Motor Vehicle Commission
Information Technology Management

July 1, 2004 to November 18, 2005
The Honorable Jon S. Corzine  
Governor of New Jersey  

The Honorable Richard J. Codey  
President of the Senate  

The Honorable Joseph J. Roberts, Jr.  
Speaker of the General Assembly  

Mr. Albert Porroni  
Executive Director  
Office of Legislative Services  

Enclosed is our report on the audit of the Motor Vehicle Commission, Information Technology for the period of July 1, 2004 to November 18, 2005. If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair  
State Auditor  
May 9, 2006
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>2</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Driver History Database</td>
<td>4</td>
</tr>
<tr>
<td>Network Security</td>
<td>6</td>
</tr>
<tr>
<td>Network and System Access</td>
<td>6</td>
</tr>
<tr>
<td>Network Monitoring and Maintenance</td>
<td>8</td>
</tr>
<tr>
<td>Network Services</td>
<td>8</td>
</tr>
<tr>
<td>Service Providers' Internal Control</td>
<td>9</td>
</tr>
<tr>
<td>Public Information</td>
<td>10</td>
</tr>
<tr>
<td>Change Management</td>
<td>10</td>
</tr>
<tr>
<td>Disaster Recovery and Business Continuity</td>
<td>10</td>
</tr>
<tr>
<td>Central Repository and Responsibility for Computer and IT Related Inventory Control</td>
<td>11</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>13</td>
</tr>
</tbody>
</table>
Motor Vehicle Commission
Information Technology Management

Scope

We have completed an audit of the Motor Vehicle Commission (MVC), Information Technology Management for the period July 1, 2004 to November 18, 2005. We assessed network vulnerability and reviewed the adequacy of selected information technology (IT) policies and procedures for the MVC, and for the portion of the commission’s network operated by the Department of Transportation (DOT). Our audit evaluated selected controls in place over the agency’s and department’s network and systems that process and protect both public and private information. They are as follows:

- Business continuity plans in the event of processing interruptions.
- Protection of computer resources from unauthorized access, use, and alteration.
- Implementation and documentation of the change control process.
- Physical and logical security in place to protect the IT infrastructure.
- IT strategic planning.

Objectives

The objectives of our audit were to determine the adequacy of controls over the computer network to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to ensure changes are properly implemented and documented, and to provide for adequate planning.

This audit was conducted pursuant to the State Auditor’s responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.
Methodology

Our audit was conducted in accordance with *Governmental Auditing Standards* issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the Open-Source Security Testing Methodology Manual provided by the Institute for Security and Open Methodologies, and benchmarks issued by the Center for Internet Security.

In preparation for our testing, we studied legislation, agency operation plans, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those requirements was verified by interview of key personnel, observation and access of network infrastructure, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

Conclusions

DOT and MVC management have recognized the importance of security over the commission’s network and the services it provides. We found controls in place and functioning to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to ensure changes are properly implemented and documented, and to provide for adequate planning. However, in making these determinations we identified several control weaknesses meriting management’s attention. We have also provided the DOT and the MVC with a management letter containing a more detailed discussion of network security specifics.

Overview

The Motor Vehicle Commission is responsible for the collection of motor vehicle fees, taxes, fines and surcharges. It is also responsible for driving licensing, auto related business licensing, vehicle titling and registration, vehicle safety and
emissions inspection functions, and maintenance of driving and vehicle history records.

The commission was created in 2003 as a result of the Motor Vehicle Security and Customer Service Act. This law, based on recommendations from the FixDMV Commission, created the Motor Vehicle Commission (MVC) and abolished the Division of Motor Vehicle Services. From 1994 until the law took effect, Motor Vehicle Services had been part of the Department of Transportation (DOT). The DOT is responsible, through a Service Level Agreement, for providing and securing the network infrastructure for MVC operations. The commission, however, is responsible for their own applications and their interface with the DOT infrastructure.

The Motor Vehicle Commission headquarters is located in Trenton. The commission operates 45 motor vehicle agencies, four regional service centers, three specialty sites, and the headquarters building. Each facility connects to the Garden State Network through a series of switches and routers. There are over 1600 logon ids that access the MVC network and more than 6500 logon ids that access MVC’s COMP system which contains driver history databases.

As part of the FixDMV Commission report dated November 7, 2002, the commission recommended that the DMV should issue a Request for Proposal for a Digitized Driver License application and undertake a complete overhaul of the COMP system. The report also identified services DMV could provide online, ultimately reducing the number of in-person visits to agencies. The Digital Driver License application started with a pilot project at the MVC headquarters, and gradually the application was rolled out to the remaining agencies. The COMP system is currently in the planning process of being rewritten to incorporate the recommendations of the FixDMV Commission. These projects have been the major initiatives MVC has undertaken over the last two years.
Driver History Database

The Motor Vehicle Commission has not performed an analysis of their driver history database. Database integrity is important as the information supports the validity of the state’s new secure digital drivers’ licenses.

We analyzed the MVC driver history database to determine the integrity of driver license data. As part of this analysis, we compared the driver history database with the Department of Health, Division of Vital Statistic’s deceased in-state and out-of-state resident files. We also reviewed what appear to be excessive issuances of duplicate licenses recorded in the database.

Results from our analyses revealed 15.5 million licenses recorded as issued since the system’s inception. Social Security Numbers (SSN) were reviewed and we found over 6 million licenses had SSNs that contained all zeros (000-00-0000) or all nines (999-99-9999), which are no longer accepted when applying for a license.

The 6 million licenses with SSNs containing all zeros and nines were analyzed for propriety and the following results were disclosed:

- 95 percent of the licenses have expired but are not designated as expired in the non-comm field.

- 220,500 of the licenses remain active.

The remaining 9.5 million driver’s licenses with SSNs that were not all zeroes or nines were analyzed for propriety and we found in the non-comm field that 2.9 million licenses have expired but are not designated as expired.

When we compared the driver history database with the Department of Health, Division of Vital Statistic’s deceased resident files we found
75,000 deceased persons listed as having a NJ driver’s license that have not been designated as deceased in the MVC driver history database. We also found 3,400 licenses of deceased persons recorded as issued after the deceased’s date of death, of which over 500 were designated as deceased in the driver history database, but were issued anyway.

The duplicate license field was also reviewed for propriety. Any person who was issued five or more duplicates and whose license has not expired was included. Our results disclosed that 11,600 individuals are recorded as receiving a duplicate license more than four times. The highest number of duplicates for a license that has not expired is 26.

**Recommendation**

We recommend that the MVC regularly analyze the database for propriety. Furthermore, we recommend the MVC:

- consider using the allowed value of “6” in the non-commercial status field, which indicates that the driver’s license has expired, for the 8.6 million licenses that are past the expiration date,

- investigate the 220,500 active licenses that have a SSN of all zeros or all nines to determine if the license issued is warranted,

- mark all licensees who have died as deceased,

- contact the Department of Health’s Bureau of Vital Statistics and obtain the deceased persons database for comparison with the driver history database on a scheduled basis,

- investigate all licenses issued after the date of death and forward those that
appear to be fraudulent to the Division of Criminal Justice,

- determine why over 500 licenses of deceased persons were issued even though the non-commercial and commercial fields in the database were valued as “1”, indicating that the licensee was deceased, and

- review those records with an excessive number of duplicates to determine if they are warranted; those that appear fraudulent should be forwarded to the Division of Criminal Justice for further action.

Network Security

Network security should be strengthened.

Comprehensive network security requires that all connections to the network be properly controlled. In addition, sufficient controls need to be in place to assure that network services are not compromised or disrupted. Our audit work revealed control weaknesses in these areas. We have provided management with technical details to allow them to address these issues.

Recommendation

We recommend the DOT and the MVC take the appropriate steps to improve network security.

Network and System Access

Network and System access should be more tightly controlled.

Control Objectives for Information and related Technology (CobiT) Delivery and Support objective 5.4, User Account Management, states: “Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of
user accounts.” Delivery and Support Objective 5.5, Management Review, states: “Management should have a control process in place to review and confirm access rights periodically.” The MVC and the DOT do have formal procedures for establishing, issuing, suspending, and closing user accounts, yet not all divisions within the Commission or department follow the procedures nor are user accounts reviewed jointly by the Network Operations unit and Human Resources.

Adequate control over a network requires proper administration of passwords and user accounts, compliance with accepted technical standards, and the granting of access privileges based on need.

*Network, Mainframe and Comprehensive System Access*

Our tests of all 14,373 logon ids for three network domains and four critical areas of the state’s mainframe revealed the following:

- 20 percent have not accessed network domains or the mainframe since 2004 or prior;
- 12 percent have never accessed network domains or the mainframe; and
- 10 percent have passwords that do not expire.

Our tests of all 13,083 users for the three network domains and four critical areas of the state’s mainframe revealed 16 percent have transferred or retired but still have access to MVC or DOT network domains and/or critical areas of the State’s mainframe. An additional 45 users are deceased. Furthermore, 162 users have two or more logon ids, with one user having 121 logon ids.
The DOT/MVC should strengthen controls over these areas, and we have provided management with the technical details on these matters.

**User Identification Naming Conventions**

The Department of Transportation's network operations unit does not use the names as shown on the Personnel Management Information System (PMIS) when adding users to NJDOT or MVC network domains.

**Recommendation**

Management should take steps to ensure network and system access is properly limited and controlled, and the network operations unit should utilize users' names as shown on PMIS to facilitate such control.

**Network Monitoring and Maintenance**

Strong network administration requires the recording and monitoring of activity to prevent unauthorized system access and usage, and the timely updating of network software to close security holes. We have provided management with the details pertaining to specific security weaknesses.

**Recommendation**

The DOT should take the necessary steps to strengthen network monitoring and maintenance.

**Network Services**

The MVC network has open services through logical connections between computers that are not necessary. Leaving these services open increases the risk of unauthorized access and network disruption. We have provided the MVC with the necessary technical details to correct this weakness.
Recommendation
Network administrators should turn off unnecessary services and regularly monitor the network to ensure none are improperly enabled in the future.

Service Providers’ Internal Control
The commission uses the services of two service provider organizations to process transactions from new car dealers. These providers rely heavily on computers and related equipment to process these transactions. Computer and IT related security controls in place at the service provider may not be adequate to protect data received, processed and transmitted. The commission should consider requiring a Statement on Auditing Standard (SAS) 70 review from these providers to determine that the computer controls and network security devices are in place and functioning to adequately protect the data. SAS 70 provides guidance for independent auditors who issue audit reports on the processing of transactions by a service organization and states that the service auditor must report on the operating effectiveness of the control procedures placed in operation.

Recommendation
We recommend the Motor Vehicle Commission request a copy of the service organizations’ most recent SAS 70 review to determine that the internal control structure as it relates to IT security is adequate. If such a review has not been performed, the commission should consider requiring one as part of the contracting process.
Public Information

Greater control should be exercised over public information.

Care must be taken in exposing information to the public that could pose a security risk. The DOT should strengthen policies and practices in this area, and we have provided them with specific areas of concern.

Recommendation

Management should establish policies regarding the exposure of information, and regularly monitor what is provided to the public.

Change Management

A formal change management policy should be implemented.

A strong system of internal control over hardware and software changes mandates that changes be documented in order to create an adequate audit trail and to guide future development. We noted that a policy has been developed but not implemented.

Recommendation

We recommend management implement the policy previously developed.

Disaster Recovery and Business Continuity

The Department of Transportation has not tested its disaster recovery plan.

The Department of Transportation is responsible for the Motor Vehicle Commission's network architecture. The commission is responsible for the collection of motor vehicle fees, taxes, fines, and surcharges. It is also responsible for driver licensing, auto related business licensing, vehicle titling and registration, vehicle safety and emissions inspection functions, and maintenance of driver and vehicle history records. The capability to process, store, and record these transactions and data is important to state operations. Therefore, procedures must be in
effect to safeguard information resources, minimize the risk of unplanned interruptions, and enable the recovery of critical operations in the event such interruptions occur. This comprehensive business continuity plan should address all potential disruptions to division operations.

We found the department’s business continuity and disaster recovery plan to be adequate, but the department has not tested the plan to determine its adequacy in the event of a disaster.

**Recommendation**

The DOT should test its disaster recovery plan for the commission’s network.

---

**Central Repository and Responsibility for Computer and IT Related Inventory Control**

Treasury Circular Letter 91-32-OMB requires the maintenance of a fixed asset inventory for all items with a value of $1,000 or greater and that the list be updated annually.

Our survey work and audit testing of computer and IT related inventory at the agencies noted that there is no central repository or responsibility for inventory control. Currently, there are four separate listings on Excel spreadsheets in various degrees of completeness prepared by four different units with no apparent coordination of effort. One of the units, the Inventory Control Unit within the DOT Warehouse Operations, maintained the most accurate listing with respect to MVC asset tag number information. One of the inventories lists all computer equipment but no associated asset tag number, user, or location information. Failure to maintain accurate records increases the risk of assets being stolen or lost without detection.
**Recommendation**

We recommend that inventory control and recordkeeping be the responsibility of one unit, with one inventory record that is regularly tested.
May 5, 2006

Mr. Richard L. Fair
State Auditor
Office of State Auditor
P.O. Box 067
Trenton, New Jersey 08625-067

Re: OLS Audit-Motor Vehicle Commission Information Technology

Dear Mr. Fair:

The Department of Transportation (DOT) and the Motor Vehicle Commission (MVC) appreciates the staff in the thorough audit performed of the Motor Vehicle Commission-Information Technology Management for the period of July 1, 2004 to November 18 2005. Since this audit addresses issues currently shared by both MVC and DOT the responses are addressed accordingly:

**OLS Recommendations:**

**Driver History Database**

**OLS Recommendation:** MVC should consider using a value of “6” to indicate in the non-commercial status field that the driver’s license has expired.

**MVC Response:** Currently the expiration date is the key field for processing a transaction. Drivers are given up to three years to renew their license. After the three years has expired, the driver is required to be retested. Upon recommendation of the OLS audit, we will develop a system change request that will monitor expiration dates and then add the new status code “6” to the field. Given guidance from the Division of Archives and Records Management, we may be able to take off-line the records and store those that have expired for a period greater than ten years. All records containing certain moving violations must be kept on file.

**OLS Recommendation:** Investigate the 220,500 active licenses that have a SSN of all zeros or all nines to determine if a license should be issued.

**MVC Response:** We have recently initiated a project that prevents the issuance of a DDL unless the SSN is correct. MVC has also organized a task force of a cross-section of the Commission to address all SSN issues. They are developing a management report with

*On the Road to Excellence
www.njmvc.gov
New Jersey is an Equal Opportunity Employer*
recommendations to modify the business process with regards to SSN verification, while maintaining customer service. MVC, today, verifies the correct SSN via an on-line connection with the Social Security Administration. The SSA system is called the Social Security On-Line Verification (SOLV) and it connects from MVC to SSA through AAMVAnet. The 220K drivers with an invalid SSN will be corrected through this system at the time of their renewal. Please note the SSN has only been a requirement for Commercial Drivers since 1991. All basic drivers were not required to provide a SSN until recently. This accounts for the numerous records that have zeros or nines in the SSN field. MVC will review and take appropriate action on the 220,500 licenses mentioned when it receives the detailed records from OLS.

**OLS Recommendation:** Mark all licensees who have died as deceased. Contact the Department of Health’s Bureau of Vital Statistics to obtain the deceased persons database for comparison. And investigate all licenses issued after the date of death.

**MVC Response:** MVC has been updating our database with deceased records from BOVS since 2004. To implement this project, MVC determined that it would be prudent to post deceased records from the year 2000 to correspond with our renewal cycle. However, BOVS can provide MVC with deceased records going back to the time that they began to computerize their records (1993). If required, we can request a run of their entire database to match all MVC records. Note there is no legal requirement for citizens to notify MVC when someone in their family dies. Also, the BOVS does not require that the paperwork submitted to them by the County Surrogates/Funeral Directors have a Driver License Number included, nor do they have this field in their database. The best we can do at this point is to match the deceased record by SSN and date of birth. Updating the MVC database will be more accurate in the future, when all drivers have a valid SSN on record.

**OLS Recommendation:** Investigate all licenses issued after the date of death and forward those that appear to be fraudulent to the Division of Criminal Justice. Also, determine why over 500 licenses of deceased persons were issued even though the non-commercial status field was valued as “1” deceased.

**MVC Response:** The agency system is currently programmed to prevent the issuance of any type of license if the status field has a value of “1” deceased. The list of 500 drivers that may have been issued a license after the date of death as posted in the status field should be provided to the IT Systems Development Unit and to the Security and Investigation Unit. Each of the above cases will be reviewed on a case by case basis after the Commission receives the detailed records. All cases that appear to be fraudulent will be turned over from the MVC Security and Investigation Unit to the Division of Criminal Justice.

**OLS Recommendation:** Investigate drivers who have obtained an excessive number of duplicate licenses.

**MVC Response:** At this time there is no legal requirement that would prevent a driver from obtaining any number of duplicate licenses. However, MVC has recently added a field to count the number of duplicates that a driver obtains. As part of the SSN project this field would identify the driver as a “high risk” driver. This means that the driver record would be reviewed before the issuance of a renewal document. This process will be fully implemented when the SSN project is totally implemented. MVC has initiated a large development project to
completely replace and retire its current mainframe legacy COMP and Agency Systems. The new application, MATRX, will make use of leading edge Rules Engines and other technology to look for this and other similar activity that may warrant detailed review and possible submission to the Division of Criminal Justice.

**Network Security**

**OLS Recommendation:** DOT and MVC should take appropriate steps to improve network security.

**MVC Response:** The next three categories address the identified Network Security issues.

**Network and System Access**

**OLS Recommendation:** Management should take steps to ensure network and system access is properly limited and controlled, and the network operations unit should utilize users’ names as shown on PMIS to facilitate such control.

**MVC Response:** MVC has a procedure to control ACF2 IDs and access to mainframe systems. This procedure was implemented in coordination with our Human Resources Unit when the HR unit was formed at MVC. As employees are severed or change units and job functions, the Personnel Coordinators of each unit are to complete a Computer Use Authorization form and/or a System Authorization form and forward to IT. The procedure will be reviewed by both IT and HR to ensure that it is being followed and regular reviews will be conducted.

Prior to this procedure being implemented, MVC’s Human Resource functions were the responsibility of Shared Services and prior to that, DOT. It was towards the end of their servicing MVC that these procedures were not followed and information on severed or transferred employees was not relayed to IT to change or remove accesses. These need to be addressed by MVC IT and MVC Human Resources.

**DOT Response:** In order to address the disconnect that often occurs between units regarding the termination of an employee and the disabling of that account, DOT Network Administration will be working with MVC’s Human Resource area to have an electronic email sent upon the termination of an employee so that the accounts can be disabled. Further, the DOT Network Administration staff has recently acquired a software package that allows for the collection and generation of reports associated with user accounts, software revision levels and a myriad of other functions. The DOT has been aggressively addressing both server and workstation irregularities that have surfaced in these reports and will continue to do “due diligence” in addressing the problems cited in the report. However, this will take some time due to the lack of staffing in the Network area.

Naming conventions, in general, consistently follow what is listed on an employee’s PMIS file. There are several exceptions where a user is specifically known by a name other than his/her “given name” and we have attempted to accommodate those requests on a limited basis.
Network Monitoring and Maintenance

**OLS Recommendation:** The DOT should take the necessary steps to strengthen network monitoring and maintenance.

**DOT Response:** The DOT has configured and deployed WSUS servers to address the automatic updating of security patches to both DOT and MVC servers.

Network Services

**OLS Recommendation:** Network Administrators should turn off unnecessary services and regularly monitor the network to ensure none are improperly enabled in the future.

**DOT Response:** When the NJDOT Network Administration staff initially setup the MVC networks at both the HQ and agency locations, ports not in use were “turned off” at the switch. However, due to lack of staffing at both MVC and NJDOT, the time required to contact a Network Admin, have them go in and open up the requested port and then have the MVC Help Desk person test connectivity resulted in a significant drain on the time required by an MVC Help Desk person to address the installation and setup of new equipment. Further, if a Help Desk person was physically at an agency and required that a port be opened, he/she would have to wait until they could reach someone in the DOT Data Comm. unit to address this issue. Again, the drain on staff time became a factor in the decision to leave ports open thereby providing the MVC Help Desk personnel with more flexibility.

**MVC Response:** There is a recommendation to transition the Network IT services from DOT to MVC-IT. If this recommendation for the creation and staffing of MVC’s Information Technology Infrastructure Support Unit is approved, it will absorb this function and will be able to better maintain security while addressing functional needs.

Service Providers Internal Control

**OLS Recommendation:** OLS recommends the Motor Vehicle Commission request a copy of the service organizations’ most recent SAS 70 review to determine that the internal control structure as it relates to IT security is adequate. If such a review has not been performed the commission should consider requiring one as part of the contracting process.

**MVC Response:** MVC Internal Audit and OIT Audit Unit have both recently completed audits of MVC’s two service provider organizations. The State Auditors may have a copy of these reports if deemed necessary.

MVC is also in the process of updating and signing a new Memorandum of Understanding (MOU) between the State and these two service providers, TriVin and CVR. At this time MVC will include language that will require a Statement of Auditing Standard (SAS) 70 review be completed by these vendors on a periodic basis.

Public Information

**OLS Recommendation:** Management should establish policies regarding the exposure of information, and regularly monitor what is provided to the public.
**MVC Response:** MVC, with the assistance of an outside vendor and OIT, is undertaking a major overhaul of its Internet Presence and its content. They are reviewing what information should be made public and what information should be maintained privately for security reasons. MVC is also revamping and writing new policies for almost all aspects of its business since its creation and removal from the Department of Transportation. These will include and address security, information, IT requests, IT account management and maintenance, and other critical aspects of the Commission’s Mission and Goals.

MVC has a multi-level review before placing anything on its external website. The IT staff along with OIT develops information and applications, internal Legal and Communication Offices review for any legal issues and other concerns. This is done before anything is posted to the site.

**Change Management**

**OLS Recommendation:** Management should implement the policy previously developed (but not implemented).

**MVC Response:** MVC’s production systems software and hardware are maintained by OIT at their two Data Center’s. Changes to the Comprehensive (mainframe), and the Agency (server) software systems follow OIT’s change control methodology. MVC IT is pursuing the same software module for its internal change and problem management solution. Training, implementation, and policies will then be deployed to provide complete internal control and an audit trail for all systems.

**Disaster Recovery and Business Continuity**

**OLS Recommendation:** The DOT should test its disaster recovery plan for the Commission’s network.

**DOT Response:** DOT, in conjunction with OIT WAN Operations, is currently installing redundant circuits in each of the MVC agencies in order to minimize the agency’s exposure. At present, the agency servers house no information. They serve as a pass through and are used primarily for logon verification. When a server has gone down, DOT Network Admin staff has directed the traffic to other servers that also house the login information. These redundant servers are located throughout the state, therefore, if any server is lost, traffic can be redirected (and has been), through one of the other servers. Once the redundant circuits have been installed, tests will be scheduled with agency personnel to verify that rerouting of agency traffic is being performed. This will provide the agencies with the redundancy necessary to ensure continuous operations utilizing the network components supported by DOT.

**Central Repository & Responsibility for Computer and IT Related Inventory Control**

**OLS Recommendation:** OLS recommends that inventory control and recordkeeping be the responsibility of one unit, with one inventory record that is regularly tested.
**MVC Response:** MVC is currently researching a consolidated Inventory Control solution. In the meantime, we’ve collaborated with all parties who maintain these individual inventories to store these in one logical place until a final solution is implemented and an Infrastructure Support Unit is approved for MVC to support this.

The recent OIT IT Assessment has also identified that an enterprise inventory solution could benefit many agencies and MVC would like to be considered as part of this project.

Respectfully submitted,

[Signature]

Sharon A. Harrington
Chief Administrator

C: Kris Kolluri, Commissioner, DOT