A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
Boston, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2007-0511-4T

OFFICE OF THE STATE AUDITOR'S REPORT
ON INFORMATION TECHNOLOGY CONTROLS AT
THE REGISTRY OF MOTOR VEHICLES

July 1, 2005 through February 21, 2008

OFFICIAL AUDIT
REPORT
JULY 9, 2008

TABLE OF CONTENTS

INTRODUCTION 1

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY 4

AUDIT CONCLUSION 12

AUDIT RESULTS 17

1. **Criminal Traffic Citations** 17
   a. **Processing of Adjudications** 17
   b. **Driver's License Suspensions and Revocations** 18
2. **RMV Assessment of Motor Vehicle Excise Tax Billings** 22
3. **Criminal Offender Record Information Background Checks** 26
4. **Disaster Recovery and Business Continuity Planning** 29
5. **Inventory Controls Over Computer Equipment** 33

APPENDIX – AUDITEE'S RESPONSE TO AUDIT CONCLUSIONS 38

INTRODUCTION

The Registry of Motor Vehicles (RMV) was created by Chapter 16, Section 9, of the Massachusetts General Laws (MGL) and established within the Executive Office of Public Safety by MGL Chapter 6A, Section 18. Chapter 291, Section 20, of the Acts and Resolves of 2004 amended MGL Chapter 6A, Section 18, and relocated the RMV from the Executive Office of Public Safety to the Executive Office of Transportation. The Secretary of Transportation and Public Works for the Commonwealth of Massachusetts directs the Executive Office of Transportation (EOT). The Secretary has direct oversight over the Massachusetts Highway Department, Registry of Motor Vehicles, and the Massachusetts Aeronautics Commission, and serves as the Chair of the MBTA Board of Directors. The Registrar directs strategic planning for the RMV and sets operational priorities for its approximately 950 employees located in its central office at Newport Avenue in Quincy and the 35 branch and satellite offices throughout the State. The RMV is supported by a budget of approximately $53 million for fiscal year 2008. As of October 2007, there were approximately 4 million Massachusetts licensed drivers.

The RMV's mission is to enable Massachusetts' citizenry to travel roads safely by licensing drivers, assisting in maintaining driver histories, and providing registrations and titles for safe and environmentally sound vehicles. To achieve this goal, the RMV issues and maintains records related to motor vehicle registrations and operators' licenses; enforces motor vehicle laws to promote highway safety by ensuring that every driver meets minimum competency standards and withdrawing driving privileges from individuals who prove to be a threat to other drivers. The RMV is also responsible for collecting fees for registrations, titles, drivers' licenses, special plates, Civil Motor Vehicle Infractions (CMVIs), inspection stickers, and other miscellaneous fees, and remitting them to the Office of the State Treasurer. Chapter 90 of the General Laws provides the statutory guidelines governing the RMV and Code of Massachusetts Regulations 540 C.M.R. provides regulatory responsibilities for RMV.

The RMV's mission-critical automated system, which is called the Automated Licensing and Registration System (ALARS), was developed in the mid 1980's as the RMV's mainframe/database for all registry transactions. ALARS is used to maintain all records for Massachusetts licensed drivers, including licenses, registrations, criminal and civil citations, inspection stickers, and various miscellaneous fees. The RMV information technology (IT) infrastructure used to support ALARS and other administrative applications consists of local area networks (LANs) installed at the central office as well as the branch and satellite offices linking over 900 workstations within a network providing access to print and file servers. The ALARS application is hosted within the Executive Office of Transportation's (EOT) data

center located in Chelsea with connectivity to local area network (LAN) operations that are transmitted from RMV's central office in Quincy. The RMV offices are able to access ALARS data files and software directly through the wide area network (WAN) to the EOT's file servers containing the ALARS database. Through the WAN, the workstations also provide access to the state's Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

The EOT IT Department currently maintains, supports and operates the RMV's systems, networks and data bases on in-house and off-site computer platforms and also provides accounts for web mail users. The IT Department is headed by a Chief Information Officer (CIO) who is responsible for applications, operations, purchasing, computer-aided design and drafting (CADD), and the Uninsured Motorist System (UMS). The EOT IT Department consists of two distinct groups. The Applications group has four primary functions - project management/business analysis, application design and development, application support, and quality assurance and testing. The Operations group has five areas of responsibility including helpdesk/desktop, data center/server, network infrastructure, telecommunications, and security & administration.

The RMV provides the Merit Rating Board (MRB) with access to ALARS, which is a state agency that administers the Safe Driver Insurance Plan and is the central repository for all criminal and civil motor vehicle violation citations issued within the Commonwealth of Massachusetts. The two agencies are interdependent and use the same IT data infrastructure.

Under Chapter 60A of the General Laws, all Massachusetts residents who own and register a motor vehicle must annually pay a motor vehicle excise tax. The formula used for the assessment is based upon the requirements of Massachusetts General Law, Chapter 60A, Section 1. Excise tax bills are prepared by the RMV according to the information on the motor vehicle registration. In order to produce excise tax bills, vehicles are valued by obtaining the Manufacturer Suggested Retail Price (MSRP). The National Automobile Dealers Association Used Car Guide (NADA) is the primary valuation tool used and is available as an on-line reference within the RMV's ALARS application. The NADA is used in an automated fashion to value most cars, light trucks and motorcycles based on each vehicle's unique vehicle identification number. The MSRP is then entered in the RMV database as part of each vehicle's record. The excise tax bills are generated and then sent to city or town assessors who submit them to the local tax collectors for distribution and collection of payment. The excise tax revenues become part of the local community treasury.

Our examination focused on a review of selected internal controls over ALARS, physical security and environmental protection controls over IT resources at the RMV's production site and administrative offices, system access security, business continuity planning, and on-site and off-site storage of computer-related media. In association with our review of access security we also performed a review regarding the adequacy of controls in place to protect the integrity and confidentiality of personally identifiable information contained in the ALARS database. We performed a review of the controls over the protection of personal identifiable information on RMV documents and during payment card transactions. In addition, we performed an assessment of controls in place by the RMV to ensure that current and accurate driving records were available and that licensees who abused their driving privileges received the required suspension or revocation period in a timely manner and were not inappropriately reinstated. We also performed an assessment regarding the effectiveness of the RMV's efforts to calculate, prepare, and distribute excise bills to city and town assessors for collection.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Registry of Motor Vehicles for the period of July 1, 2005 through February 21, 2008. The audit was conducted from May 2, 2007 through February 21, 2008. Our audit scope included a general control examination of internal controls related to the organization and management of IT activities and operations; physical security and environmental protection over the RMV's IT infrastructure, system access security, inventory controls over IT equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media. We also performed a review regarding the adequacy of controls in place to protect the integrity and confidentiality of personally identifiable information contained in the ALARS database and payment card transactions in connection with our evaluation of system access security. In addition, we also performed a review of the RMV's control practices regarding the Criminal Offender Record Information (CORI) background checks required prior to an individual's employment as well as annually for all current RMV personnel**.**

Our audit scope also focused on the RMV's process for suspending, revoking and reinstating drivers' licenses. Consequently, we performed an assessment of controls in place by the RMV to ensure that current and accurate driving records were available via ALARS and that licensees who abused their driving privileges received the required suspension or revocation period in a timely manner and were not inappropriately reinstated. We also performed an assessment regarding the effectiveness of the RMV's efforts to calculate, prepare, and distribute motor vehicle excise bills to city and town assessors for collection.

Audit Objectives

Our primary audit objective was to determine whether the RMV's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives were in place and in effect to support the RMV's business functions. In this regard, we sought to determine whether adequate controls were in place and in effect to provide reasonable assurance those IT resources would be safeguarded, properly accounted for, and available when required.

Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether the RMV had implemented IT strategic and tactical plans to assist the RMV in fulfilling its mission, goals, and objectives and whether the RMV and EOT had appointed a steering committee to oversee its IT Department and activities.

We sought to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the data center, central and sections of the selected branch offices, and the on-site and off-site media storage areas was limited to authorized personnel. Moreover, we sought to determine whether sufficient environmental protection was being provided to the same areas noted above that would prevent or detect damage or loss of IT-related equipment and media.

Our objective regarding system access security was to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to RMV's application systems and data files. We evaluated whether procedures were in place to prevent and detect unauthorized user access to automated systems and IT resources, including the ALARS application, through the local area network (LAN) file servers and microcomputer workstations. In addition, we determined whether the RMV had documented controls in place for the ALARS system to sufficiently protect against unauthorized disclosure of information, including personally identifiable information. We also reviewed RMV controls regarding data modification or deletion and whether RMV was actively monitoring user account activity and password administration. In addition, we determined that status of the RMV's compliance with Payment Card Industry (PCI) Data Security Standards (DSS) and associated milestones.

With regard to inventory control over IT equipment, including notebook computers, we evaluated whether an annual physical inventory and reconciliation was conducted and whether IT equipment was accurately reflected, accounted for, and properly maintained in the system of record.

Regarding systems availability, we sought to determine whether adequate business continuity plans were in place to help ensure that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render processing inoperable or inaccessible. Moreover, we sought to determine whether adequate controls were in place to provide reasonable assurance that appropriate magnetic backup copies of application systems and data files would be available on-site and off-site to support disaster recovery and business continuity planning objectives.

We also sought to determine whether selected state laws, regulations, and control practices regarding the completion of CORI background checks and that the submission of supporting documents was performed by RMV prior to an individual's employment, changes in position, and annually for all RMV employees.

We performed an assessment of enforcement actions via ALARS, specifically criminal uniform citations, to evaluate the timeliness of the RMV's process for suspending and revoking driving licenses within the authority granted to the Registry. We sought to determine whether licensees' driving records were timely and accurately updated by the RMV for applicable adjudicated convictions received from the Courts as well as the effectiveness of the RMV's process for reinstating drivers' licenses.

In addition, we sought to determine whether the RMV has adequate controls in place to accurately calculate the value of each motor vehicle excise tax amount. We examined the RMV's records and internal control and evaluated its compliance with applicable State laws, rules, and regulations.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of the RMV's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of the RMV's organization and operations, we gained an understanding of the primary business functions supported by the automated systems. We documented the significant functions and activities supported by the technology and reviewed automated functions related to operations designated as mission-critical by the Registry.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure and reporting lines of the EOT's IT Department. We obtained, reviewed, and analyzed relevant IT-related policies and procedures and strategic and tactical plans to determine their adequacy. To determine whether the RMV's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technological expertise requirements, we obtained a current list of the personnel employed by the RMV, including their duties and job descriptions, and compared the list to the IT Department's organizational chart, each employee's statements concerning their day-to-day IT-related responsibilities, and the technology in use at the time. We inspected the data center in Chelsea and the central office in Boston, reviewed relevant documents, such as the network configuration, internal control plan, and business continuity plan, and performed selected preliminary audit tests.

We interviewed RMV management to discuss internal controls regarding physical security and environmental protection over and within the data center housing the file servers, the business offices where workstations are located, and the on-site and off-site storage areas for mission-critical and essential magnetic media storage. In conjunction with our audit, we reviewed written, authorized, and approved policies and procedures for control areas under review. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with regulations and to meet accepted control objectives for IT operations and security.

To determine whether physical access over computer equipment was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft, or damage, we performed audit tests at the central offices and the data center. To determine whether adequate controls were in effect to prevent or detect unauthorized access to the selected business offices housing IT resources, we inspected physical access controls, such as the presence of security personnel on duty, locked entrance and exit doors, the presence of a receptionist at the entrance point, intrusion alarms, and whether sign-in/sign-out logs were required for visitors. We reviewed physical access control procedures, such as the lists of staff authorized to access the data center and magnetic key management regarding door locks to the central office's entrance and other restricted areas within the central office. We determined whether the RMV maintained incident report logs to record and identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of computer-related equipment.

To determine whether adequate environmental protection controls at the central offices and data center were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), uninterruptible power supply (UPS) and surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the data center or in the vicinity of computer-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in business offices and the data center that houses the file servers. Moreover, we reviewed control procedures to prevent and detect water damage to automated systems, agency records, and magnetic backup media stored on site.

With respect to system access security, our audit included a review of access privileges of those RMV employees authorized to access the network and associated personal computer systems. To determine whether the RMV's control practices regarding system access security would prevent unauthorized access

to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with senior management responsible for the network and evaluated selected controls to the automated systems. In connection with our review of security practices, we reviewed RMV's supporting documentation and interviewed senior management to determine the status of RMV's ability to meet compliance with Payment Card Industry (PCI) standards and RMV's control mechanisms to protect personally identifiable information (PII) in ALARS. The payment card industry ranks merchants based upon the number of transactions processed and the RMV is a level 2 merchant. To store, process or transmit cardholder data that comply with its Cardholder Information Security Program (CISP). One aspect of this program is that merchants must adhere to the Payment Card Industry Data Security Standard. The data security standard is a 12 point list of security requirements and includes a comprehensive checklist (Payment Card Industry Self-Assessment Questionnaire), which can be used by merchants to evaluate controls over the protection of personal payment card information. We also reviewed policy and guidance issued by the Commonwealth's Information Technology Division through Chapter 93H of the Massachusetts General Laws regarding the protection of sensitive agency information and reviewed RMV's policies and procedures to safeguard PII.

To determine whether the administration of logon ID and passwords was being properly enforced, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the analyst responsible for access to the file servers and workstations on which the RMV's application systems operate. In addition, we reviewed control practices used to assign and grant staff access privileges to the application programs and data files. To determine whether controls in place were adequate to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application systems and related data files. We reviewed documents related to the granting of authorization to access automated systems and requested and received a current listing of third-party users. To determine whether RMV users with active privileges were current employees, we obtained the list of individuals with access privileges to the network and microcomputer workstations and compared all users with active access privileges to the RMV's personnel roster of current employees. Furthermore, we determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly account for the RMV's IT resources, we reviewed inventory control policies and procedures and requested and obtained the RMV's inventory system of record for computer equipment dated May 2, 2007. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the

value, location, and condition of IT-related fixed assets. We also performed a data analysis on the inventory and made note of any distribution characteristics, duplicate records, unusual data elements, and missing values. To determine whether the system of record for computer equipment was current, accurate, complete, and valid, we used Audit Command Language (ACL) to select a statistical sample of 187 items out of a total population of 2,138 items for our test. We traced the inventory tags, location, description and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand.

To verify the relevance and completeness of the RMV's system of record for IT related equipment, we judgmentally selected 112 additional computer hardware items in various locations and determined whether they were properly recorded on the RMV's inventory record. To determine whether selected computer hardware purchases for fiscal years 2006 and 2007 were accurately listed, we randomly selected 336 items, valued at $121,350, and verified whether the amounts recorded on RMV's purchase orders and invoices were accurately recorded on the inventory system of record. To determine whether the RMV had appropriate control practices in place and in effect to account for and safeguard notebook computers, we interviewed representatives from the IT Department. Furthermore, we reviewed the control form regarding their notebook computer equipment loan policies for employees, and requested for review the RMV's documented policies and procedures to control the assignment and use of notebook computers.

To determine whether the RMV complied with Commonwealth of Massachusetts regulations for accounting for assets, we reviewed evidence supporting the RMV's performance of an annual physical inventory and reconciliation of IT assets. Furthermore, to determine whether the RMV complied with Commonwealth of Massachusetts regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT-related equipment disposed of during the audit period, as well as IT-related equipment that the RMV plans to request Commonwealth approval to dispose of as surplus. Finally, to determine whether the RMV was in compliance with Chapter 647 of the Acts of 1989, regarding reporting requirements for missing or stolen assets, we reviewed incident reports for missing or stolen IT-related equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers and workstations be unavailable for an extended period. We interviewed senior management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan

was in place and had been periodically reviewed. Furthermore, we reviewed and evaluated procedures in place to resume normal business functions should the file servers or the personal computer workstations be rendered inoperable or inaccessible.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed RMV management responsible for generating backup copies of magnetic media for administrative work processed at the RMV and the mission-critical application Automated Licenses and Registration System (ALARS) residing on the mainframe. We reviewed the adequacy of provisions for on-site backup copies of mission-critical and essential magnetic media at the data center. We did not review the Information Technology Division's backup procedures for transactions processed through MMARS and HR/CMS.

We also sought to determine whether selected laws, regulations, and control practices regarding the completion of CORI background checks and the submission of supporting documents were performed prior to an individual's employment, changes in position or acceptance into a position at the RMV.

Regarding our assessment of enforcement actions, i.e. suspensions and revocations, performedby the RMV via ALARS we interviewed RMV, Administrative Office of the Trial Courts, and MRB personnel, observed processes and procedures, examined system configurations, transactions and records, reviewed appropriate technical literature and computer generated reports, and performed various other procedures as deemed necessary in the circumstances. Our audit included examinations of various criminal transactions (as well as events and conditions) occurring during the period July 2004 through June 2006. To determine whether the RMV personnel were effectively managing criminal suspensions via ALARS, we requested and received data from the Merit Rating Board (MRB) regarding the new criminal citation activity for fiscal year 2005 and fiscal year 2006. We then requested and received from the MRB an aging summary for all of the 245,634 criminal uniform citation dispositions mailed to the RMV from the Courts for calendar years 2005 and 2006. Our analysis revealed that the Courts did not submit dispositions for over 21,114 (9%) criminal uniform citations to the RMV within thirty days of adjudication. We then selected the 11,015 and 10,099 citations from calendar years 2005 and 2006, respectively, and selected a statistical sample of 205 criminal traffic citations for testing from the population of 21,114. We reviewed each citation sample to assess the RMV process for effectiveness and compliance with laws, rules, policies, and procedures of the RMV and the Courts. To gain a further understanding of the suspension process, we spoke with individuals in the Driver Control Unit. We then compared citation data to data input into ALARS and conducted analyses of the criminal citations where

the court determined the offenders' licenses were to be suspended, including the time period between the date of adjudication to the date the MRB received the information.

To determine whether adequate controls were in place and in effect to properly collect and account for the RMV's excise tax collections, we reviewed laws regarding excise tax collection, requested and obtained the RMV's Excise Tax Recovery Initiative, dated May 22, 2007. The Excise Tax Recovery Initiative was a document describing the RMV's evaluation of ALARS that concluded some vehicles had either no value or were undervalued resulting in no or undervalued excise tax computations. We also reviewed and analyzed RMV documentation explaining the excise tax process and an excise tax value discussion as well as the excise tax totals for years 2003 through 2006. We reviewed the requested documentation and met with the consultant who completed the aforementioned papers and was responsible for the excise tax program at the RMV. We reviewed the process of how the RMV uses National Automobile Dealers Association (NADA) then examined the vehicles from model year 2006, and the RMV's estimates of their corrected valuation and how much additional revenue could generated.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at the Registry of Motor Vehicles (RMV), we found that adequate controls were in place to provide reasonable assurance that information technology (IT) related control objectives would be met with respect to IT organization and management, physical security, environmental protection, and on-site and off-site storage of backup copies of magnetic media. We found that controls needed to be strengthened to provide reasonable assurance that control objectives regarding business continuity planning and inventory control over IT equipment will be met. Although adequate controls were in place to provide reasonable assurance that only authorized users could access RMV systems, users needed to be more timely deactivated from the system when no longer employed by the Registry. We also found that RMV needed to establish sufficient assurance mechanisms for the security of Personally Identifiable Information (PII), including the monitoring and encryption of ALARS data transmitted to third-party users. The RMV and the Administrative Office of the Trial Court need to address excessive delays in the integrity of record keeping for criminal traffic citations to ensure that driver's license suspensions and revocations are processed timely. The Registry needs to further improve the process of assessing excise taxes to ensure consistency and accuracy with the method of calculating motor vehicle excise taxes. We also found that the RMV needed to improve its effectiveness for monitoring and evaluating the Criminal Offender Record Information (CORI) background checks performed prior to, and during, an individual's employment at the RMV.

Our review of IT-related organizational and management controls indicated that the RMV had a defined IT organizational structure, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for IT staff that reflected current responsibilities. Our review of IT-related planning found that the RMV, in conjunction with the Executive Office of Transportation's (EOT) IT Department, had developed comprehensive strategic and tactical plans to address IT functions within the Registry and across the 35 branch and satellite offices. With respect to documented policies and procedures and the use and the safeguarding of information technology, we determined that formal policies and procedures were in place; however, the RMV needed to strengthen business continuity and contingency planning. The absence of sufficiently documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced.

Our examination of physical security revealed that controls provided reasonable assurance that the RMV's IT resources were safeguarded from unauthorized access for the data center, central office, and selected branch offices. We found that the data center was locked and that a list was maintained of individuals who had key access to the facility. The RMV's data center had full-time security guards on

duty 24 hours per day, seven days per week, and the facility was equipped with intrusion alarms. Our examination also disclosed that the data center had restricted keycard access to only approved individuals. In addition, visitors are escorted when accessing the data center to minimize the risk of damage and/or theft of computer equipment. Our review of areas housing workstations in the central office and selected branch locations disclosed that on-site security make periodic rounds nightly to verify that all office doors are locked and secure.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply, were in place in the building housing the RMV to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We found that an uninterruptible power system (UPS) was in place to prevent sudden loss of data and that hand-held fire extinguishers were located within the data center. Moreover, evacuation and emergency procedures were documented and posted within the data center, and that staff, according to management, had recently been trained in the use of these emergency procedures.

Regarding system access security, our audit revealed that the RMV had developed and documented appropriate procedures regarding the granting of access privileges for RMV employees to automated systems and activation of logon IDs and passwords. Regarding procedures to deactivate RMV employee access privileges, we found that formal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. However, ALARS user accounts were found to be active for individuals no longer employed by the RMV. Our audit tests revealed that 27 of the 911 active RMV ALARS users were no longer associated with the RMV. It should be noted that for the entire 27 user accounts that were still active past their respective separation date, there was no evidence that any of these accounts had been used after the individual's departure from the RMV. However, the failure to deactivate user accounts in a timely manner places the RMV at risk of unauthorized use of established privileges, such as using another individual's user account having higher access privileges, or to unauthorized access. For example, areas of significant impact would include the handling of ALARS transactions that involve the exchange of cash and the suspension/revocation of licenses.

Our review determined that the RMV appeared to be nearing completion of their action plan to help ensure Payment Card Industry (PCI) Data Security Standards (DSS) compliance for proactively protecting customer credit card account data that is either stored, processed, or transmitted. The RMV action plan incorporated the PCI DSS into a data security standard that has a 12 point list of security

requirements and includes a comprehensive checklist (Payment Card Industry Self-Assessment Questionnaire), which can be used by level 2 merchants such as the RMV to evaluate controls over the protection of personal payment card information. We believe that the PCI DSS action plan should be updated whenever an application or database involved in the processing of payment card information is upgraded or replaced. In this way, the items in the action plan are re-evaluated and that RMV periodically reviews the security of sensitive information.

Our review determined that drivers' personally identifiable information (PII) appeared to be properly secured in the ALARS database; however, when transmitted or stored outside of ALARS, the data may be exposed to potential unauthorized access or unapproved use. We found that the RMV had not established sufficient mechanisms to provide adequate assurance that third-party controls were in place to protect this data. We recognize the position of the RMV that the Registry must make public certain information under the Massachusetts Freedom of Information Act, and this is accomplished by providing a batch tape of the bulk information. Local newspapers and private companies purchase the bulk data and in some cases resell the data. The RMV also provides on-line access to a network of entities including insurance companies, car dealerships, and local constables. However, these third-party network transmissions were not encrypted and personally identifiable information has been transmitted in clear text. If intercepted during transmission, drivers' personally identifiable information could potentially be subjected to unauthorized access and unapproved use. In addition, the RMV did not have adequate assurance that third parties exercised appropriate controls over the PII provided by the registry.

We believe that the previously agreed level of access granted to external organizations and the information provided by the RMV, including PII, may not make sense in a post 9/11 world, and current procedures could be enhanced to reflect new security requirements such as Chapter 93H of the Massachusetts General Laws. We recommend that the RMV establish a new interconnection security agreement and memorandum of understanding with third-party users to document security requirements, identify authorities, and specify responsibilities of both organizations, such as the encryption of the data and the security assurance required to meet minimum security standards. We also recommend that the RMV enhance procedures for controlling downloads of PII to remote systems. For example, the RMV should establish monitoring and evaluation procedures to ensure that RMV places restrictions on the type of information that could be downloaded to remote computers.

Our audit indicated that adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media. We determined that the RMV had implemented procedures and schedules for generating backup copies of magnetic media and had documented procedures for

maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which backup tapes were stored off-site, and logs were maintained demonstrating the authorized schedule for the transport and return of backup copies.

Although on-site and off-site storage of backup media was in place, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. Specifically, our audit disclosed that the RMV did not have a comprehensive disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for ALARS could be regained effectively and in a timely manner should a disaster render automated systems inoperable. Although there was an updated Continuity of Operations Plan (COOP) from January 31, 2007 and a potential alternate processing site had been selected, user area plans for functional areas and branch offices had not been established to document the procedures required to regain business operations in the event of a disaster.

Our audit also disclosed that RMV did not effectively monitor the timeliness of the judicial process for criminal violations and did not attempt to address significant delays by the Courts regarding traffic citation dispositions to the RMV. As a result, driver histories were incomplete and the RMV cannot ensure that problem drivers are promptly identified and held responsible for the consequences of their actions. Our test results revealed that the Courts did not submit dispositions for over 21,000 criminal uniform citations to the RMV within thirty days of adjudication. Also, the RMV did not always timely notify licensees of suspensions or revocations; therefore, licensees could improperly retain their licenses. In some instances, habitual traffic offenders were reinstated due to ineffective control features within ALARS and timing and communication problems with the Courts.

Our audit revealed that the RMV failed to make timely and accurate excise tax billing computations that resulted in over $1.3 million of uncollected excise tax revenues for the Commonwealth's cities and towns that could have been used to fund important local services. In addition, we determined that the RMV did not have a process in place to accurately record all vehicle values including luxury cars, trucks, buses, and motor homes, used to generate excise tax billings We determined that the RMV, over the course of several years, assigned well below market valuations for thousands of vehicles that resulted in undervalued excise tax computations to local cities and towns. These undervalued vehicles included luxury vehicles (Ferrari, Lamborghini, Bentley, Jaguar, e.g.); large trucks and buses; trailers; and specialized vehicles constructed on a chassis, such as ambulances and auto homes.

Our audit revealed that that Criminal Offender Record Information (CORI) background checks were not being performed as required by the RMV's policies and procedures. We determined that the RMV's CORI policy requires that …"a Massachusetts criminal record check shall be performed on all current and prospective personnel. Current personnel will be subject to an annual criminal record check. Prospective personnel will be subject to a criminal record check as part of the pre-employment evaluation process." However, based on our audit testing, we concluded that CORI checks were not performed on a consistent basis for current or prospective personnel. We also determined that individuals hired before 1996 fell into the category of not being required to have a CORI background check performed at the time of hiring. We also determined that those individuals hired before the law took effect were "grandfathered" in and were not required to have annual CORI background checks performed.

Our audit revealed that RMV could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon, since an annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. We found that 84 IT purchases made during fiscal year 2007 were not included in the inventory system of record, and our data analysis of the entire population of 2,138 IT hardware items indicated that there were missing fields of information with respect to value, asset tag number, location, and description. Our test of 112 hardware items, traced from multiple physical locations back to the inventory listing, indicated that 12 of the selected items were not on the inventory list. Also, our inventory test of 111 items taken from the inventory list and traced back to their actual location indicated that 100 of the selected pieces of computer equipment could be located. Furthermore, an inventory test of 75 notebook computers indicated that five of the notebook computers could not be found.

Regarding surplus property and equipment, our audit revealed that the RMV was aware of, and in compliance with, Operational Services Division's policy and procedures regarding surplus computer equipment. In addition, we found that the RMV's internal control policies included control and reporting requirements set forth in Chapter 647 of the Acts of 1989.

AUDIT RESULTS

1. Criminal Traffic Citations

a. Processing of Adjudications

Our audit determined that there was a significant delay between the date of the Court's guilty adjudications of criminal citations and the date the RMV receives the adjudication and takes action to suspend or revoke drivers' licenses. Although once received from the Courts, adjudications are forwarded by the RMV to the Merit Rating Board (MRB) for data entry to the ALARS, and subsequent actions are taken by RMV within their established time frames, there are no procedures in place on the part of the Registry and the Courts to determine whether all adjudications are received and processed by RMV in a timely manner.

At the time of our audit, there were no procedures in place to reconcile the dates that criminal traffic or motor vehicle violations are adjudicated by the Judiciary, received by the RMV and entered manually by the MRB into the Registry's automated system, and when licenses are revoked or suspended and notifications are mailed by the RMV to inform offenders of the actions taken. In addition, although both the Registry and the Courts were aware that there are often significant delays before the RMV receives the adjudications, there are no control procedures in place at the Registry to identify, age and report to the Courts on the status of the receipt of adjudications. As a result, in addition to the possibility of delays in updating licensees' driving records and in not having appropriate actions taken, such as revoking driving privileges, the RMV cannot verify that all of the criminal citations related to traffic or motor vehicle violations adjudicated by Courts are actually placed on drivers' records. Under these circumstances, state agencies and others who may use ALARS may not always obtain a current and accurate record of a licensee's driving history, which could adversely affect public safety. Moreover, given the sheer volume of criminal citations, tickets could be lost or removed at any time during the process without detection.

Based on all new criminal citations for 2005 and 2006, we determined that effective suspension and revocation dates for thousands of criminal citations were on average, one to four years after the Court's adjudication. Although RMV senior management advised us that they were aware of the Court's delays and had discussed this issue with senior management at the Administrative Office of the Trial Court (AOTC), the RMV did not believe they had the authority or responsibility to address the delays. While the delays are primarily the result of the timeliness of notification of the Court's decisions, we believe that the RMV, as the entity responsible for the safety of citizenry on the roads of the Commonwealth, has an obligation to monitor the timeliness of submissions of judicial adjudications and to work in conjunction with the management of the Judiciary to address this issue. At the very least, the RMV should have been

closely tracking the receipt of adjudications and providing the AOTC with documentation on the extent of delays and source of mailings to help ensure that adequate management attention would be afforded to the problem. We also believe that because the RMV had never performed an aging of submissions of adjudicated criminal citations, the RMV was not fully aware of the actual extent of the delays.

Our audit determined that the Courts did not always submit criminal traffic citation dispositions to the RMV in a timely manner. As a result, not all driver histories are complete and the RMV cannot ensure that problem drivers are promptly identified and held responsible for the consequences of their actions. We requested and received from the MRB an aging summary for the 245,634 criminal uniform citation dispositions mailed to the RMV for calendar years 2005 and 2006. Our analysis revealed that 11,015 and 10,099 criminal uniform citations from calendar years 2005 and 2006, respectively, were not submitted by the Judiciary to the RMV within thirty days of adjudication. We performed an aging analysis of the total 21,114 of these criminal uniform citations further revealing that 4,313 of the adjudications had not been submitted to the RMV from a period of one to 17 years after the Court's disposition with 70% being submitted in the one to four range. Senior AOTC management informed us that the reasons for the delays in reporting adjudications occurred as a result of staffing issues, volume of dispositions, and the retention of case files by judges after adjudication.

Because of delays in receiving criminal traffic dispositions, the RMV could not update licensees' driving records in a timely manner. Under these circumstances, state agencies and others who may use ALARS will not always obtain a current and accurate record of a licensee's driving history. While this issue could adversely affect public safety and the RMV management advised us they were aware of the delays in the adjudication of criminal driving offenses, the RMV did not believe it bears legal responsibility for monitoring of this matter. However, since the RMV is the primary Commonwealth agency responsible for the administration of Massachusetts' motor vehicle and driving laws, we believe that the RMV is uniquely well positioned to monitor and seek remedies for this public safety issue.

b. Driver's License Suspensions and Revocations

Our audit tests determined that a large number of motorists who were found guilty of serious criminal vehicle violations were able to keep their licenses and legally drive on Massachusetts' roads for a significant period beyond the date that their licenses should have been revoked because of administrative delays in the processing of criminal traffic citations. Although these motorists represent a relatively small number in comparison to the four million licensed drivers, we identified 7,500 to 9,000 of these motorists representing three to four percent of the 245,634 criminal uniform citation dispositions for calendar years 2005 and 2006. Penalties (such as suspensions or revocations of driving privileges) were

in some cases delayed for over three years, during which time these individuals were not held responsible for the consequences of their actions and permitted to continue driving. In some instances, the delays were so great that the suspension or revocation period had expired prior to the RMV notifying the licensee of the suspension or revocation. The untimely processing of driver's license suspensions and revocations results in problem drivers remaining on the road for extended periods of time, which potentially compromises public safety.

Pursuant to Massachusetts General Laws Chapter 90, the RMV is responsible for maintaining lifetime records on each licensed driver and revoking or restricting driving privileges when specific events have occurred. Suspension or revocation of driving privileges can occur when drivers commit various offenses, as set forth in law. Examples include accumulating certain point totals for traffic infractions, violating a traffic law and failing to pay the fine or appear in court as directed, or driving under the influence of alcohol, drugs, or other substances.

The RMV's Driver Control Unit (DCU) is responsible for processing license suspensions and revocations of those who abuse their driving privilege. The following definitions or explanations provide a contextual framework for our findings and recommendations:

- A license suspension is the temporary withdrawal of a licensee's privilege to drive a motor vehicle.
- A license revocation is the termination of driving privileges. Reinstatement of driving privileges can occur, in some cases, if specific requirements were met as specified by law or by a judge. One example is enrollment in an approved driver treatment program allowing first time O.U.I. offenders the ability to apply for a hardship license.

License suspensions and revocations are based on electronic and manual analysis of the information within ALARS. Criminal citation dispositions related to suspensions and revocations often occur as a result of licensees being convicted of committing specific driving-related offenses (for example, O.U.I. or D.W.I.). License suspensions also result from outstanding arrest warrants. In addition, a temporary suspension may be issued by a police officer at the time of a violation that results in an immediate suspension ranging from 45 to 360 days. In those instances in which a license is being suspended or revoked, the RMV is required to notify the licensee after receipt of final disposition, however; the law does not provide a time frame for making the notification.

As part of our test, we selected a statistical sample of 205 from the previously noted population of 21,114 adjudicated criminal uniform citations for the calendar years 2005 and 2006 to determine whether the RMV properly and timely notified licensees whose license was being suspended or revoked. In addition,

we determined how long these individuals had an active license within ALARS after their criminal citation adjudication date. We found that 89 individuals, 43% of the sample population, inappropriately had an active license within ALARS. In some instances, licenses remained active within ALARS for over three years after their associated criminal conviction.

We determined that in one case an individual was allowed an early reinstatement of their license because ALARS lacked effective control features to reduce the possibility that the RMV will reinstate driving privileges prior to a notification of a court-hearing disposition of a criminal citation. We determined that timing and communication problems resulted in a premature reinstatement. The individual was automatically notified through ALARS that their temporary suspension period ordered by local police had expired. After paying the associated fee the individual was reinstated as an active driver within ALARS. However, because of timing issues involving posting the latest offenses to the driving record the RMV authorized the reinstatement, without knowledge that the individual was adjudicated as guilty and was to have their driver's license suspended for a two-year period for their 2nd O.U.I. offense. We also determined that in some instances the delays were so great that individuals that had believed their suspension would be in effect from the date of the Court's adjudication learned later that their actual suspension period did not begin until after formal notification by the RMV. This resulted in leaving some individuals without licenses for much longer than the intended time frame dictated by Courts.

During the course of our audit, AOTC senior management had agreed to implement an interim solution to deliver an electronic version of the criminal citation abstracts to the RMV. This process would enable the RMV to produce daily reports outlining all adjudicated criminal citations by the Judiciary. The RMV would be able to compare and contrast the criminal citation abstracts to the actual criminal citations received via the mail and to denote any missing adjudicated citations and help remove the possibility of criminal citations that are lost or removed from being posted to drivers' records within ALARS.

By not implementing a more efficient method to obtain timely adjudicated criminal citations and the lack of specific RMV monitoring and evaluation procedures, the general public has been placed at risk. Drivers in Massachusetts are unknowingly sharing the roadways with individuals that should not be on the road, drivers that have been convicted of offenses such as vehicular homicide, O.U.I. 2nd and 3rd offenses, possession and distribution of drugs in a school zone, driving to endanger, and leaving the scene of a personal injury accident. As a result of inefficient processing and monitoring procedures, these drivers remain on the road long after their licenses should have been suspended or revoked.

Recommendations:

We recommend that the RMV develop and implement processes to monitor the timeliness with which the results of adjudication for criminal traffic offenses that require RMV action are recorded by the Registry, and that such information be provided to the Judiciary on an established schedule. We recommend that the RMV monitor the receipt of adjudications and provide the AOTC with documentation of the extent of delay and source of the judicial mailings. In order to provide current and accurate licensee driving records and enhance public safety, we recommend that the RMV, in conjunction with AOTC, provide suggestions to the Courts to encourage prompt filing of disposition information and create an assurance mechanism that these instructions are carried out. The Legislature should consider making statutory changes that would require that the Judicial Branch report the final disposition of each criminal offense written on a uniform traffic citation to the RMV within an established time frame.

We recommend that the RMV seek methods to reduce the processing time of adjudicated criminal citations to help ensure that dangerous drivers are removed from the roads in a more timely manner. Working with the Courts, the RMV should develop an automated process to transmit adjudicated criminal citations electronically. Electronic transmission of adjudicated citations would improve this process and reduce the potential for data entry errors and the possibility of citations being lost or removed.

Auditee's Response:

The Audit Report analyzed the delay by the Courts in sending the RMV court abstracts of criminal adjudications, thereby delaying mandated license suspensions/revocations. This has been an issue of continuing frustration for the RMV. Despite attempts over the last 10 years to position the RMV and the Court Systems to establish a direct electronic connection which would be the most secure and effective solution; these attempts have fallen short because of the prohibitive cost.

As recently as September 14, 2007, at the request of the Auditors, a summary report of all courts showing the age of each criminal citation from disposition date to receipt by the MRB for the years 2005 and 2006 were sent to the CIO of the Trial Courts and the Under Secretary of the Executive Office of Public Safety. This report reveals that 98.5 percent of the total number of criminal citations (129,031) received by the MRB in 2005, were sent to the MRB between 0-360 days after their date of adjudication. 1.5 percent was received by the MRB in 360+ days after their date of adjudication. In 2007, the MRB received 132,026 criminal citations. 98.2 percent were received between 0-360 days after their date of adjudication, and 1.8 percent was received 360+ days after their date of adjudication.

The RMV has tried to encourage collaborative efforts to develop and implement a practical interim protocol for tracking the progress of criminal violations from adjudication to RMV notification. The RMV has conducted an exhaustive internal examination of the time it takes to process a citation once it is received by the MRB. The

RMV renews its resolve to work with the Massachusetts Court System and the public safety community to develop a workable solution by taking the following action items:

RMV Commitments:

1. *The Registrar, Rachel Kaprielian will convene an Executive Working Group this summer to reach a shared resolution to this long-standing concern. The Registrar will reach out to the highest level executives and their IT and security experts including: The Chief Justice for the Administration and Management of the Massachusetts Trial Courts (the "Chief Justice"); the Executive Office of Public Safety; the State Police; and, the Criminal History Systems Board to meet and commit to a resolution that will end the delay in reporting criminal adjudications. The Executive Working Group could possibly facilitate a legislative effort to secure funding to implement the Group's solutions.*

2. *The RMV will request that the Executive Office of Public Safety, through its Merit Rating Board (the "MRB"), track on a monthly basis the aging of criminal convictions from the date of conviction to the date of receipt by the MRB and develop a report based on those findings. Such report shall be provided on to the Executive Working Group for analysis.*

Auditor's Reply:

We believe that the course of action outlined by the Registrar will provide the management attention and focus necessary to more appropriately monitor the receipt and processing of criminal adjudications, and hopefully realize a technical solution for receiving adjudications in a more timely manner from the Courts. While a short-term technical solution may be achieved, we recognize that ultimately upgrades to IT systems are required.

We agree that the summary report requested by the audit team demonstrates fairly significant delays in the receipt of criminal adjudications (example: 98.5 percent of the total number of criminal citations (129,031) received by the MRB in 2005 were sent to the MRB between 0-360 days after their date of adjudication). We suggest that tighter time frames be used for the aging reports to be generated from the monitoring and evaluation processes. We also believe that the RMV and the Courts need to implement procedures for the reconciliation of issued criminal citations to ensure that all adjudications are received, recorded, and processed by the RMV in a timely manner.

2. RMV Assessment of Motor Vehicle Excise Tax Billings

We determined that the Commonwealth's cities and towns were deprived of millions of dollars in potential excise tax due to untimely and inaccurate billings to owners of high-end luxury vehicles. Excise tax bills for 12,000 model year 2005 vehicles were delayed by as much as two years. As a result, over 4,600 excise tax invoices could not be collected because these vehicles were no longer registered in Massachusetts, resulting in over $1.3 million of uncollected excise tax revenues that could have been used

by cities and towns to fund important local services. In addition, we determined that the RMV did not have a process in place to accurately identify all vehicle values used to generate excise tax billings, including luxury cars, trucks, buses, and motor homes. We determined that the RMV, over the course of several years, assigned well below market valuations for thousands of vehicles, resulting in undervalued excise tax computations for local cities and towns. According to the RMV, to go back and determine the difference between the excise tax bills had the vehicle been correctly valued and what it was actually billed for would be a "tremendous and laborious effort." In addition, the Department of Revenue determined that because the undervalued vehicle excise tax was paid, the RMV could not re-bill individuals for the correct and higher valuations. These undervalued vehicles included luxury vehicles (Ferrari, Lamborghini, Bentley, Jaguar, e.g.); large trucks and buses; trailers; and specialized vehicles constructed on a chassis, such as ambulances and auto homes, that resulted in millions of dollars in uncollectible revenue.

Under MGL Chapter 60A, all Massachusetts residents who own and register a motor vehicle must annually pay a motor vehicle excise to the city or town within which the licensed motorist resides. The annual motor vehicle excise taxes that vehicle owners in Massachusetts pay are an important and significant source of revenue for cities and towns. For example, the excise tax bills prepared by the RMV for Massachusetts cities and towns totaled $700.4 million for 2006. The excise tax is levied by the city or town where the vehicle is principally garaged and the revenues become part of the local community treasury. The formula used for the assessment is based upon the provisions of Massachusetts General Law, Chapter 60A, Section 1. Excise bills are prepared by the Registry of Motor Vehicles according to the information on the motor vehicle registration and are then sent to city or town assessors who commit them to the local tax collectors for distribution and collection of payment. Cities and towns may also prepare their own bills based on excise data sent by the Registry in conformity with Registry requirements.

According to the RMV, for most motor vehicles, the calculations are performed electronically using valuation tapes. For automobiles and light trucks, the valuation tape is created by the National Automobile Dealers Used Car Guide Company (NADA); for heavy trucks and school buses, the tape is created by Maclean Hunter Market Reports, Inc., publisher of the Truck Blue Book; and for motorcycles, the tape is created by Hap Jones, publisher of the Motorcycle Blue Book. In each case, it is the vehicle identification number (VIN) that drives the electronic valuation process. However, we determined that the NADA data used by the RMV to assign values to motor vehicles does not include every vehicle. Luxury vehicles, such as Ferrari and Lamborghini, would require a manual valuation process of looking through multiple periodicals to determine the actual values of these vehicles.

We determined that at one time the RMV had employees that specialized in performing the manual valuations for these types of vehicles, employees who understood the excise tax process well. However, as these "specialized workers" retired, resigned or were reassigned within the agency, fewer and fewer manual valuations could be completed, resulting in many undervalued vehicles. We determined that the RMV was unaware of the staffing shortages that occurred in this capacity over the course of time from the late 1990s up to calendar 2003. As a result of inadequate staffing, thousands of vehicles were assigned below market Manufacturer Suggested Retail Prices (MSRP), resulting in undervalued excise tax computations for local cities and towns. This issue of lost potential revenue may have placed many cities and towns in a precarious situation with regard to funding essential services.

The end of the manual valuation process in calendar year 2003 resulted in a large number of vehicles that had no value assigned to them. In order to ensure that these vehicles had some value associated with them, the RMV, through ALARS, assigned a default value of $17,000 for any vehicle that did not have an assigned value. However, the majority of the vehicles that required a manual valuation process had a higher MSRP than the new $17,000 default value. This automated process therefore increased the risk of incorrectly placing a value on vehicles for excise tax billing purposes. For example, a new Maserati that was not identified within the NADA would now have an automated default valuation of $17,000, although the MSRP for this vehicle was actually $325,000. The error valuation would result in an excise tax bill of only $382.50, rather than the correct excise tax bill of $7,312.50. Other examples include vehicles such as Bentleys, Lamborghinis, Astin Martens, certain BMWs; large trucks and buses; trailers; and specialized vehicles constructed on a chassis, such as custom campers that had values of up to $1.5 million, which were given much lower default values. We determined that the RMV was capable of reassessing undervalued vehicles and preparing correctly valued excise tax bills, determining the variances, and then assigning a dollar amount of the underpayment for remittance.

The RMV stopped assigning the default value of $17,000 for any vehicle that did not have an assigned value by the end of 2004. Model year 2005, 2006, and 2007 vehicles whose MSRP could not be identified automatically were not sent excise tax bills. In early 2007 the RMV completed an evaluation of ALARS and discovered that some vehicles either did not have a value or were undervalued. The RMV had an independent consultant undertake an effort to identify and review all of the vehicles on ALARS without an accurate valuation. The RMV initially determined in May 2007 that over 124,000 vehicles did not have values recorded within ALARS. At that time, the RMV selected model year 2006 for the initial manual valuation effort and estimated that the corrected valuation could generate an additional $6 to $8 million in excise tax revenue for the Commonwealth. When the revaluation process ended, the RMV determined that there were actually over 131,000 vehicles without recorded values

within ALARS, and that the corrected valuation could generate an additional $32 million in excise tax revenue. During the course of our audit, the RMV began sending out excise tax bills to city and town assessors for these vehicles, which prevented us from determining the amount of actual collections. However, we were able to determine that for the 12,000 model year 2005 vehicles that previously had no reported value, the RMV was only able to create revised excise tax bills for 7,326 vehicles, as the remaining 4,674 vehicles were no longer registered within the Commonwealth. The revised excise tax bills for the 7,326 vehicles referenced above averaged $280.00 per vehicle. Applying this average to the 4,674 vehicles no longer registered with the RMV, we determined that Massachusetts cities and towns lost the opportunity to collect $1,308,720 in excise tax revenues for these vehicles. During the course of our audit, it was our understanding that the RMV was preparing, but had not yet fully developed, a corrective action plan that would ensure that all vehicles would be properly assessed at their current values and billed accordingly.

Recommendation:

We recommend that the RMV set up assurance mechanisms to identify staffing shortages before they could adversely affect key business processes, such as the generation of excise tax bills. We further recommend that the RMV fully implement their recommended plan to produce timely and accurate excise tax bills. Specifically the plan called for:

- A twice annual focused valuation.
- Using outside valuation processes (sales tax and contracting manufacturers e.g.) for vehicles NADA will never value (buses, hearses, and ambulances e.g.)
- Capture better vehicle descriptions at to help ensure accurate initial vehicle valuation.
- Capture the MSRP at the point of the sale to determine excise tax on vehicles not included within the NADA.
- Segregate duties between Customer Service for the error correction and interface with assessors and the valuation process with the Registration and Title area.

In addition, once the RMV has implemented the new excise tax process, the RMV should set up monitoring and evaluation procedures to verify that the excise tax computations are accurate, valid and complete.

Auditee's Response:

> *The Audit Report examined the excise collection mechanisms of the RMV. Specifically, the Report determined that excise taxes had not been properly collected for exotic, and composite or specialized vehicles. As such, the RMV failed to prepare excise tax billings for cities and towns in the amount of $1.3 million dollars. The 2006 excise billings prepared by the RMV were $700.4 million dollars. As a percentage of overall receipts, this error represents a failure rate of less than one percent. However, the RMV*

recognizes the pressure that many community budgets are under and will not settle for any gap in collections. As such, the RMV has identified and purchased a new web-based valuation product that will capture many of the vehicles not included in the NADA valuation tape currently used.

RMV Commitments:

1. *The RMV has undertaken a review of the new vehicle registration process to identify methods to improve vehicle descriptions and capturing the MSRP. The RMV has begun a series of enhancements to ALARS to improve this process including publishing these standards to automobile dealers and insurance agents (who generate the majority of the documentation for initial registrations).*

2. *The RMV has begun performing twice annual valuations.*

3. *The RMV has hired personnel with specialized knowledge of automobiles to manage excise valuations. An RMV Manager will conduct a periodic review and informal audit of the new hiree's work, to verify the accuracy of his vehicle valuations.*

Auditor's Reply:

We commend the actions of the RMV to initiate a process for capturing MSRP values for all vehicles, including luxury automobiles. We concur with the corrective action to be taken by the RMV to better address the generation of excise tax invoices for cities and towns in the Commonwealth. We suggest that control practices be implemented to provide adequate assurance that valuations and periodic reviews are conducted in accordance with management's directives. However, potential losses in revenue collection of cities and towns may well have exceeded the one percent failure rate had the RMV formally calculated the losses in excise tax revenues resulting from the undervaluation of vehicles for years prior to 2005.

3. Criminal Offender Record Information Background Checks

We determined that Criminal Offender Record Information (CORI) background checks were not being performed as required by RMV's policies and procedures. Our audit revealed that RMV's CORI policy states that the agency will conduct CORI background checks prior to the time of employment for all prospective, temporary, and contract employees. Additionally, the CORI policy states that current employees will be subject to annual criminal record checks.

We determined from our statistical sample of 75 individuals that 39, or 51%, of the RMV employees tested received a criminal background check. Of the remaining 36 individuals, 32 were "grandfathered" and did not receive a CORI check, because they were hired before the implementation of the RMV CORI policy in 1996. Further analysis indicated that one of the individuals hired in 2006 never received a

CORI check. The remaining three individuals, although listed in the sample as active employees, had been previously terminated.

According to 803 CMR, "CORI compiled by each criminal justice agency shall be entered into and maintained in Criminal Justice Information Systems (CJIS) in accordance with procedures established by Criminal History Systems Board (CHSB)". The RMV is a criminal justice agency certified as such by the Criminal History Systems Board. As a criminal justice agency within the Executive Office of Public Safety, Registry employees may have access to confidential information on licensed drivers, including criminal traffic citations. As such, the Registry of Motor Vehicles should ensure the integrity of its employees and perform CORI checks as stipulated in the RMV CORI policy.

Although the RMV's CORI policy states that job applicants are subject to background checks, we found that similar checks are not performed when an employee transfers to other positions within the RMV. Although not required**,** a CORI background check might provide additional assurance that only qualified individuals are employed by the Registry. RMV employees have recently been reassigned as examiners to replace the State Police in administering road test exams, thereby increasing risk to public safety if CORI checks are not uniformly administered for all employees and contractors. In addition, the RMV policy states that current personnel will be subject to annual criminal record checks; however, our audit revealed that the RMV does not perform annual CORI checks on any of its current employees. It is the policy of the RMV "to disqualify from initial or continuing employment in certain positions any prospective or current personnel having a record of criminal offenses, which indicates that the person poses a significant risk to the security and integrity of the RMV or the interest and safety of the driving public." We found that accepted standards suggest that periodic background reinvestigations should be performed, consistent with the sensitivity of the position. However, RMV officials have not assigned different levels of sensitivity to job positions and have not performed reinvestigations.

We also determined that the RMV's policy states that in addition to a criminal record check of activity in Massachusetts' criminal courts, all prospective or current personnel that have resided in another state may be subject to a criminal records check in that state. We determined that the RMV rarely performs out-of-state CORI checks or inquiries. When CORI checks and inquiries were being performed, they were being performed by the State Police. The CORI background check provides relevant information regarding convictions in Massachusetts, but does not include any crimes committed in another state. For example, an individual convicted of a rape in New York, who subsequently moved to Massachusetts and as required by law registered as a sex offender, would not be identified as such on a Massachusetts CORI background check. CORI and Sexual Offender Registry Information (SORI) databases are not currently

linked. Therefore, enforcement of annual CORI checks by the RMV, with corresponding inquiries regarding individuals from outside the Commonwealth, would mitigate the risk to the security and integrity of the RMV, as well as the interests and safety of the driving public by identifying RMV employees that should not be employed in sensitive positions.

Recommendation:

We recommend the RMV modify their CORI policy to more accurately reflect their current business processes and ensure that annual CORI checks are performed on all prospective and current employees. The RMV should put in place proper monitoring and evaluation procedures to ensure that RMV complies with its amended policy. The RMV should assign different levels of sensitivity to job positions and ensure that CORI background checks are performed on employees who transfer to positions designated as sensitive that may require unsupervised contact with potentially vulnerable individuals. Completion of annual CORI background checks would also include any new offenses that occurred after employment that should preclude individuals from candidacy for new or sensitive positions. Lastly, RMV should perform SORI background checks for specific individuals as defined by state law. Chapter 6, Section 178I, of the General Laws states that the RMV "shall receive at no cost from the board a report to the extent available pursuant to Sections 178C to 178P, inclusive, which indicates whether an individual identified by name, date of birth or sufficient personal identifying characteristics, is a sex offender." We recommend that the RMV initiate a process to submit requests for SORI reports to the Sex Offender Registry Board for those positions designated as sensitive. The RMV risks not being able to detect unacceptable employee actions when CORI and SORI background checks are not performed for individuals who have the potential for unsupervised contact with potentially vulnerable groups.

Auditee's Response:

The Audit Report accurately determined that although the RMV had a policy of performing Criminal background checks ("CORI") prior to employment and annually throughout employment, that policy was not universally followed. The RMV has, since the period of the audit, adopted the standards imposed by the Governor's Executive Order 495, set forth on January 11, 2008. The spirit of the Executive Order is to provide employment opportunities to persons with a criminal record who have been rehabilitated. It creates standards by which government employers must adhere in their hiring practices.

The Audit Report recommends that the RMV conduct an annual CORI for prospective and current employees. To conduct CORI checks on union employees will require negotiation with the union (NAGE/SEIU) as part of the Collective Bargaining Agreement.

The Report includes concern that the RMV does not conduct checks for out of state convictions. The only background check database that contains all U.S. state is the Interstate Identification Index, also known as Triple I ("III"). This system is maintained by the Federal Bureau of Investigation and it is limited to access by criminal justice agencies. Non-criminal justice agencies (such as the RMV) may only access III as specifically authorized by statute. Once authorized, each person who is checked must produce a fingerprint which will be sent to the FBI.

RMV Commitments:

1. *The RMV will draft a policy standard in accordance with the Governor's Executive Order 495. Toward that end, the RMV is currently reviewing the Model CORI Policy established by the Criminal History Systems Board and adapting it to the RMV. The RMV will distribute the policy to all employees and ensure that its managers are fully trained on the policy.*

2. *The RMV will contact the union to begin negotiations of CORI background checks for prospective and current employees. Such negotiations will include a statement in all hiring postings that the position may be subject to a criminal background check prior to employment and during employment.*

3. *The RMV will analyze and classify which positions would, due to the nature of the work, require a SORI prior to employment or promotion .The RMV will then work with the SORB to establish a protocol whereby a SORI would be conducted.*

Auditor's Reply:

We agree with the course of action to be taken by the RMV with the regard to the CORI/SORI procedures. We believe that requiring employees who are already employed or will be transferred into an area that the RMV has classified as high-risk or sensitive to undergo a CORI/SORI review will help minimize risk and exposure to the Registry. The RMV should continue to negotiate with union workers to ensure that positions may be subject to a criminal background check prior to and during employment.

4. Disaster Recovery and Business Continuity Planning

We determined that the Registry of Motor Vehicles (RMV) did not have a disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems be rendered inoperable or inaccessible. At the time of our audit the RMV presented an EOT Continuity of Operations Plan (COOP) dated January 31, 2006, which had not been signed or updated. The COOP presented a management framework that established high-level operational procedures and guidelines for EOT businesses if normal operations were not available. The plan only referenced the RMV's Automated Licenses and Registration System (ALARS), and failed to provide recovery strategies for system components or architecture. The COOP also did not identify the detailed steps RMV would need to take to recover from a disaster. In addition, RMV's senior management had

not developed a comprehensive strategy outlining details for business contingency planning, off-site processing, and addressing important telecommunication and security matters that might arise. The lack of processing capability could result in the inability of the RMV's ALARS to have accurate, up-to-date, and complete driver's license and registration information for the over 4 million drivers in the Commonwealth.

Business continuity planning enables an organization to minimize the loss of communications and important computer operations during an emergency. As agencies become increasingly dependent upon IT processing capability in all areas of their operations, the ability to quickly and effectively recover from adverse conditions becomes essential. This is especially true for an agency with important public safety and security responsibilities such as the RMV, where management of licensed drivers and registrations is highly computerized. Good business continuity planning can significantly increase the probability of surviving a major disaster. Although the COOP covers Continuity of Operations and lists potential impact to EOT's businesses, there is no specific detail regarding the RMV's systems and infrastructure.

Over the years many different terms have been used for planning for recovery from computer outages, such as "disaster recovery," "contingency planning," and "business continuity planning." All have a slightly different focus, with business continuity planning being the most encompassing. Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. By necessity, it includes planning for contingencies and planning for disaster recovery, and is focused on the information system functions that are the most necessary to continued agency operations. Control Objectives for Information and Related Technology (CobiT) standards indicate that an organization has implemented a sound business continuity strategy when management:

- Develops a written continuity plan that is in line with the organization's objectives.
- Reviews and updates the plan periodically.
- Tests the plan and periodically updates it based on the test results.
- Conducts periodic staff training on carrying out the plan.
- Establishes adequate off-site storage for critical backup tapes.
- Identifies alternatives for backup processing sites and replacement computers.
- Contracts for offsite hardware and processing facilities in advance of an emergency.
- Develops alternative processing procedures for user departments to implement until processing can be restored.

The Business Continuity and Contingency Plan (BCCP) itself should:

- Focus on sustaining an organization's business functions during and after a disruption. An example of a business function may be an organization's payroll process or customer information process.
- Contain an inventory of the most critical hardware, software, and supplies.

- Discuss the most likely types of disasters and describe various levels of disaster.
- Specify the detailed steps to take to recover services, including assigning specific roles and responsibilities to specific staff members.
- Detail how to operate the critical computer programs.
- Contain amended documents, i.e., the disaster recovery plan, business resumption plan, and occupant emergency plan.
- Set responsibilities and priorities and should be coordinated with those in the Continuity of Operations Plan (COOP) to eliminate possible conflicts.

Senior management has implemented some sound practices, such as a well-developed system for backing up critical data, including off site storage of backup tapes. Although ALARS is backed-up nightly at the Massachusetts Information Technology Center (MITC), RMV only performs monthly off-site storage of data. The RMV should consider increasing the frequency of off-site storage of backup media because of the sensitive nature of the data. The RMV also has developed alternative procedures for users to follow when computer services are unavailable, although the procedures are not written. The RMV's mission critical computer programs reside on the RMV's mid-range computer at MITC. Senior management informed us that in the event of an emergency, there is a contract in place with SunGard for a remote site in New Jersey. However, the New Jersey location site is not a hot site and RMV operations could be significantly impacted in the event of a disaster.

The EOT's COOP does not address specific telecommunications and security issues that would arise if processing had to take place at a site other than the RMV's data center. A great deal of confidential information contained in the ALARS is transmitted over the RMV's network, as well as from the agency's central office in Quincy and branch offices to the data center at MITC. According to senior management, should a disaster occur at the data center at MITC, telecommunication and information system support will allow the RMV to establish a network connection from another site. However, no planning or testing has been done to implement secure transmissions from the central office or the 35 branches and satellite offices throughout the state. In addition, the RMV has not completed any recent training for staff in what to do in an emergency. Without training and testing, when an emergency occurs staff can be disorganized, thus taking much longer to recover processing.

Recommendation:

RMV should establish a business continuity planning framework that incorporates criticality and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training, and communication. RMV, in conjunction with the EOT, should develop and implement a comprehensive business continuity and contingency plan should a disaster disrupt its data processing or business operations. To ensure that the RMV reacts optimally in the event of a disaster, a

corresponding document should be correlated to the EOT COOP detailing RMV's specific information, which should include: updating the plan for the RMV's current mission critical ALARS system; performing a risk analysis that assesses various disaster scenarios; developing an expanded disaster recovery plan that addresses the most likely disasters that might befall the RMV and its branches.

RMV should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The plan should assign specific staff assign with roles and responsibilities and present detailed steps for them to follow in recovering computer operations. The plan should also address the telecommunications and security issues that would arise if the RMV had to conduct off site computer operations. In addition, the RMV business continuity plan should document vendor protocol for the emergency use of computers suitable for operating the RMV's mission-critical application. The RMV should conduct periodic training for the staff and ensure that a complete hard copy and electronic copy of the plan should continue to be stored in a secure off-site location.

Auditee's Response:

The Audit Report recommends that the RMV create and implement a business continuity and contingency plan that would address a disaster disruption of RMV data processing and business operations. The RMV is sensitive to the issue of data disruption and disaster planning. It has been sending both IT and Legal representatives to attend the meetings of the Enterprise Security Board and participate in its mission. Recently, nine RMV employees, including a Deputy Registrar, the CIO for EOT, and the RMV Director of Business Development, participated in a tabletop cyber exercise, ("Mass Attack") which had been coordinated by ITD and Homeland Security. It should be noted that the RMV was determined to have been both responsive and proactive in its reaction to the injections of the exercise. The RMV members were well informed, prepared and a model for other state participants.

RMV Commitments:

1. *As a member of the Massachusetts Mobility Compact, the RMV is participating in the development of a security and disaster recovery plan which will include testing and training.*

2. *The RMV is participating in a Secretariat wide development of a back-up system for all RMV data and e-mail that is maintained on network based drives. This system, "ComVault", will centralize storage and recovery for the business based operations (not to include ALARS).*

3. *EOT and the RMV are undertaking a review of all EOT networks and creating redundant, separate path connections to either the major hubs or branch locations.*

4. *The RMV fully supports ITD's efforts to locate and build a "hot" back up data center in the Commonwealth. While this may be long in coming, the RMV is*

hopeful that ITD will be successful and the RMV's critical systems can be included in its facility.

5. *The RMV will utilize the detailed recommendations contained in the Audit Report in establishing its disaster recovery and business continuity plan.*

Auditor's Reply:

We are pleased that the RMV recognizes the need for developing and implementing a comprehensive disaster recovery and business continuity strategy. We acknowledge RMV's participation in the Massachusetts Mobility Compact to assist in the development of a disaster recovery plan and the opportunities for collaborative efforts with ITD and other agencies. However, until appropriate disaster recovery and business continuity plans are completed, the RMV needs to continue to focus on risk management and contingency planning.

5. Inventory Controls Over Computer Equipment

Our audit disclosed that the RMV's inventory controls over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in the RMV's inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, or lost. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not in place. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders the RMV's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Although we determined that the RMV had documented internal controls regarding the purchasing and receiving of IT resources, we found that documented policies and procedures needed to be enhanced regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. For example, although documented procedures were in place requiring that a perpetual inventory be conducted, we could not find documentation to support an annual physical inventory. Also, although the RMV had adequate policies and procedures for the disposal of surplus property and Chapter 647 requirements, they were not being followed, as evidenced by the RMV's failure to submit required Chapter 647 reports to the Office of the State Auditor.

Our analysis of the RMV's inventory system of record indicated that most required data fields, including description, identification tag, user name, serial number, cost, and location were present. We found that the system of record lacked integrity, since of the total population of 2,138 records we reviewed, information related to certain data fields including "serial number" (20%), "date of purchase" (93%), "cost" (98%), and "condition code" (99%) were missing information in these data elements. We also found that the IT inventory listing did not include a data field for the purchase order number. The inclusion of this information will help ensure that the agency's IT related computer equipment will be properly accounted for during the agency's annual physical inventory. Although the RMV provided an inventory system of record that listed IT related assets as of May 2, 2007, we were unable to determine the total value of the inventory because the cost was not recorded in 98% of their respective data fields. By failing to record the historical cost of purchased computer hardware items and their purchase dates on the RMV's inventory system of record, the RMV was not in compliance with the Office of the State Comptroller's 2005 fiscal year fixed-asset requirements and Office of the State Comptroller (OSC) Memorandum No. 313A.

With respect to the recording of IT-related assets, we found that the RMV lacked appropriate and adequate management oversight to prevent and detect errors in the recording of identifying data for received computer equipment into the RMV's inventory system of record for IT equipment. Our tests indicated a significant error rate and inconsistency in identifying data recorded by staff on the RMV's computer hardware inventory listing. Specifically, our audit tests comparing data recorded on invoices for purchased computer equipment to the RMV inventory listing indicated 84 errors in recorded identifying data for our sample, or an error rate of 25% in the recording of 336 tested hardware items purchased in fiscal year 2006 and 2007. Because of the rate of data input errors, the failure to record asset costs and acquisition dates, and inadequate management of the system of record, an acceptable level of data integrity did not exist for the RMV's inventory system of record for IT equipment at the time of our audit. The RMV needs to ensure that appropriate controls are in place for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory database.

Our inventory tests were conducted against the 2,138 IT-related assets on the RMV inventory record. Based on a statistical sample of 111 items valued at $59,323, we verified by inspection the existence and the recorded location of the computer equipment. We found that 54, or 49%, of the 111 PCs and monitors valued at $26,551 were not at the locations indicated on the inventory system of record. We provided the Deputy Registrar with a list of the 54 missing items. With the assistance of the Deputy Registrar, we were able to subsequently verify the location of 46 of the missing items valued at $21,051.

We could not verify the location of the remaining eight items totaling $5,500. Our tests indicated that of the remaining 57 items from our sample of 111 PCs and monitors, all of the items were properly tagged, included correct serial numbers and manufacturer's identification, and were listed on the inventory system of record with proper descriptions. Furthermore, to verify the integrity and completeness of the inventory system of record, we judgmentally selected 112 additional IT-related items in adjacent locations to the items selected in our statistical sample. We determined that 100, or 89% of the 112 items were properly identified on the RMV's listing of inventory computer equipment. However, our audit test indicated that the remaining 12, or 11% of the IT related items, were not recorded on the inventory system of record. In addition, our inventory test results of 75 notebook computers found that 70, or 93% of the sampled items were in the correct location as listed on the system of record. However, we could not verify the location of five, or 7%, of the notebooks listed on the inventory system of record. Of the five notebooks, three were associated with individuals who were no longer RMV employees.

We determined that the RMV maintained a policy of obtaining signed acknowledgements that users have received a notebook computer; however, we found the following by reconciling the signed acknowledgments to the notebook inventory system of record:

Description	No.	Percent
Properly signed and approved acknowledgments:	24	33%
Acknowledgments not properly signed and recorded:		
• Unable to locate acknowledgments	25	33%
• Acknowledgments associated with stored equipment	18	22%
• Not signed by the employee; signed by the manager	5	7%
• Employee or the manager did not sign	3	5%
Total not properly signed and recorded:	51	67%
Total:	75	100%

We determined that although the RMV has procedures in place for acknowledgment that users have received a notebook, assignments of 51, or 67%, of the 75 notebooks on the inventory system of record did not have supporting documentation identifying who notebooks were assigned to and a signoff approval form indicating receipt of the notebook computer. As a result, there is an increased risk that notebook computers may be lost or stolen.

Recommendation:

The RMV should strengthen its current practices to comply with the Office of the State Comptroller's (OSC) requirements that each state agency conduct an annual physical inventory to ensure the proper accounting for, and disposal of, property and equipment, and that IT resources are adequately maintained

and safeguarded. The RMV should conduct an annual physical inventory and reconciliation of IT resources to help ensure that an accurate, complete, and valid inventory record is being maintained and includes information such as cost, date of acquisition, and references to the appropriate purchase order.

We recommend that the RMV enhance its inventory control policies and procedures related to the receiving function by increasing supervision and oversight to help ensure that the agency properly records all received items of computer equipment on the inventory system of record. The agency should segregate the functions of receiving, tagging, recording, and distribution of assets to reduce the risk of undetected data entry errors, unrecorded items, and loss of IT related equipment. A member of the IT staff should continue to assist in the verification of equipment deliveries and the subsequent tagging of equipment.

With respect to IT configuration management, the RMV should expand the inventory data fields to include reference to the appropriate purchase order number. In addition, the agency should update missing information in its inventory data fields with specific attention to "serial number", "date of "purchase", "cost", and "condition code". In addition, the agency's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

In order to ensure safeguarding of notebook computers, we recommend that the RMV strengthen its controls to maintain complete and up-to-date signed acknowledgements that users have received or returned their notebook computers, thereby reducing the risk that notebooks may be lost or stolen.

Auditee's Response:

The Audit Report accurately portrayed the need for the RMV to update and improve its inventory control over computer equipment. While some of the problems with inventory control were the result of the RMV's consolidation of its IT department into the EOT Secretariat, the consolidation now provides us with the opportunity to correct the problems noted by the Auditor.

RMV Commitments:

1. *The RMV through EOT will, beginning this summer, deploy a new inventory management system that ties the purchasing of equipment (PO#) to its receipt and deployment. The RMV will continue to segregate the receiving, recording and inventorying of office equipment from its ordering and deployment. The new inventory management system will record the physical location of the equipment and, for equipment assigned to an individual, record that assignment.*

2. *The RMV will hire an individual who will be responsible for an annual auditing/physical inventory of the office equipment and will, as part of this effort, implement a signed duplicate User Agreement form and process for all of the individually assigned equipment.*

3. *EOT will also deploy full disk encryption software to protect the data on the RMV's laptop devices.*

Auditor's Reply:

We commend the actions initiated by the RMV to improve fixed-asset inventory controls. We believe that a single comprehensive inventory control system for all RMV fixed assets is an important ingredient for the Registry's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding fixed assets and assist the RMV in making IT infrastructure and configuration management decisions.

We believe that controls to ensure adequate accounting of fixed assets will be strengthened by updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory to the system of record. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for any lost, stolen, or surplused equipment. In addition, these efforts should help minimize the risk of lost or stolen equipment and improve the identification of the status of equipment for configuration management purposes.

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF TRANSPORTATION
REGISTRY OF MOTOR VEHICLES

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

BERNARD COHEN
SECRETARY

RACHEL KAPRIELIAN
REGISTRAR

AUDITEE RESPONSE - RESPONDENT OVERVIEW

June 5, 2008

John Beveridge
Deputy Auditor
Office of the Auditor of the Commonwealth of Massachusetts
One Ashburton Place, Room 1819
Boston, MA 02108

Re: RMV Audit Response

Dear Mr. Beveridge:

Please accept the enclosed RMV Response to the Audit Report No. 2007-0511-4T. I have read the Report and analyzed its findings and recommendations. I am grateful to the Auditors for having so comprehensively and fairly addressed both the good work that the RMV employees perform every day, as well as those areas in which the RMV must improve its performance. Let me stress from the outset that I welcome the findings of the Report, and I am committed to begin implementing its recommendations.

The RMV's response to the Audit Report reviews each aspect of the RMV's business practices which require improvement. As part of the response, I have included those changes that the agency has implemented since the completion of the Audit. As you will see, the changes demonstrate that the RMV is already working toward resolution of problems that have been systemic at the RMV and other governmental communities. The Response also includes the steps that will be taken as I move forward in my position as Registrar.

I am committed to immediately convene the working groups necessary to effect the required changes. These groups will represent the highest level of officials, as well as the internal experts necessary to carry out the changes. I ask that as the RMV completes the implementation of each change, I may reach out to you and the services of your office, to review the implementation of corrected actions. While many of the changes will occur quickly, others will take longer to develop. As the RMV makes strides towards its improvement, I would welcome the review and input of your office.

I thank you and your team for the professional review and analysis of the issues facing the RMV, and I look forward to the opportunity to improve upon the many services that the agency provides the public each day.

Very truly yours,

Rachel Kaprielian
Registrar

RMV Responses to Audit Conclusions

1. Deactivate IDs

Auditee's Response:

The RMV Audit Report revealed that the RMV failed to deactivate the ALARS IDs of 27 employees who were no longer employed by the agency. While none of the 27 former employees made any attempt to access ALARS since their departure, the Audit reveals a weakness that can be easily addressed and the RMV is committed to implementing the following action items:

RMV Commitments:

1. The RMV's current employee deactivation process requires branch managers and the HR department to notify IT security when an employee leaves, in addition to a periodic reconciliation where security sends a list of all currently active IDs to the managers to verify. The RMV will improve and expand its reporting of an employee's departure.

2. The RMV will work with EOT to implement an automated process using HRCMS (Human Resources Compensation Management System) to inform IT Security upon an employee's departure. In this manner, there is one source for all deactivations that need to occur.

3. The Registrar included this issue as part of the RMV's bi-annual training session at the Manager's Meeting last December. Managers were advised to be diligent in their reporting of employees who leave the agency.

Auditor's Reply:

We believe system access security in the RMV's IT environment is critical and commend the actions taken to improve controls in this area. We acknowledge RMV's efforts to enhance policies and procedures for access security based on our audit recommendations. We believe the RMV should continue to ensure that user privileges be clearly specified and documented for every active user account and constantly monitored and evaluated to ensure that only authorized users are allowed access to network application systems and data.

Third Party Access to ALARS – Security Concerns

Auditee's Response:

The Audit Report raised concerns regarding the security of personally identifiable information (PII) when accessed by third parties ("Business Partners"). The RMV considers the security of the personal information contained in its database as critical to its mission. Dissemination of personal information held by the RMV is wholly regulated under the statutory requirements of the Federal Driver Privacy Protection Act (the "DPPA") (18 U.S.C. 2721 et seq.) Since its effective date of September 13, 1997, the DPPA has established one category of data users who are required to have access to the RMV database and 14 categories of "Permitted Users" who may access the RMV's database. This limitation of access to RMV data fully pre-empts the Massachusetts Public Records laws. Access to RMV data is further established by statute at M.G.L. c. 90, §30A to divisions of the Commonwealth, municipalities as part of their official functions, and to insurers and their agents for purposes of the Safe Driver's Insurance Program.

The interpretation of the DPPA by the RMV was initially established by the Department of Justice ("the DOJ") the enforcing agency. On October 9, 1998, the DOJ sent an interpretation letter to the Massachusetts Office of the Attorney General. In the DOJ's letter to the Office of the Attorney General, the DOJ opined that the RMV could distribute its database containing PII to a commercial distributer (Worldwide Information Systems), as they were a Permitted User of the data under the auspices of the DPPA. The RMV recognizes that the greatest testament to the strength of our database security lies in the fact that we have not had a major data breach. However, the RMV remains vigilant to the future possibility. To that end, the RMV shares the concerns of the Auditor and has already implemented the following action items:

RMV Commitments:

1. The RMV requires all Business Partners to enter into a Security and Use Agreement. Access by Business Partners is by either secured, hardwired, private networks or the ITD approved Virtual Private Network ("VPN") for connectivity. The RMV has been reviewing its processes for transmitting data, recognizing and balancing the need for security along with the need to conduct business. To that end, the RMV will be insisting all of our VPN users upgrade, over the next year, to the new and enhanced VPN that ITD is now supporting.

2. Currently, the RMV utilizes the ITD forms as the basis for its Security and Use Agreements with third party users. The RMV has convened a working group to review, update and enhance these documents to reflect the recommendations of the Auditor.

Auditor's Reply:

We acknowledge that the RMV has initiated corrective action regarding the protection of personally identifiable information (PII) in order to address our concerns outlined in the audit report. We believe that the RMV's utilization of the ITD Security and Use and Agreement form for third-party users, designation of a working group to address PII security concerns, and upgrading VPN access will help the RMV ensure that PII information is more secure during transmission, receipt, and dissemination of data. However, we recommend that the RMV ensure that all third-party network transmissions are encrypted and not sent in a clear text format. Also, the RMV should monitor and evaluate compliance with ITD's Security and Use Agreement for third-party users.