended Security Countermeasures for ITS Subsystems

In this section, the applicability to the Maryland ITS of the candidate countermeasure security mechanisms developed in Section 4 are discussed and general recommendations made. Outside the context of an actual system design, with all the specific constraints applicable at that time, these recommendations are intended only as general guidelines. Specific recommendations or selections would depend on such factors as the legacy applications and complete subsystems to be retained; MDOT funding availability; the impact on other systems sharing the same physical network or platforms; and security product availability and cost at the time a detailed design and implementation are performed.

Exhibit 5-1 indicates the potential applicability of each of the candidate mechanisms to each of the four Maryland ITS systems (center, remote access, roadside, and vehicle) and to other/external systems. A “Yes” entry indicates that a candidate is potentially applicable; a “No” entry indicates that it should not be used; and a blank indicates that the mechanism is logically inapplicable to that type of system (or in the case of external systems (“terminators”), outside the scope of this report). Because the Maryland systems do exchange data with the external systems, and critical data flows have been identified in those exchanges, it is appropriate to discuss the potential applicability of the candidate communication security mechanisms for those exchanges or interfaces. Each of the subsequent subsections discusses each system (column) in more detail.

Note that mitigation of many ITS security weaknesses can be accomplished by securing communications between devices and/or applications. This does not necessarily mean communication encryption, but it does mean that the communications be authenticated in some manner.

Some communications use a proprietary protocol—such as between a transponder and a receiver. Other communications comply with well-known standards such as TCP/IP. It is strongly recommended that only standards based communications be employed between ITS elements. Standards based communication protocols, such as the evolving IP version 6 (next generation IP), offer built in support for network security—which is a way of extending trust from the originator to the receiver at the system level. IP v.6 is valid for communication over LANs, WANs, and other sophisticated ITS networks. By way of contrast, the evolving NTCIP suite of ITS communication protocol standards currently lacks embedded communication authentication between controlling systems and remote ITS devices, e.g., VMS, toll transponder sensors, CVAS roadside components, and the like. This oversight must be corrected if adequate security is to be provided to these systems.

Exhibit 5-1. Specific Countermeasures for Maryland ITS

Type of Protection Requirement	Candidate Mechanism Types	Maryland ITS Systems				Other
		Center System	Remote Access System	Roadside System	Vehicle System	External System
1. Access Control	a. External physical/admin controls only	No	Yes	Yes	Yes	
	b. Platform-O/S access control mechanism.	Yes		Yes		
	c. Appliqué access control mechanism.	Yes		No		
	d. Appl-specific access control mechanism	Yes		Yes		
2. User Authorization	e. External physical/admin records only	No	Yes	Yes	Yes	
	f. Platform-operating system user account establishment and access privilege entry	Yes		Yes		
	g. Appliqué access control mechanism account establishment and access privilege entry	Yes		No		
	h. Application-specific access control mechanism account establishment and access privilege entry	Yes		Yes		
3. User I&A	i. None	No		No		
	j. External	No	Yes	Yes		
	k. Identifier & Fixed password	Yes		Yes		
	l. Identifier & Dynamic password	Yes		Yes	Yes	
	m. [Identifier &] Biometric data	Yes		No		
	n. Shared secret-challenge response	Yes		Yes		
	o. User token device + shared secret	Yes		No		
	p. User token device + digital signature	Yes		No		
q. Integrated with other crypto protections	Yes	Yes	No	Yes		
4. User Accountability	r. None	No		No		
	s. External logging (e.g., paper records)	No	Yes	Yes	Yes	
	t. Native platform O/S system audit trail	Yes		Yes		
	u. Appliqué audit trail mechanism	Yes		No		
	v. Appl-specific accountability mechanisms	Yes		Yes		
5. Comm Security	w. Physical isolation	No	No	No	No	
	x. Enclave-level net screening mechanism	No	No	No	No	No
	y. Data link level encr/error det, node-node	Yes	Yes	Yes	Yes	No
	z. End-to-end encr/error-detection bet pltfms	Yes	Yes	Yes	Yes	Yes
	aa. End-to-end encr/error-detection bet apps	Yes	Yes	Yes	Yes	Yes
6. Network Entity I&A	bb. None/Anonymous peer system	No	No	No	No	No
	cc. None/Physical isolation	No	No	No	No	No
	dd. Shared secret exchanged in the clear	Yes	Yes	Yes	Yes	Yes
	ee. Shared secret-based response	Yes	Yes	Yes	Yes	Yes
	ff. Digital signature of challenge/time/etc.	Yes	Yes	Yes	Yes	Yes
	gg. Integrated with other cryptographic protections	Yes	Yes	Yes	Yes	Yes

5.1.1 Center System

Center subsystems deal with those functions normally assigned to public/private administrative, management, or planning agencies. In Maryland these functions include traffic management, emissions management, transit management, toll administration, and commercial vehicle administration subsystems.

Traffic management includes everything from traffic light, freeway, and incident management to the management of roadside sensors that collect information on roadway conditions. The Maryland traffic management system is a composite of the State Highway Administration (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.

Emissions management collects and processes pollution data and provides demand management input to traffic management. These functions are performed by MdTA at their two tunnel locations.

Transit management collects operational data from transit vehicles and performs strategic and tactical planning for drivers and vehicles. The Mass Transit Administration (MTA) is responsible for this function. There are four MTA Operations Centers, one each for busses, Metro (subway), Light Rail, and MARC.

Toll administration provides general payment administration capabilities to support electronic assessment of tolls. This system falls within the purview of MdTA and includes responsibility for the maintenance and operation 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).

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 information requestors. These functions are performed in Maryland by the Commercial Vehicle Information Systems and Networks (CVISN) program within the Department of Motor Vehicles.

Access Control Mechanisms. All of the Center subsystems support multiple users and have requirements to segregate access to specific information resources based on the identity of a user who has specific accesses assigned on the basis of role. Hence, external physical access control is not sufficient. Operating system access controls in a controlled access (evaluated C2) system are adequate for those subsystems where all the resources or objects to be controlled correspond well with the native objects created and controlled by the operating system. For those subsystems that include critical information objects at the application level (not known to the operating system) then additional appliqué and/or application-specific control mechanisms should be considered.

User Authorization. User authorization mechanisms are a natural part of and correspond to the potentially applicable Center access control mechanism(s).

User I&A. For those Center subsystems that are connected to user only via dedicated links, or handle no critical functions or sensitive information, the standard user ID and fixed password I&A mechanism native to the operating system and/or appliqué and application controls is quite adequate. For Center subsystems where users can access the subsystem platform via shared networks or when the platform carries especially sensitive information or critical functions, then use of the stronger supplemental I&A mechanisms (l - q) should be considered.

User Accountability. Applicable user accountability auditing mechanisms correspond to the potentially applicable Center access control mechanism(s).

Communications Security. Center subsystems are required to communicate beyond the confines of a physically protected facility. As countermeasures to the vulnerabilities introduced by this exposure, additional mechanisms must be deployed to protect critical Center communications. While local-to-external network boundary screening mechanisms (firewalls, filtering routers) are highly recommended to minimize undesired traffic and help prevent and detect intrusion attempts originating outside the protected network, these mechanisms should be viewed more as a first line of defense than a full communications security measure. Additional cryptographic mechanisms are needed to protect the confidentiality and integrity of sensitive/critical information. The selection of the best cryptographic protection mechanism should be part of the overall architectural design that considers acquisition and operational costs, the application and protocol environment, interoperability issues, and other operational requirements.

Network Entity I&A. Center subsystems are required to accurately identify the remote end-point of communication. Hence one or more of the robust remote end-point I&A mechanisms (ee - gg) is required. Shared secrets exchanged in the clear (dd), while potentially usable, is generally not recommended, because of its vulnerability to various network eavesdropping or replay attacks.

5.1.2 Remote Access (Traveler) System

Remote access or traveler systems represent platforms for ITS functions of interest to travelers or commercial bus operators in support of multimodal traveling. These systems may be fixed (kiosks or home/office computers) or portable (a palm-top computer) and may be accessed by the public through kiosks or by individuals through cellular phones or personal computers. At the present time, only the MTA is deploying kiosks for traveler support.

Access Control Mechanisms. Remote access subsystems function as client applications to Center subsystems and do not contain multiple information objects whose access is to be protected and segregated from different users. These subsystems are required to be physically protected from theft and intrusion when located in public places (e.g., Kiosks). The public-access subsystems (e.g., at Kiosks) are dedicated to specific applications with strong application level controls to limit what functionality available to only a menu of public functions. (There should be no user access to the underlying operating system services.) On the other hand, a user issued a hand-held subsystems has physical position and control. Administrative control of issuance and

return, plus physical personal control of personal subsystems should be adequate. When laptops contain sensitive information and cannot be given continuous physical protection, additional protective mechanisms such as media encryption should be considered.

User Authorization. Public access remote subsystems require no user authorization; they are available to the traveling public. Authorization for personal, portable systems is administrative through their issuance process.

User I&A. While the servers in the Center system with which the Remote Access System communicates require I&A, the Remote Access system itself requires none. For issuance of portable systems, “I&A” is administrative only (identifying the employee checking out the device).

User Accountability. For public Remote Access subsystems, there is no accountability. For personal, portable systems, accountability is administrative.

Communications Security. Because sensitive and critical information is exchanged between the Remote Access system and Center system, cryptographic protection of communications is highly recommended. Data link encryption is not feasible because of the need for traversal of non Maryland ITS nodes. Hence, end-to-end platform or application level encryption mechanisms are recommended.

Network Entity I&A. Because sensitive and critical information is exchanged between Remote Access subsystems and Center subsystems, strong, remote end-point I&A is required. The recommendations reflect those of the Center system.

5.1.3 Roadside System

Roadside systems include functions that require convenient access to a roadside location for the deployment of sensors, signals, programmable signs, and other interfaces with travelers and vehicles of all types. Roadway subsystems provide traffic management surveillance, signals, and signage for traveler information. Toll collection subsystems interact with vehicle toll tags to collect tolls and identify violators. Parking management subsystems collect parking fees and manage parking lot occupancy/availability. Commercial vehicle check subsystems collect credential and safety data from vehicle tags, determines conformance to requirements, posts results to the driver, and records the results for the Commercial Vehicle Administration (Central) subsystem. All of these subsystems exist in Maryland.

Access Control Mechanisms. Some of the Roadside subsystems support multiple users and have requirements to segregate access to specific information resources or functionality based on the identity of a user who has specific accesses assigned on the basis of role. For those subsystems, external physical access control is not sufficient. Operating system access controls in a C2-type system are adequate for those subsystems where the resources or objects to be controlled correspond well with the native objects created and controlled by the operating system. For those subsystems that include critical information objects at the application level (not known to the operating system) then additional appliqué and/or application-specific control mechanisms should be considered. An example of an application that creates “information objects not known to the operating system” is a roadside toll-collection system that keeps and

manages toll collection accounts and sub-accounts with different financial operations permitted on those accounts by different operators, according to their assigned authority. The application design could carry all of this account information (a set of information objects) within a single file. The operating system would be unable to discriminate between the different detailed operations permitted to different operators, because it is concerned only with access to the overall container (the file).

User Authorization. User authorization mechanisms are a natural part of and correspond to the potentially applicable center access control mechanism(s).

User I&A. Some Roadside subsystems are connected to a user only via dedicated links, or handle no critical functions or sensitive information, and hence the standard user ID and fixed password I&A mechanism native to the operating system and/or appliqué and application controls is quite adequate. For remote access to maintain or reconfigure these subsystems, then the applicability of the stronger supplemental I&A control should be considered.

Roadside subsystems that handle critical functions and/or sensitive information (e.g., critical ITS roadway devices) will also need stronger supplemental I&A control. As noted in Section 4.4, it could be cost efficient to the ITS community to expand the NTCIP standard to include the needed security mechanisms.

User Accountability. Applicable user accountability auditing mechanisms correspond to the potentially applicable roadside access control mechanism(s).

Communications Security and Network Entity I&A. To combat fraud, strong communications security is required between Roadside subsystems and Vehicle subsystems, since wireless communications (e.g., short range RF/IR) are subject to interception and false signal generation. For Roadside/Vehicle communication we accordingly recommend use of any of the three potentially applicable cryptographic mechanisms (Exhibit 5-1, items y, z, and aa) depending on the overall system design context tradeoffs. The same mechanisms and their rationale are applicable to communications between the Roadside and Center subsystems—except that, as for Center subsystems, data link layer encryption (y) is not recommended for this application. When the communication path between a Roadside subsystem and a Central subsystem employs wireless communications (e.g., cellular telephony), it is exposed to interception and false origination. Current analog cellular systems have no built-in communications security, and security flaws are known to exist in current “secure” digital cellular standards. Even if built-in cryptographic protection for cellular systems becomes available, it can secure only the cellular hop portion of the total link. For this reason, cryptographic protection between a Roadside subsystem and a Central subsystem should be end-to-end (z or aa).

5.1.4 Vehicle System

Vehicle subsystems are installed in personal vehicles for the purposes of navigation, toll collection, and advanced vehicle control. They are also installed in transit vehicles to provide operational data, network status, and enroute traveler information; in commercial vehicles to store safety data, identification numbers, last check event data, and in-vehicle signage for driver pass/pull-in messages; and in emergency vehicles to provide vehicle and incident status.

In Maryland, only the transit vehicle subsystem is currently being implemented although commercial vehicle subsystems are expected to become available concurrent with the deployment of CVISN. The transit subsystems currently under consideration in Maryland (e.g., TRVS and automatic toll collection stickers) are embedded systems having no “user” functions, or need for internal access controls.

Access Control Mechanisms. Access controls required are physical, e.g., strong, tamperproof attachment to the vehicle.

User Authorization. Administrative.

User I&A. Administrative.

User Accountability. Administrative.

Communications Security and Network Entity I&A. To combat fraud, strong communications security is required between Vehicle subsystems and the Roadside subsystems, since wireless communications is subject to unauthorized monitoring and subsequent false signal generation. For subsystems like the TRVS, we recommend use of any of the three potentially applicable mechanisms (Exhibit 5-1, items y, z, and aa), as discussed for Roadside to Vehicle communication security. Similarly, for subsystems such as automatic toll collection stickers and/or transponders, we recommend use of any of the four potentially applicable mechanisms (dd, ee, ff, and gg) depending on the overall system design context tradeoffs.

5.2 Funded ITS Projects Mapped to Maryland Subsystems and Countermeasures

The Appendix contains a description of all known funded Maryland ITS projects including, in Exhibit A-1, a table mapping these projects to applicable ITS systems and subsystems. With this information, one can identify the ITS system types for each Maryland project and then, using Exhibit 5-1, identify the appropriate countermeasures for that project. By way of example, a Maryland project to “Upgrade Transit Information Center” is identified in Exhibit A-1 as both a Center system and Remote Access system project. Using Exhibit 5-1, the Center and Remote Access columns identify those countermeasures applicable to this Maryland project.

In the design and implementation of the project, each of the security countermeasures identified above should be considered for implementation. This consideration should be structured within the framework of a business risk analysis, i.e., what is the cost of providing this countermeasure versus the cost of the damage that might result from a failure to do so. As a final step in the design process, any security countermeasures designed into a project should be mapped against the data flows for that project to ensure that each and every critical data flow is in fact protected.

6 Barriers to Implementation

In discussions with MDOT security personnel concerns were expressed that the necessary funds and personnel would not be made available to implement the recommendations contained in this report. Certainly, security is expensive—but not nearly as expensive as the damage to State revenue sources and State reputation that would result from a failure to implement appropriate security measures. While it is beyond the scope of this study to identify specific implementation problems and costs, a description of a few of the barriers to implementation that were evident during discussions with MDOT personnel follow.

6.1 Policy

Although the security policies promulgated by the State Data Security Committee and MDOT cover most ITS needs, these policies need to be expanded to specifically address certain ITS security issues. Section 2.4 of this report describes those areas that require the issuance of additional policy guidance.

There is also concern that while a number of very good security policies have been promulgated, there exists only limited evidence of full compliance. During the course of CSC interviews, allusions were made to a lack of personnel and resources to examine even the limited audit data that is currently available. Additionally, it was stated that in certain locations multiple personnel use the same password and that some new personnel are placed in sensitive positions prior to the required criminal background check. Although the accuracy of these statements cannot be verified, there appears to be sufficient evidence to justify further investigation by those responsible for MDOT security.

6.2 Organizational

The MDOT security structure was undergoing reorganization as this Phase 2 Report was being prepared. While one can only speculate on what structure might result, security can only be assured if those responsible for security have the resources and authority to ensure that good security practices are implemented and practiced. It was for that reason that it was recommended in Section 2 that the Secretary of MDOT appoint an ITS Security Officer with the authority and resources to ensure compliance with established ITS security standards and to perform internal system audits.

6.3 Technical

The MVA Information Systems Center (ISC) recently had a Security Assessment Report prepared that specifically addressed the MVA/ISC backbone network. A number of recommendations were made for the protection of Financial Management Information Systems (FMIS) data, Motor Vehicle applications, and State Highway Contract and Payment accounting data contained in those systems.

Similar studies need to be performed as ITS becomes operational. ITS and the personal and financial data contained therein are equally sensitive and even more vulnerable because of their disbursed nature. While this Phase 2 Report identifies specific security requirements which must

be meet in support of ITS, it does not attempt to identify specific designs and costs to meet these requirements. This needs to be done prior to ITS becoming operational. Ideally, it should be done concurrent with project development and, as recommended in Section 2.4 of this Phase 2 Report, security should be a specific requirement and evaluation factor for any RFPs issued for ITS work.

6.4 Resources

In the end, effective ITS security is a function of the quality of personnel and sufficiency of funds made available to implement it. The telecommunications networks supporting ITS must be managed; systems to ensure availability, confidentiality, and integrity must be installed; auditing programs must be put in place; and qualified security personnel must be made available to review the information obtained. **Failure to do so is likely to result in significant tax, license, toll, and fare revenue losses to the state and, more importantly, a loss of MDOTs reputation as a leader in ITS implementation and management.**

In the implementation of ITS security, MDOT may not have to rely on its resources alone. There is considerable interest at the Federal level in the security of ITS and the possibility for joint, innovative approaches to ITS security would appear to exist.

7 Conclusions and Recommendations

In the conduct of this study of the security vulnerabilities of Maryland ITS systems, both Phases 1 and 2, a number of conclusions were reached as to the usefulness of data flow information from the national ITS physical model and the most effective approach to actually design countermeasures for ITS systems. Specifically, we found that:

- Data flow information from the national ITS physical model is useful in conceptualizing ITS system and subsystem relationships and is helpful in the development of broad security policies affecting ITS.
- The security policies developed as part of this study (Section 2.1) should be applicable to all state ITS.
- Critical data flows applicable to a particular state are useful in the development of specific ITS security requirements for that state based on a high-level business risk analysis of those flows.
- The mapping of critical data flows to specific ITS security requirements (Section 3) ensures that each and every critical data flow is protected by a required security mechanism.
- The candidate security countermeasures identified as part of this study (Section 4) are potentially applicable to all state ITS although the specific recommendations contained in Section 5 (Exhibit 5-1) must be tailored to individual state needs.
- The mapping of individual state ITS projects (Appendix) to specific ITS systems and subsystems combined with the use of Exhibit 5-1 provides a useful way to identify which countermeasures are applicable to specific ITS projects.
- In the design and implementation of a specific ITS project, each of the security countermeasures identified for that project should be considered for implementation. This consideration should be structured within the framework of (1) does it meet an identified security requirement and (2) what is the cost of providing this countermeasure versus the cost of the damage that might result from a failure to do so.
- As a final step in the design process, all security countermeasures designed into a project should be mapped against the data flows for that project to ensure that each and every critical data flow is in fact protected.

Complementing these conclusions, a number of recommendations have been made throughout this report. Specific additions to existent Maryland security policy were recommended in Section 2.4, Exhibit 2-3, and recommendations for security countermeasures applicable to Maryland ITS were made in Section 5.1, Exhibit 5-1.

While most of these recommendations addressed specific issues, there is one additional recommendation concerning communications protocols that deserves special note. Standards based communication protocols, such as the evolving IP version 6 (next generation IP), offer built-in support for authentication and other network security mechanisms recommended in this report. The new National Transportation Communications for ITS Protocol (NTCIP) is another evolving protocol for the transmission of data and messages between ITS devices that we hope will evolve to include embedded security mechanisms. We strongly recommend that MDOT

follow these developments closely because the use of new communications protocols such as those described would effectively solve many, but not all, of the identification and authentication issues discussed in this report.

Finally, we suggest that current and planned Maryland ITS projects be “tested” against the “strawman” security policies enumerated in Exhibit 2-1 and the candidate security countermeasures described for each ITS system category in Exhibit 5-1. This is a relatively simple step that can be accomplished by Maryland ITS project personnel with a small expenditure of time and money. In those cases where security policies or countermeasures are not met, corrective action is essential if Maryland revenue sources and citizen confidence in MDOT are to be maintained.

Appendix

MDOT ITS Projects and Studies

This appendix maps the National ITS Architecture model systems and subsystems to Maryland- and Federally-funded projects. Exhibit A-1 lists the results of the mapping sorted by project name. Column 4 includes the reference to a detailed description of the project. Exhibit A-2 presents the same information sorted by ITS system and subsystem.

Exhibit A-1. Mapping of Funded Maryland ITS Projects to National ITS Architecture Systems and Subsystems

Funded Project	System	Subsystem	Reference
Aerial Surveillance Program	Center	TMS	Exhibit A-8
Automatic Vehicle Identification (AVI)/Electronic Toll and Traffic Management (ETTM) System Study	Center	TMS	Exhibit A-11
Automatic Vehicle Location and Monitoring (AVL/M) System	Vehicle	TRVS	Exhibit A-4
Baltimore-Washington Parkway (National Park Service Segment) Detection	Roadside	RS	Exhibit A-8
Build and Consolidate Networks	Center	TMS	Exhibit A-10
Bus Priority Control System	Center	TMS	Exhibit A-11
CHART System Integration	Center	EMMS	Exhibit A-5
	Center	TMS	Exhibit A-5
	Roadside	RS	Exhibit A-5
Dynamic Travelers Alert Sign Deployment	Roadside	RS	Exhibit A-9
Commercial Vehicle Information Systems and Networks (CVISN) Program	Center	CVAS	Exhibit A-6
	Center	CVCS	Exhibit A-6
Computer Aided Dispatch/Automatic Vehicle Location (CAD/AVL) for CHART Vehicles	Center	TMS	Exhibit A-7
Electronic Toll Collection System	Central	TAS	Exhibit A-5
	Roadside	TCS	Exhibit A-5
Lane Control and Variable Speed System	Center	TMS	Exhibit A-11
Mobile Probe System Study	Center	TMS	Exhibit A-8
National Capital Region Traveler Information Showcase	Center	TMS	Exhibit A-9
Park & Ride Lot/Transit Integration Feasibility Study	Center	TMS	Exhibit A-11
Public and Employee Parking Improvements at Baltimore/Washington International Airport (BWI)	Roadside	PMS	Exhibit A-3
Ramp Metering System Study	Center	TMS	Exhibit A-11
Resource Sharing	Center	TMS	Exhibit A-10

Exhibit A-1. (Continued)

Funded Project	System	Subsystem	Reference
-----------------------	---------------	------------------	------------------

Funded Project	System	Subsystem	Reference
System Integration	Center	TMS	Exhibit A-10
Traffic Speed Monitoring	Roadside	RS	Exhibit A-8
Travelers Advisory Radio (TAR) Enhancements	Roadside	RS	Exhibit A-9
Travelers Advisory Telephone (TAT)	Roadside	RS	Exhibit A-9
Travelers Alert Sign Deployment	Roadside	RS	Exhibit A-9
Upgrade Transit Information Center	Center	TRMS	Exhibit A-4
	Remote Access	RTS	Exhibit A-4
Variable Message Sign Deployment	Roadside	RS	Exhibit A-9
Video Verification and Monitoring	Roadside	RS	Exhibit A-8
Wireless Media Study	Center	TMS	Exhibit A-10
Work Zone Surveillance and Monitoring Study	Center	TMS	Exhibit A-8
World Wide Web Interface	Center	TMS	Exhibit A-9

Exhibit A-2. Mapping of Maryland National ITS Architecture Systems and Subsystems To Funded Projects

System	Subsystem	Funded Project	Reference
Center	CVAS	Commercial Vehicle Information Systems and Networks (CVISN) Program	Exhibit A-6
Center	CVCS	Commercial Vehicle Information Systems and Networks (CVISN) Program	Exhibit A-6
Center	EMMS	CHART System Integration	Exhibit A-5
Center	TAS	Electronic Toll Collection System	Exhibit A-5
Center	TMS	CHART System Integration	Exhibit A-5
Center	TMS	Computer Aided Dispatch/Automatic Vehicle Location (CAD/AVL) for CHART Vehicles	Exhibit A-7
Center	TMS	Aerial Surveillance Program	Exhibit A-8
Center	TMS	Work Zone Surveillance and Monitoring Study	Exhibit A-8
Center	TMS	Mobile Probe System Study	Exhibit A-8
Center	TMS	World Wide Web Interface	Exhibit A-9
Center	TMS	National Capital Region Traveler Information Showcase	Exhibit A-9
Center	TMS	Build and Consolidate Networks	Exhibit A-10
Center	TMS	System Integration	Exhibit A-10

Exhibit A-2. (Continued)

System	Subsystem	Funded Project	Reference
Center	TMS	Wireless Media Study	Exhibit A-10

System	Subsystem	Funded Project	Reference
Center	TMS	Resource Sharing	Exhibit A-10
Center	TMS	Bus Priority Control System	Exhibit A-11
Center	TMS	Ramp Metering System Study	Exhibit A-11
Center	TMS	Automatic Vehicle Identification (AVI)/Electronic Toll and Traffic Management (ETTM) System Study	Exhibit A-11
Center	TMS	Lane Control and Variable Speed System	Exhibit A-11
Center	TMS	Park & Ride Lot/Transit Integration Feasibility Study	Exhibit A-11
Center	TRMS	Upgrade Transit Information Center	Exhibit A-4
Remote Access	RTS	Upgrade Transit Information Center	Exhibit A-4
Roadside	PMS	Public and Employee Parking Improvements at Baltimore/Washington International Airport (BWI)	Exhibit A-3
Roadside	RS	CHART System Integration	Exhibit A-5
Roadside	RS	Video Verification and Monitoring	Exhibit A-8
Roadside	RS	Traffic Speed Monitoring	Exhibit A-8
Roadside	RS	Baltimore-Washington Parkway (National Park Service Segment) Detection	Exhibit A-8
Roadside	RS	Variable Message Sign Deployment	Exhibit A-9
Roadside	RS	Dynamic Travelers Alert Sign Deployment	Exhibit A-9
Roadside	RS	Travelers Alert Sign Deployment	Exhibit A-9
Roadside	RS	Travelers Advisory Radio (TAR) Enhancements	Exhibit A-9
Roadside	RS	Travelers Advisory Telephone (TAT)	Exhibit A-9
Roadside	TCS	Electronic Toll Collection System	Exhibit A-5
Vehicle	TRVS	Automatic Vehicle Location and Monitoring (AVL/M) System	Exhibit A-4

Exhibits A-3 through A-11 summarize the projects for each applicable MDOT Modal. Excluding Exhibit A-6, the first column of the following exhibits (labeled either *CTP Reference* or *CBP Project Number*) references one of the following two documents:

- *Consolidated Transportation Program, 1997 State Report on Transportation, FY 1997-FY 2002*. MDOT, Annapolis, MD, 1997. (Referred to hereafter as “CTP.”)
- *Chesapeake Highway Advisories Routing Traffic, CHART Business Plan, Project Details*. MDOT, October 1, 1996. (Referred to hereafter as “CBP.”)

Exhibit A-6 describes a project that is funded by the US DOT and FHWA.

A.1 Maryland Aviation Administration (MAA)

Exhibit A-3. MAA ITS Projects

CTP Reference	Project Name	Description
Page 74	Public and Employee Parking Improvements at Baltimore/Washington International Airport (BWI)	<p>This project provides for a 1,000 space expansion of the public parking facility and the creation of a new 1,800 space public/satellite parking facility. The project is needed to handle the increase in passengers and employees as a result of the introduction of new and expanded airline service at BWI. The new public/employee parking lot adds 1,000 public spaces and consolidates the majority of the employee parking at BWI thereby allowing prior employee satellite parking to be converted to public parking. This project also contributes to the State's economic and business development.</p> <p>The MAA manages the parking lots at BWI. The Parking Management Subsystem (PMS) central computer is physically located in the Parking Administration Building at BWI and is operated and maintained by a contractor as an agent of the MAA. One other contractor staffs and operates the satellite parking facility, also an agent of the MAA.</p>

A.2 Mass Transit Administration (MTA)

Exhibit A-4. MTA ITS Projects

CTP Reference	Project Name	Description
Page 156	Automatic Vehicle Location and Monitoring (AVL/M)	<p>The AVL/M project entails the fleet wide installation of AVL/M equipment for bus and light rail. 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.</p> <p>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.</p> <p>The Vehicle Logic Unit (VLU) installed onboard the MTA vehicles corresponds to the National ITS Architecture Transit Vehicle Subsystem (TRVS) model.</p>
Page 157	Transit Information Center Upgrade	<p>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. Phase 3 is ongoing and will incorporate a trunked radio system supporting two-way cellular, UHF or VHF communications between the Operations Centers and the fleet vehicles. It will also integrate the Transit Watch Information Network (TWIN).</p> <p>The two-way radio system includes a microwave trunk and two receiver towers. The trunk infrastructure 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</p>

CTP Reference	Project Name	Description
	Transit Information Center Upgrade (continued)	<p>information to the public.</p> <p>As part of this project the MTA is also developing the architecture for Kiosks to be deployed in the near future. Initially, the MTA will be the only organization interfacing with the Kiosks. Other MDOT modals could be added in the future, but there is no definite plan to do so at this time.</p> <p>The functionality of the MTA Operations Centers maps to the National ITS Architecture Transit Management Subsystem (TRMS) model. In addition, the MTA Kiosk infrastructure and operations concepts map to the National ITS Architecture Remote Traveler Subsystem (RTS) model.</p>

A.3 Maryland Transportation Authority (MdTA)

Exhibit A-5. MdTA ITS Projects

CTP Reference	Project Name	Description
Page 492, Item 7	Electronic Toll Collection System	<p>A new, state-of-the-art electronic toll collection (ETC) system is 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 (TAS) 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 associated Toll Collection Subsystem (TCS) is and will continue to be operated by MdTA employees.</p>
Page 492, Item 8	CHART System Integration	<p>MdTA maintains and/or operates certain ITS highway capabilities along the I-95 corridor from Baltimore east to the Delaware border and at the Oriole's Camden Yards Stadium in central Baltimore. The ITS devices include traffic counters, cameras, and weather sensors, in addition to air quality sensors that are deployed in the Ft. McHenry and Harbor Tunnels. Many of these devices are part of the CHART network. Currently, the MdTA maintains two Traffic Control Centers (TCCs), one at each of the aforementioned tunnel locations. MdTA operations personnel use the same CHART workstations as their counterparts located in SHA facilities. Additionally, an I-95 Corridor Information Exchange Network (IEN) is maintained at the Ft. McHenry TCC.</p> <p>As part of this project, additional ITS devices will be deployed and the Ft. McHenry TCC will subsume the Harbor Tunnel TCC functions.</p> <p>The functionality of the MdTA map to the National ITS Architecture Traffic Management System (TMS). The ITS field devices including the air quality sensors in the tunnels map to the National ITS Architecture Roadway Subsystem (RS). A subset of the EMMS functions identified in the National ITS Architecture Emissions Management Subsystem (EMMS) model are performed locally at both MdTA TCCs. No Maryland organization performs all of the functions defined in the National ITS Architecture EMMS model.</p>

A.4 Motor Vehicle Administration (MVA)

Exhibit A-6. MVA ITS Projects

Reference	Project Name	Description
<p>Federally-funded by USDOT and FHWA</p>	<p>Commercial Vehicle Information Systems and Networks (CVISN) Program</p>	<p>CVISN is being developed 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.</p> <p>CVISN will deliver new electronic services in the areas of safety, credentials administration, and electronic screening. Examples of these services include:</p> <ul style="list-style-type: none"> • Timely safety information to inspectors at roadside, • Operating credentials to motor carriers electronically, • Exchange of registration and fuel tax information electronically, and • Electronic screening of commercial vehicles at fixed and mobile sites while vehicles are in motion. <p>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. Within Maryland, the Commercial Vehicle Administration Subsystem (CVAS) performs administrative functions supporting credentials, tax, and safety regulations while the Commercial Vehicle Check Subsystem (CVCS) operates at the roadside to enable credential checking and safety information collection. Today, the CVAS and CVCS consist of a number of individual systems and databases which reside in the Information Systems Center (ISC) of the MVA.</p>

A.5 State Highway Administration (SHA)

The CHART Capital program includes the implementation of specific projects (including studies) which will contribute to the progress and development of the five functional areas of CHART including: **Incident Management;** **Traffic and Roadway Monitoring;** **Traveler Information;** **Communications;** and **Traffic Management.** Exhibits A-7 through A-11 summarize the funded projects as described in the CBP. The information in the tables was extracted from the CBP. The third column, labeled “Priority,” includes values that range from P-1 to P-4, where P-1 is the highest and P-4 is the lowest priority.

Exhibit A-7. SHA CHART Incident Management Projects

CBP Project Number	Project Name	Priority	Description
2.1.2	Computer Aided Dispatch/Automatic Vehicle Location (CAD/AVL) for CHART Vehicles	P-1	<p>The development of an enhanced computerized emergency traffic patrol (ETP) and emergency response unit (ERU) dispatching system will provide the CHART incident management element with the ability to observe traffic and deploy incident equipment rapidly. A computer aided dispatch system coupled to automatic vehicle location will be considered for development to monitor the ETP and ERU fleet from the Statewide Operations Center or Traffic Operations Centers and will significantly reduce CHART unit response time. System compatibility with VDOT and Maryland State Police (MSP) units is essential given the interrelation with MSP on incident management and the fact that VDOT is deploying similar capability in northern Virginia.</p> <p>An on-board vehicle communications computer coupled to a global positioning system (GPS) and operator communication device provides direct, instantaneous dispatch and communication to/from the nearest CHART units. The system should provide instantaneous location reporting and a display of all AVL equipped vehicles to aid in the identification of the incident location and response.</p> <p>Initial deployment in FY 1998 will include 23 CHART vehicles and 12 designated Office of Maintenance (OOM) and Office of Traffic and Safety (OOTS) CHART support vehicles. This project will be coordinated with the systems integration project (2.4.2) to ensure compatibility between the GPS and Geographic Information System (GIS) interfaces. These units will prototype CAD/AVL for SHA and MDOT vehicles. CAD/AVL will significantly enhance the database of the CHART system by</p>

CBP Project Number	Project Name	Priority	Description
	CAD/AVL		<p>capturing exact time and location of units when incidents are detected and responded to.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS). It is funded for FY 1998.</p>

Exhibit A-8. SHA CHART Traffic and Roadway Monitoring Projects and Studies

CBP Project Number	Project Name	Priority	Description
2.2.1	Video Verification and Monitoring	P-1 and P-2	<p>Continue an ongoing moderate and conservative deployment of 62 video cameras at key traffic management locations over a 6-year time frame.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS). Funding is projected through FY 2002.</p>
2.2.2	Traffic Speed Monitoring	P-1 and P-2	<p>Install additional overhead radar-based speed monitors to compliment and backfill “gaps” in the existing metropolitan detection coverage area. Backfilling is defined as placing an additional 139 radar detectors at a 1-mile average spacing between detectors on congested freeways over a 6-year time frame</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS). Funding is projected through FY 2002.</p>
2.2.4	Baltimore-Washington Parkway (National Park Service Segment) Detection	P-1	<p>Place 13 traffic detection stations along the National Park Service-owned segment of the B-W parkway.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS) and is funded through FY 1998.</p>
2.2.5	Aerial Surveillance Program	P-3	<p>This project includes mounting a camera on a stabilized aerial platform (i.e., an airplane), and sending the video signal to the SOC via a combination of microwave radar and land line communications. This will allow CHART to investigate problems during incidents and major events. Technology issues to consider include 1) receiver antenna connectivity to the SOC; and 2) use of infrared observation cameras for nighttime applications.</p> <p>A study will be performed to consider the integration of CHART’s incident management needs with either Metro Traffic, Shadow Traffic or Montgomery County.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS). A study is funded for FY 1998, and deployment will occur in FY 1999. Funding is projected through FY2002.</p>

Exhibit A-8. (Continued)

2.2.6	Work Zone Surveillance and Monitoring Study	P-3	<p>Work zones present a unique problem to SHA's traffic management on the freeways and surface arterials. A significant amount of work is conducted during off-peak or nighttime hours, which is when the CHART traffic management systems are not at full function. Incidents in work zones have significant effects on traffic in the area and present a serious safety concern with respect to possible secondary accidents.</p> <p>This project involves conducting a study to address the need and alternatives for using ITS for surveying and monitoring construction and maintenance work zones. The study will address both safety within the work zone and construction project limits, as well as the benefits of surveying real-time traffic conditions at critical work zones.</p> <p>This system will interface and integrate with the incident management and traveler information systems.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected for FY 1999.</p>
2.2.7	Mobile Probe System Study	P-4	<p>This project includes a study of utilizing new technology which is mandated by the FCC to locate the source of cellular phone calls. This technology may be available within a 6-year time frame and can be used for traffic monitoring. If this technology can be leveraged for traffic monitoring, the result may be cost reductions due to the reduced need for infrastructure.</p> <p>Additionally, this project will include a study of the application of the Global Positioning System to determine the location, speed and progress of vehicles on the highway. Data obtained would better support a reliable automated traffic management system.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected for FY 1999 and FY 2000.</p>

Exhibit A-9. SHA CHART Traveler Information Projects

CBP Project Number	Project Name	Priority	Description
2.3.1	Variable Message Sign Deployment	P-1, P-2, and P-3	<p>This project will continue the deployment of VMSes which provide en-route traveler information that allows a motorist to make more informed decisions regarding mode or route choices. The goal is to install 38 VMSes at all primary-to-primary interchanges over a 6-year period.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS) and funding is projected through FY 2002.</p>
2.3.2	Dynamic Traveler Alert Sign Deployment	P-1	<p>Dynamic Traveler Alert Signs include a standard aluminum panel sign with flashing beacons to announce “urgent” TAR messages. These signs satisfy a similar informational need as VMSs, at a lower cost. An additional 29 signs will be deployed over the next three years.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS) and funding is projected through FY 1999.</p>
2.3.3	Traveler Alert Sign Deployment	P-1	<p>Traveler Alert Signs are aluminum panel signs, mounted on an existing VMS structure within a TAR broadcast area. This minimizes the deployment of additional devices while also enhancing the en-route traveler information system. An additional 16 signs will be installed over the next four years.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS) and funding is projected through FY 2002.</p>
2.3.4	Travelers Advisory Radio (TAR) Enhancements	P-1 and P-3	<p>Ten existing TAR portables will be retrofitted with solar power and cellular communications systems over the next 3 years.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS) and funding is projected through FY 1999.</p>
2.3.5	Travelers Advisory Telephone (TAT) TAT (continued)	P-1	<p>The Travelers Advisory Telephone (TAT) is a telephone informational system which provides regional reporting of real-time traffic conditions. This project will 1) replace the current Traffic Operations Center 5 (Chesapeake Bay Bridge- Eastern Shore Traffic Operations) system with a simple one-level (no menus) system; and 2) monitor the National Capital Region Traveler Information Showcase, which will use a multi-level TAT in the Washington, DC area over the next 3-year period. If the National Capital project is successful, expansion in the Baltimore area will be considered.</p> <p>This project maps to the National ITS Architecture Roadway Subsystem (RS) and funding is projected</p>

CBP Project Number	Project Name	Priority	Description
			through FY 1999.
2.3.6	World Wide Web Interface	P-1	<p>This project will provide static and dynamic traveler information on the Internet's World Wide Web. It will be implemented in three phases over the next four years. Phase I will display static information such as construction, special events, and major incidents. Phase II will implement semi-dynamic displays of information such as TraView maps, some camera images, and incident information. Phase III will include full dynamic display of information such as selectable TraView where the user can click on a link to get speed, accident details, or camera images.</p> <p>SHA will automate wherever possible to maximize effectiveness and needs to have a firewall to prevent outside access to SHA computers.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected through FY 2000.</p>
2.3.7	National Capital Region Traveler Information Showcase	P-1	<p>The National Capital Region Traveler Information Showcase is a large-scale, multi-jurisdictional and multi-disciplinary traveler information demonstration project. Public sector partners include: SHA, MTA, Prince George's County; FHWA, Washington Council of Governments, Washington DC Department of Public Works, Washington Metro Area Transit Authority, and other local transit agencies. Private sector partners include: prime contractor Batelle and team members SmartRoute Systems, Castle Rock Consultants, DeLeuw Cather, ETAK, Global Exchange, JHK & Associates, Scientex, Street Smarts, System Resources Corporation, and TRW.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and is funded for FY 2000.</p>

Exhibit A-10. SHA CHART Communications Projects

CBP Project Number	Project Name	Priority	Description
2.4.1	Build and Consolidate Networks	P-1	CHART is a statewide program covering over 540 miles of highway and therefore a statewide network is

CBP Project Number	Project Name	Priority	Description
			<p>needed to support CHART. The SHA is also one agency within MDOT, and state government as a whole, all of which have rapidly expanding requirements for communications infrastructure. Clearly, SHA's needs must be viewed in the broadest context to ensure that all opportunities are considered for providing taxpayers with the most effective total system.</p> <p>The SHA recently completed a landmark study where business requirements were defined and various networking options analyzed. The network was designed with the participation of the Department of General Service's Tele-communications Office (now under the Department of Budget and Fiscal Planning's Office of Information Technology.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected through at least FY 2002.</p>
2.4.2	System Integration	P-1	<p>The CHART system and communications infrastructure support functions such as incident management, traffic monitoring, traveler's information, emergency operations, etc. Over the next three years new functionality is required to make the system more effective and integrated with other areas.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected through FY 2002.</p>
2.4.3	Wireless Media Study	P-3	<p>Wireless may be an appropriate communications media for certain roadside locations. A study of the different technologies could prove to have significant benefits over wireline media. Specifically, technologies such as spread spectrum and microwave should be examined and field tested to determine if the technology can be employed for roadside communications. The conclusion will provide a cost analysis and recommendations for use in Maryland.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and is funded for FY 1998.</p>

Exhibit A-10. (Continued)

2.4.4	Resource Sharing	P-1	<p>Resource sharing refers to joint ventures between the State and private telecommunications firms where the State barter right-of-way access in exchange for bandwidth capacity and/or revenue. Resource sharing will reduce lease charges for network circuits.</p>
-------	------------------	-----	--

			This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected through at least FY 2002.
--	--	--	---

Exhibit A-11. SHA CHART Traffic Management Projects and Studies

CBP Project Number	Project Name	Priority	Description
2.5.1	Bus Priority Control System	P-2	<p>This system will provide transit busses with priority movement through signalized intersections to shorten travel times. The shorter travel times will encourage commuters to park their cars in favor of a bus service, thus reducing vehicular trips and congestion.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected through FY 2001.</p>
2.5.2	Ramp Metering System Study	P-3	<p>This is a study of ramp metering systems, which use traffic signals at the ends of on-ramps to “meter” the rate at which traffic enters the freeway.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and is funded for FY 1998.</p>
2.5.3	Automatic Vehicle Identification (AVI)/Electronic Toll and Traffic Management (ETTM) System Study	P-3	<p>This is a study to examine the feasibility of using electronic “tags” on vehicles to augment the detection system along freeways.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected for FY 1999.</p>
2.5.4	Lane Control and Variable Speed System	P-4	<p>This is a study of lane control systems and/or lane-specific speed limits along congested portions of freeways.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected for FY 1999.</p>
2.5.5	Park & Ride Lot/Transit Integration Feasibility Study	P-4	<p>This is a study of real-time information to both pre-trip and en-route motorists on the status of park & ride lots and transit lots and the status of arrival and departure of AMTRAK, MARC and light rail trains.</p> <p>This project maps to the National ITS Architecture Traffic Management Subsystem (TMS) and funding is projected for FY 1999.</p>

Acronym List

AUD	Audit
AVI	Automatic Vehicle Identification
AVL/M	Automatic Vehicle Location and Monitoring
BWI	Baltimore Washington International
CHART	Chesapeake Highway Advisories (for) Routing Traffic
CAD	Computer-Aided Dispatch
CIO	Chief Information Officer
COI	Community of Interest
COTS	Commercial off-the-shelf
CVAS	Commercial Vehicle Administration Subsystem
CVCS	Commercial Vehicle Check Subsystem
CVISN	Commercial Vehicle Information Systems and Networks
CVS	Commercial Vehicle Subsystem
DAC	Discretionary Access Control
DBMS	Database Management system
DCE	Distributed Computing Environment
EMMS	Emissions Management Subsystem
ETC	Electronic Toll Collection
ETP	Emergency Traffic Patrol
ETTM	Electronic Toll and Traffic Management
ERU	Emergency Response Unit
EVS	Emergency Vehicle Subsystem
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FMIS	Financial Management Information System
GIS	Geographic Information System
GPS	Global Positioning System
GSS-API	General Security Service Application Programming Interface
I & A	Identification and Authentication
IEN	Information Exchange Network
IP	Internet Protocol

ITS	Intelligent Transportation Systems
ISC	Information Systems Center
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
MSP	Maryland State Police
MTA	Mass Transit Administration
MVA	Motor Vehicle Administration
NTCIP	National Transportation Communications for ITS Protocol
OOM	Office of Maintenance
OOTs	Office of Traffic Safety
OR	Object Reuse
O/S	operating system
PCCIP	Presidential Commission on Critical Infrastructure Protection
PIN	Personal Identification Number
PMS	Parking Management Subsystem
RFP	Request for Proposal
RS	Roadway Subsystem
RTS	Remote Traveler Subsystem
SHA	State Highway Administration
SOC	Statewide Operations Center
TAR	Travelers Advisory Radio
TAS	Toll Administration Subsystem
TAT	Travelers Advisory Telephone
TCC	Traffic Control Center
TCS	Toll Collection Subsystem
TCSEC	Trusted Computer System Evaluation Criteria
TMS	Traffic Management Subsystem
TOC	Traffic Operations Center

TRMS	Transit Management Subsystem
TRVS	Transit Vehicle Subsystem
TWIN	Transit Watch Information Network
U1t	2-way wide-area wireless
U2	2-way short-range
US DOT	U.S. Department of Transportation
VDOT	Virginia Department of Transportation
VLU	Vehicle Logic Unit
VMS	variable message sign
VS	Vehicle Subsystem
W	Wireline
WAN	Wide Area Network
x21	Financial institution
x22	Government administrators
x29	Multimodal crossings
x33	Other TRM
x35	Other TM
x42	Secure area environment
x53	Transit maintenance personnel
x58	Weather service
x64	DMV
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, USDOT, Project Number 099618C4-0A, Contract Number DTFH61-95-C-00040. Washington, DC, May 1997.
2. Booz·Allen & Hamilton, *Authentication Analysis (DRAFT)*. Maryland Department of Transportation (MDOT), Information Systems Center, Glen Burnie, MD, June 20, 1997.
3. Booz·Allen & Hamilton, *Firewall Analysis*. MDOT, Information Systems Center, Glen Burnie, MD, October 1, 1996.
4. Booz·Allen & Hamilton, *Network Security Policy (DRAFT)*. MDOT, Information Systems Center, Glen Burnie, MD, February 19, 1997.
5. Booz·Allen and Hamilton, *State of Maryland Network Study*. State of Maryland, 1997. <http://www.dgs.state.md.us/~dgs/netstud.html>.
6. Booz-Allen & Hamilton, *Security Assessment Report*. MDOT, Motor Vehicle Administration, Glen Burnie, MD, July 11, 1996.
7. *Chesapeake Highway Advisories Routing Traffic, CHART Business Plan, Project Details*. MDOT, State Highway Administration, Glen Burnie, MD, October 1, 1996.
8. Computer Sciences Corporation, *Maryland State Highway Administration CHART Telecommunications Analysis Summary Report*. MDOT, State Highway Administration, Glen Burnie, MD, 1996.
9. *Consolidated Transportation Program, 1997 State Report on Transportation FY 1997-FY 2002*. MDOT, Annapolis, MD, 1997.
10. *FMIS Security Policy for Access to Third-Party Networks*. Department of Budget and Fiscal Planning, State of Maryland, Annapolis, MD, August 15, 1995.
11. *Internet Security and the FMIS Network*. Maryland Department of Budget & Fiscal Planning, Annapolis, MD, August 1995.
12. *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/>.
13. *Maryland Transportation Plan, Implementation Report*. Maryland Department of Transportation, Annapolis, MD, 1997.
14. *Standards and Procedures Manual, Administrative Volume, Security*. MDOT, Information Systems Center, Glen Burnie, MD, October 9, 1996.
15. *State Computerized Record System Security Requirements and Recommendations*. State of Maryland, State Data Security Committee, Annapolis, MD, July 12, 1996.

