Audit Report

Department of Transportation
Motor Vehicle Administration

May 2014

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.

- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.

- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.

- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

May 19, 2014

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Maryland Department of Transportation - Motor Vehicle Administration (MVA) for the period beginning July 10, 2009 and ending July 24, 2012. MVA's primary purpose is to oversee a variety of activities related to the ownership and operation of motor vehicles, including the registration and titling of vehicles.

Our audit disclosed that controls over MVA's collections and vehicle titling and registration transactions need to be strengthened. For example, our review of the related processes at three branch locations disclosed that, at one location, collections were not safeguarded prior to deposit and access to inventory (such as vehicle license plates) was not properly restricted. At two branch locations, system overrides for vehicle registration transactions were processed without evidence that the applicable documentation had been obtained. These three locations processed collections totaling $173 million during fiscal year 2012. MVA also did not use certain security features to help ensure the propriety of online credit card payments received from customers through its eStore.

We also noted that MVA did not properly restrict access to certain critical information systems, including the Driver Licensing and Point of Sale systems, and monitoring of security reports was not comprehensive. In addition, customers' sensitive personally identifiable information stored in these systems' databases was not encrypted. Effective controls were not established over MVA's virtual servers, which were used to support online services to customers.

We also noted that MVA did not always suspend vehicle registrations when motorists defaulted on payment plans with the Department of Budget and Management's Central Collection Unit for uninsured motorist penalty fees.

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

An executive summary of our findings can be found on page 5. The Maryland Department of Transportation's response to this audit, on behalf of MVA, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by MVA.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

*** Denotes item repeated in full or part from preceding audit report**

Executive Summary

Legislative Audit Report on the
Motor Vehicle Administration (MVA)
May 2014

- **MVA did not establish sufficient controls to safeguard cash receipts at one branch location with collections totaling over $141 million during fiscal year 2012 or collections received at headquarters for vehicle registration renewals processed at county offices. In addition, documentation was not always maintained at branch offices to support the propriety of vehicle titling and registration transactions processed by customer agents (Findings 1 through 3).**

  MVA should take steps to improve accountability and control over all cash receipts processed at branch offices and at headquarters, and maintain documentation supporting titling and registration transactions.

- **MVA did not use the bank's credit card verification value (CVV) security feature for online customer payments and assigned excessive account permissions for the related banking services (Finding 4).**

  MVA should activate the CVV security feature and restrict permissions on the bank's online service user accounts.

- **A number of security and control deficiencies were noted with respect to MVA's information systems. For example, monitoring and access controls over critical systems were not sufficient, controls over the virtual server environment did not properly protect critical virtual servers, and MVA customers' sensitive personally identifiable information was not properly protected (Findings 5 through 7).**

  MVA should take the recommended actions to address information system security weaknesses.

- **Vehicle registrations were not always suspended for motorists that defaulted on payment plans with the Department of Budget and Management's Central Collection Unit (CCU) for uninsured motorist penalty fees (Finding 8).**

  MVA should ensure that vehicle registrations are suspended for all motorists who default on payment plans with CCU.

- **MVA did not properly procure a contract for facility security upgrades at numerous locations and did not modify the contract and seek Board of Public Works' (BPW) approval for a significant change to the scope of the contract (Finding 9).**

  MVA should comply with State procurement regulations with respect to procuring sole-source contracts and modifying contracts, and prepare a contract modification and seek BPW approval for changes in contract scope, when required.

Background Information

Agency Responsibilities

The Motor Vehicle Administration (MVA) is part of the Maryland Department of Transportation and functions under certain provisions of the Transportation Article of the Annotated Code of Maryland. MVA has jurisdiction over a variety of activities related to the ownership and operation of motor vehicles, including the registration and titling of vehicles. MVA maintains a headquarters location in Anne Arundel County and 24 branch offices in 18 counties and Baltimore City with a total authorized workforce of approximately 1,600 employees. According to MVA records, during fiscal year 2012, MVA's collections totaled $1.4 billion and primarily consisted of motor vehicle excise taxes and vehicle registration fees. According to the State's records, during fiscal year 2012, MVA's operating expenditures totaled $173.8 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the 13 findings contained in our preceding audit report dated October 13, 2010. We determined that MVA satisfactorily addressed 11 of these findings. The remaining two findings are repeated in this report.

Findings and Recommendations

Cash Receipts

Background

The Motor Vehicle Administration (MVA) collects fees and penalties for a variety of activities related to the ownership and operation of motor vehicles including the registration and titling of vehicles, licensing passenger and commercial drivers, and enforcing insurance compliance. MVA also accounts for the related inventory, such as titling and registration documents. Collections are received at the headquarters location in Anne Arundel County and 24 branch offices in 18 counties and Baltimore City that may offer a full range of services or limited, express services. MVA also operates its eStore which provides online services to its customers with connectivity via the Internet and kiosks located at certain shopping centers and branch offices.

According to its records, MVA's fiscal year 2012 collections totaled $1.4 billion. Of this amount, $395.2 million was received as walk-in collections at branch offices and $167 million represented electronic payments received from customers through the eStore.

During our audit, we reviewed cash receipts procedures and controls at three branch offices that had fiscal year 2012 receipts totaling $173 million.

Finding 1
MVA had not established adequate controls to safeguard cash receipts and the related inventory at one branch location reviewed.

Analysis

MVA had not established adequate controls over certain aspects of the cash receipts process and the related stockroom inventory at one branch location. According to MVA records, collections during fiscal year 2012 at this branch location totaled over $141 million and related primarily to walk-in receipts. Specifically, we noted the following conditions:

- Cash receipts were not adequately safeguarded prior to deposit. Although receipts were kept in a safe in a locked cash bag, one employee who processed the related receipts had access to both the safe and the key to the cash bag, which gave this employee unauthorized access to the collections. In addition, the related titling and registration inventory at customer agent workstations was not always adequately safeguarded based on our observations. We noted that critical product inventory (such as certified title paper, vehicle license

plates, and registration stickers) was not secured at three unoccupied workstations on the day observed.

- The employee who processed chargeback transactions for all MVA locations also had access to the related cash receipts at the one branch location. This employee was, therefore, in a position to process a chargeback transaction to conceal a misappropriation. Chargeback transactions occur when the bank does not provide credit for items such as non-sufficient fund checks. According to the State's records, chargeback transactions for all branch offices during our audit period totaled $12.6 million.

- Proper internal controls were not established over inventory at the stockroom. The stockroom inventory included items such as driver's licensing product, vehicle license plates, and registration stickers. The employee who served as the inventory custodian also conducted the related physical inventories. This employee also performed recounts of those inventory items where variances existed between the physical counts and the perpetual inventory records and the reasons for the changes to the physical counts were not documented. Accordingly, this employee was in a position to conceal an unauthorized removal of inventory.

- Employee access to the stockroom was not adequately restricted. MVA established a badge access system for many areas within the branch office, including the stockroom; however, there were 24 employees with access to this stockroom who did not require such access as part of their job responsibilities. Furthermore, 11 of these employees had accessed the stockroom a total of 126 times (ranging up to 65 times per employee) during a five-month period reviewed.

Recommendation 1
We recommend that MVA

a. safeguard collections prior to deposit by restricting employee access;
b. ensure that inventory is secured at all times;
c. ensure that an employee independent of the cash receipts function processes chargeback transactions;
d. ensure that inventory custodians do not perform the related physical inventories, and reasons for changes to physical inventory counts are properly documented; and
e. restrict access to the stockroom based on employee job responsibilities.

We advised MVA on accomplishing the necessary separation of duties using existing personnel.

Finding 2
Documentation was not always maintained to support the propriety of vehicle titling and registration transactions processed by MVA customer agents at branch offices.

Analysis
Documentation of the propriety of vehicle titling and registration transactions processed at branch offices was not always maintained. Our test of daily walk-in transactions processed at three branch offices by 30 MVA customer agents (a single day's activity for 10 agents at each location) totaling $106,000 disclosed the following conditions:

- At two branch offices, documentation supporting system overrides was not always maintained. For the transactions processed by 6 of the 20 customer agents at those locations, 41 of 62 system overrides that required supporting documentation were processed without evidence the applicable documents had been obtained. For example, to override an administrative flag pertaining to an outstanding traffic citation, the customer must provide the agent with evidence of payment from the jurisdiction before the vehicle registration can be renewed. In addition, at the remaining branch office, customer agent closeout reports (which establish accountability over individual customer agent deposit bags that are combined into one larger branch deposit) were not maintained for 4 of the 10 customer agents tested.

- At one branch office, the report generated by supervisors during the closeout process to evidence the required supervisory review of transactions processed by 2 of 10 customer agents was not maintained. MVA policy requires a complete review be performed of at least five percent of the transactions processed by each customer agent to determine the propriety of the transactions. In addition, the policy requires that documentation of these reviews be maintained with the related closeout reports.

Recommendation 2
We recommend that MVA ensure that
a. documentation is maintained to support customer agent system overrides,
b. required supervisory reviews of transactions are performed and documented, and
c. customer agent closeout reports are maintained.

Finding 3
Certain collections received at MVA headquarters for vehicle registration renewals processed at county offices were not adequately controlled.

Analysis
Collections received at MVA headquarters from 12 counties for vehicle registration renewals they processed on behalf of MVA were not adequately controlled. Certain counties, including those that do not have MVA branch offices, have authority under State law to process registration renewals at their county offices and collect the related fees. These counties periodically forward the related fees to MVA by check. These transactions were initially recorded in MVA's Titling and Registration Information System (TARIS) when processed by the counties, but the transactions were not released to update MVA's system detail records until the related checks were received and processed for deposit by MVA. Amounts remitted to MVA by these 12 counties during fiscal year 2012 totaled $3.8 million.

- MVA did not monitor to ensure that the funds and supporting documentation due from the county offices, as reflected in TARIS, were received in a timely manner. Our test of 125 checks, totaling $1,140,855, received during calendar years 2011 and 2012 disclosed that 41 checks, totaling $520,046, were received from 6 to 141 days after the related fees were required to be submitted. State law requires county offices to submit all fees collected, and the related record of registration renewals, at the end of each week. The timely transfer of these funds enhances control over the collections and provides for timely recording of the transactions in MVA's records.

- Checks received from county offices by MVA were not adequately secured prior to deposit and were not recorded and restrictively endorsed immediately upon receipt. For example, on October 25, 2012, we observed unopened envelopes containing county checks that were not secured. At our request and in our presence, these envelopes were opened on October 31, 2012. They contained 17 county checks totaling approximately $105,000. The postmark dates on the envelopes ranged from 7 to 15 days earlier.

- Duties were not segregated in that the same employee who received the county checks was also responsible for performing the daily reconciliation to ensure that such collections received were deposited and properly recorded in MVA's accounting records. Consequently, funds could be misappropriated without timely detection.

Since the majority of these collections are from local jurisdictions, internal controls over the processing of cash receipts could be enhanced by requiring the jurisdictions to submit reimbursements via electronic funds transfer.

Recommendation 3

We recommend that MVA

a. monitor county transactions to ensure that the related collections are received at least weekly by MVA in accordance with State law;

b. secure checks prior to deposit and ensure they are recorded and restrictively endorsed immediately upon receipt;

c. segregate the cash collection, account monitoring, and deposit verification functions; and

d. pursue the use of electronic funds transfer for reimbursements from local jurisdictions.

We advised MVA on accomplishing the necessary separation of duties using existing personnel.

Finding 4

The credit card verification value (CVV) security feature was not used for online customer payments and account permissions for the related banking services were excessive.

Analysis

MVA did not use the credit card verification value (CVV) security feature for customer payments and assigned excessive account permissions for the related banking services. MVA uses an online service provided by an international bank to process credit card transactions for its online systems, including the eStore. The bank maintains a web interface that permits MVA personnel to manage accounts used to administer this online service and implement fraud controls over these operations. Specifically, we noted the following conditions:

- MVA did not request the bank to activate its CVV security feature. Every credit card is issued with either a three or four digit code on the back of the card. This code is frequently required to be entered for online transactions as a security feature designed to prove that the customer has physical possession of the card. However, MVA did not enable this available security feature with the bank. Accordingly, a transaction would process normally when an invalid CVV was entered or when a CVV was not entered during a credit card transaction. Credit card issuers (such as VISA) recommend that the CVV be captured and verified before processing an online transaction.

- Four MVA accounts used to manage the aforementioned bank's online service had excessive permissions. For example, one user account had full administrative access but only required read access to this service. Full administrative access gave this user powerful permissions, including the ability to issue credit card voids, credits, and authorizations. Accordingly, these four users could process unauthorized transactions.

Recommendation 4
We recommend that MVA

a. activate the aforementioned CVV security feature so that any online transaction with an invalid or missing CVV is rejected, and

b. restrict permissions on the bank's online service user accounts to only those permissions required by users to perform their job duties.

Information Systems Security and Control

Background

MVA's Office of Information Resources (OIR) provides information technology services to MVA. OIR staff operates and maintains various applications, servers, and local networks throughout MVA's numerous locations, including the headquarters location and its branch offices located throughout the State. OIR interacts with various contractors that provide information technology related services to MVA. In addition, the Maryland Department of Transportation – Office of Transportation Technology Services operates a mainframe computer for certain MVA applications, such as the Driver Licensing and Point of Sale systems.

Finding 5
Monitoring and access controls were not sufficient.

Analysis

Monitoring and access controls were not sufficient. Specifically, we noted the following conditions:

- A mainframe security report that logged all access violations and direct access to critical production files was only reviewed for access violations. A similar condition was commented upon in our preceding audit report. In addition, the mainframe security report of changes to security software access rules over production files was incomplete as it did not include security software rule changes over production files. As a result of these conditions, any unauthorized or inappropriate changes to critical production files or security software access rules would not have been subject to review.

- Documentation evidencing reviews of critical database security logs did not exist. In addition, four audit events (for example, audit server starts and stops) were not logged. Accordingly, assurance was lacking that these reviews were performed and that all critical audit events were subject to review.

- Seven employees had unnecessary, direct modification access to two critical files used to update drivers' records to reflect the results of various court-related actions (for example, an outstanding arrest warrant), and to update vehicle flag information. Furthermore, seven other employees had unnecessary direct modification access to 23 critical production database tables relating to the Driver Licensing and Point of Sale systems. As a result of these conditions unauthorized changes could be made to these files and tables.

- Eleven employees had unnecessary access to a critical transaction, which was used to add and remove vehicle registration flags (warning indicators for conditions such as vehicle insurance lapses) from MVA records. Consequently, these employees could make unauthorized or erroneous changes that could impact vehicle registrations. A similar condition was commented upon in our preceding audit report.

The State of Maryland Department of Information Technology's (DoIT) *Information Security Policy*, states "Information systems must generate audit records for all security-relevant events, including all security and system administrator accesses." The policy also states that "Procedures must be developed to routinely (for example daily or weekly) review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution." Also, agencies must ensure that only authorized individuals (employees or agency contractors) have access to confidential information and that such access is strictly controlled, audited, and that it supports the concepts of "least possible privilege" and "need to know."

Recommendation 5

We recommend that MVA

a. review all direct accesses to critical production files recorded on its mainframe security reports for propriety, investigate all suspicious or unusual entries, document these reviews and investigations, and retain this documentation for subsequent verification (repeat);

b. include security software rule changes over production files in its mainframe security reports;

c. perform and document reviews of critical database security logs, retain this documentation for subsequent verification, and log all critical audit events;

d. restrict direct file modification access to critical production data files and database tables to only those employees who require such access for their job duties; and

e. limit use of critical transactions to only those employees who require such use for their job duties (repeat).

Finding 6
Controls over the virtual server environment did not properly protect critical virtual servers.

Analysis

Controls over the virtual server environment did not properly protect critical virtual servers. Specialized software developed in recent years allows for a single physical host server's resources (that is, memory, CPU, and storage) to be defined and subdivided into multiple virtual servers which can each operate as a separate, unique server. As of December 2012, MVA was using 11 physical host servers to host 116 virtual servers that supported the critical eStore system. Our tests disclosed the following conditions:

- Certain security options on the host servers' virtualization software were not properly configured in accordance with the software vendor's recommended security settings. As a result, this weakened network level security for the virtual servers configured on the hosts. A similar condition was commented upon in our preceding audit report.

- Six publicly-accessible virtual servers were included in a network segment with three nonpublic host servers rather than being isolated in a separate network segment. Consequently, these six publicly accessible virtual servers, if compromised, could be used to attack the three host servers and their hosted virtual servers. The National Institute of Standards and Technology's Guide to Security for Full Virtualization Technologies recommends that host servers be separate from all other networks and only accessible by authorized administrators. A similar condition was commented upon in our preceding audit report.

- Seven accounts (assigned to three contractors and one MVA employee) had unnecessary administrative access to MVA's virtual server environment. As a result, these accounts had unnecessary administrative access to physical host servers and virtual servers and could make unauthorized changes to these servers. The DoIT *Information Security Policy* states that agencies must ensure that only authorized individuals have access to confidential

information and that such access is strictly controlled, audited, and that it supports the concepts of "least possible privilege" and "need to know."

- The configurations of the 11 host servers used for eStore operations were not backed up. In the event of a problem which would destroy or corrupt these servers, all copies of their configurations could be lost. Such a problem could result in significant delays (of an undetermined period of time) in restoring MVA's information systems above and beyond the expected delays that would exist if secure backups of the aforementioned configurations were readily available. The State of Maryland *Information Technology Disaster Recovery Guidelines* state that configuration files should be backed up and the backup media stored in a secure, environmentally controlled location. A similar condition was commented upon in our preceding audit report.

Recommendation 6
We recommend that MVA

a. configure the software on its host servers to help ensure adequate security over the resident virtual servers (repeat),
b. locate its host servers and publicly accessible servers in separate network segments and appropriately restrict access to these segments (repeat),
c. restrict administrative access to the virtual server environment to individuals whose job duties require such access, and
d. regularly backup its host servers' configurations and store those backup files at an offsite, secure, environmentally controlled location (repeat).

Finding 7
MVA customers' sensitive personally identifiable information was not properly protected.

Analysis
MVA customers' sensitive personally identifiable information was not properly protected. Specifically, we noted that the MVA Driver Licensing and Point of Sale systems' databases contained numerous MVA customer records in clear text. These records frequently contained the customer's name, driver's license number, and social security number. For example, as of January 31, 2013, one Driver Licensing system database table contained full names in clear text and 5,855,210 unencrypted drivers' license numbers and 5,405,419 unencrypted social security numbers. The earliest records in this table date back to November 1993.

This sensitive personally identifiable information is commonly sought for use in identity theft. Accordingly, appropriate information system security controls need to exist to ensure that this information is safeguarded and not improperly disclosed. Also, the DoIT *Information Security Policy* requires that confidential

information be protected with administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

Recommendation 7
We recommend that for the Driver Licensing and Point of Sale databases, MVA only retain needed sensitive personally identifiable information and encrypt the remaining records using approved encryption algorithms.

Insurance Compliance

Finding 8
Vehicle registrations were not always suspended for motorists that defaulted on payment plans with the Department of Budget and Management's Central Collection Unit for uninsured motorist penalty fees.

Analysis
Vehicle registrations were not always suspended for motorists who defaulted on payment plans with the Department of Budget and Management's Central Collection Unit (CCU) for uninsured motorist penalty fees. MVA is notified of these defaulted payments by CCU so that a registration flag can be placed on the motorist's driving record. A registration flag suspends the current registration, making it illegal for the vehicle to be driven, and prevents the issuance or renewal of a registration for any vehicle that is owned or co-owned by the motorist. According to CCU records, there were 1,674 defaulted installment plans related to uninsured motorist penalty fees during the month of July 2012, which were applicable to approximately 1,500 motorists. Our test of 10 of these motorists with outstanding balances totaling $6,189 disclosed that driving records were not flagged as of April 2013 for 5 of these motorists with outstanding balances totaling $3,423. One of these motorists was also able to renew the vehicle registration after defaulting on the payment.

Based on discussions with CCU and MVA management, the failure to suspend vehicle registrations by placing a registration flag on the driving record could be related to the manner in which defaulted payment plans are reported by CCU and interfaced with MVA records, particularly with respect to motorists who have more than one account with CCU.

State law authorizes MVA to assess a penalty fee when a vehicle's insurance terminates or otherwise lapses during the registration period, unless documentation is provided that justifies the lack of coverage. The penalty fee assessed is $150 for each uninsured vehicle for a period of 1 to 30 days and,

thereafter, an additional $7 per day; the maximum penalty is $2,500 for a 12-month period. MVA suspends the registrations of those vehicles for which lapses are reported until the required coverage is obtained, the motorist submits related supporting documentation to MVA, and any assessed penalty fee is paid. If proof of insurance has been provided but the penalty fee cannot be paid in full, the vehicle suspension will be lifted provided the vehicle owner enters into a payment plan with CCU. However, if a motorist defaults on his or her payment plan, MVA policy requires that a registration flag be reinstated on the motorist's driving record. According to CCU records, during fiscal year 2012, MVA had referred $119.4 million in uninsured motorist penalty fees to CCU for collection assistance.

Recommendation 8
We recommend that MVA

a. investigate the cause of the aforementioned reporting and interface problems and take appropriate corrective action; and
b. in consultation with CCU, immediately flag driving records and suspend vehicle registrations for all motorists who are currently in default on payment plans.

Contract Procurement and Monitoring

Finding 9
MVA did not properly procure a contract for facility security upgrades at numerous locations and did not modify the contract and seek Board of Public Works' approval for a significant change to the scope of the contract.

Analysis
MVA did not properly procure a contract for facility security upgrades at numerous locations and did not modify the contract and seek Board of Public Works' (BPW) approval for a significant change to the scope of the contract. The sole-source contract, approved by BPW, provided for facility security upgrades at 13 locations and covered the period from May 5, 2011 through December 31, 2012, at a total cost of approximately $2.3 million. Our review of the procurement and related payments for these security upgrades disclosed the following conditions:

- MVA's justification for using the sole-source procurement method for this contract did not appear adequate. The sole-source justification stated that this was the only vendor with the required software license and installation expertise to provide the security upgrades. However, we found that this software was publicly available. Also, MVA lacked evidence of any efforts to

determine the availability of other vendors for the services. We noted that another vendor subsequently performed these upgrades at certain branch locations.

- MVA did not modify the contract and seek BPW approval for a significant change in the scope of the contract, as required by State procurement regulations and a BPW advisory. Specifically, upgrades at five locations were postponed; however, $100,000 in funds originally allocated for these locations was used for additional upgrades at one of the approved locations where work had already been performed. We confirmed with BPW personnel that this represented a significant change in scope that should have been submitted for approval. Upgrades at two of the locations where work was postponed were subsequently performed under separate contracts, and MVA management advised us that it intends to perform the upgrades in the future at the three remaining locations. As of July 1, 2013, in addition to the costs paid to date of $2.3 million for the original contract, MVA anticipates it will cost $195,000 to complete the upgrades at these five locations.

According to State procurement regulations, a sole-source procurement is permissible when only one source exists which meets the requirements. The use of a contract to perform work outside of the contract scope without requesting BPW approval violates State procurement regulations which require contract modifications that significantly change the scope, amount, or any cost component of a contract by more than $50,000 to be submitted to BPW for approval. In addition, a BPW advisory states that a contract modification that changes a cost component by more than $50,000 must be submitted to BPW for approval including when components are modified or deleted, and the associated funds are shifted to increase other components or offset other contract expenditures.

Recommendation 9
We recommend that MVA

a. comply with State procurement regulations with respect to procuring sole-source contracts and modifying contracts, and

b. prepare a contract modification and seek BPW approval for the aforementioned change in contract scope, as required.

Audit Scope, Objectives, and Methodology

We have audited the Maryland Department of Transportation– Motor Vehicle Administration (MVA) for the period beginning July 10, 2009 and ending July 24, 2012. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine MVA's financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations. We also determined the status of the findings contained in our preceding audit report.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. The areas addressed by the audit included the titling and registration, licensing, license revocation, and insurance compliance processes, as well as procurements and disbursements for MVA's operating expenditures, payroll, cash receipts, and information systems security.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of MVA's operations, and tests of transactions. We also performed various data extracts of pertinent information from the State's Financial Management Information System and the Maryland Department of Transportation's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were sufficiently reliable for the purposes the data were used during this audit. In addition, we performed various data extracts of pertinent information from MVA systems. For example, we extracted data from MVA's Titling and Registration Information System for the purpose of testing vehicle titling and registration transactions and related cash receipts. We also extracted data from MVA's Automated Compulsory Insurance System for the purpose of testing insurance compliance processes. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the

purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our objectives. The reliability of data used in this report for background or informational purposes was not assessed.

Our audit did not include certain payroll support services provided by the State Highway Administration to MVA. These payroll support services are included within the scope of our audit of the State Highway Administration.

Our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of MVA's compliance with federal laws and regulations pertaining to those programs because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including MVA.

MVA's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect MVA's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to MVA that did not warrant inclusion in this report.

The Maryland Department of Transportation's response, on behalf of MVA, to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the Department regarding the results of our review of its response.

APPENDIX

Maryland Department of Transportation
The Secretary's Office

Martin O'Malley
Governor

Anthony G. Brown
Lt. Governor

James T. Smith, Jr.
Secretary

May 12, 2014

Thomas J. Barnickel, III, CPA
Legislative Auditor
Department of Legislative Services
Office of Legislative Audits
301 West Preston Street
Room 1202
Baltimore MD 21201

Dear Mr. Barnickel:

Enclosed please find the Maryland Department of Transportation's (MDOT) responses to the draft Legislative Auditor's Report dated April 2014 for MDOT- Motor Vehicle Administration (MVA) for the period July 10, 2009, to July 24, 2012. Additionally, an electronic version of this document was sent to your office via e-mail (file name: MVAFinalResponseDraftReportApril2014) to response@ola.state.md.us.

If you should have any questions regarding these responses, please do not hesitate to contact Mr. David L. Fleming, Chief Financial Officer, MDOT, at 410-865-1035, toll-free 888-713-1414 or via email at dfleming@mdot.state.md.us.

Sincerely,

James T. Smith Jr.
Secretary

Enclosure

cc: Mr. Rick A. Bilenky, Chief Internal Auditor, MVA
Ms. Brenda Cachuela, Director, Office of Audits, MDOT
Mr. Milton Chaffee, Administrator, Motor Vehicle Administration
Mr. David L. Fleming, Chief Financial Officer, Office of Finance, MDOT
Mr. Pretam Harry, Financial Services Director, MVA
Ms. Karen Howes, Senior Auditor, Office of Legislative Audits
Ms. Christine Nizer, Chief Deputy Administrator, MVA
Mr. Richard Norman, Acting Deputy Administrator Field Operations, MVA
Mr. Wilson Parran, Deputy Secretary for Administration and Operations, MDOT
Mr. Al Short, Chief Information Officer, MVA

Maryland Department of Transportation
Motor Vehicle Administration
Draft Audit Report Responses
Period July 10, 2009 to July 24, 2012

Cash Receipts

Finding 1
MVA had not established adequate controls to safeguard cash receipts and the related inventory at one branch location reviewed.

Recommendation 1
We recommend that MVA

a. safeguard collections prior to deposit by restricting employee access;
b. ensure that inventory is secured at all times;
c. ensure that an employee independent of the cash receipts function processes chargeback transactions;
d. ensure that inventory custodians do not perform the related physical inventories, and reasons for changes to physical inventory counts are properly documented; and
e. restrict access to the stockroom based on employee job responsibilities.

We advised MVA on accomplishing the necessary separation of duties using existing personnel.

Response:
The Administration concurs with the auditor's recommendations and has done the following:
For items 1a, 1b, 1d, and 1e, a verbal directive reinforcing supervisors responsibilities concerning documenting all random checks and reviews was given in March 2014. This was followed up with a bulletin dated May 7, 2014.

a. Separations of duties have been reinforced at all branch locations to safeguard all deposits prior to scheduled pickup.
b. Branch Managers, Assistant Managers and supervisors are conducting random checks of work stations to ensure inventory is secured at all times. The checks are documented and retained for audit purposes.
c. Effective April 11, 2013, the employee has been relieved of her responsibilities as backup head cashier and has no access to any cash receipts. Therefore, she is now independent of the cash receipt function.
d. Separation of duties has been outlined in each branch to prevent inventory custodians from performing inventories and changes in inventory levels are properly documented.
e. We have restricted access to stockrooms to only those employees whose job responsibilities requires access. In addition, we have asked our District Managers and Statewide Compliance team to conduct random checks of the above items. The random checks are documented and retained for audit purposes. This process is in effect as of March 1, 2014.

Maryland Department of Transportation
Motor Vehicle Administration
Draft Audit Report Responses
Period July 10, 2009 to July 24, 2012

Cash Receipts

Finding 2
Documentation was not always maintained to support the propriety of vehicle titling and registration transactions processed by MVA customer agents at branch offices.

Recommendation 2
We recommend that MVA ensure that
a. documentation is maintained to support customer agent system overrides,
b. required supervisory reviews of transactions are performed and documented, and
c. customer agent closeout reports are maintained.

Response:
The Administration concurs with the auditor's recommendations and has done the following:
a. Managers, Assistant Managers and Supervisors were given a verbal directive regarding the importance of maintaining documentation on all customer agent overrides. A follow-up bulletin was sent on May 7, 2014.
b. Managers, Assistant Managers and Supervisors were reminded via a verbal directive of the importance of completing all required transaction reviews and maintaining proper documentation. A follow-up bulletin was sent on May 7, 2014.
c. Managers, Assistant Managers and Supervisors were reminded of the importance of completing all customer agent closeouts via a verbal directive. In addition, we have asked our District Managers to perform random reviews to ensure all documentation is accounted for and the supervisory reviews are taking place as required. The reviews and documented and retained for audit purposes. Our Statewide Compliance team has also included in their audits a review of all required documentation and review that proper retention of closeout reports is being maintained. A follow-up bulletin was sent on May 7, 2014.

Cash Receipts

Finding 3
Certain collections received at MVA headquarters for vehicle registration renewals processed at county offices were not adequately controlled.

Recommendation 3
We recommend that MVA
a. monitor county transactions to ensure that the related collections are received at least weekly by MVA in accordance with State law;
b. secure checks prior to deposit and ensure they are recorded and restrictively endorsed immediately upon receipt;
c. segregate the cash collection, account monitoring, and deposit verification functions; and
d. pursue the use of electronic funds transfer for reimbursements from local jurisdictions.

We advised MVA on accomplishing the necessary separation of duties using existing personnel.

Response:
The Administration concurs with the auditor's recommendations.

a. The MVA corresponded on February 6, 2013 with the four County Treasurer's offices that were late in remitting funds, requesting the counties to comply with the Annotated Code of Maryland Section 13-404b(2). Specifically, that all fees collected and the related record of registrations made for each day be transmitted to MVA at the end of each week. Of the four County Treasurer's offices that were late in remitting funds, three out of four are now in compliance. Furthermore, by July 1, 2014, additional correspondence will go out under the Administrator's signature emphasizing the timely remittance of funds. MVA will continue to monitor County Treasurer offices' timely remittance of funds.
b. The Administration will ensure that checks are recorded and restrictively endorsed upon receipt. Effective September 4, 2013, a secured cabinet is being utilized to secure endorsed checks prior to deposit.
c. Procedures were put in place in September 2013 to improve the review of cash receipts, the verification of deposits, and the reconciliation to FMIS in a timely manner. The procedure includes the printing of the reconciliation document, and affixing the preparer's signature and date. Duties have been properly segregated with regard to this process. One employee prepares the check register, while another employee deposits the checks, and a third employee posts to the account.
d. The MVA will contact the 12 active jurisdictions by July 1, 2014, to determine the feasibility of having all funds transferred electronically.

Cash Receipts

Finding 4
The credit card verification value (CVV) security feature was not used for online customer payments and account permissions for the related banking services were excessive.

Recommendation 4
We recommend that MVA

a. activate the aforementioned CVV security feature so that any online transaction with an invalid or missing CVV is rejected, and
b. restrict permissions on the bank's online service user accounts to only those permissions required by users to perform their job duties.

Response:
The Administration concurs with the auditor's recommendations and has taken the following actions:

a. As of October 2013, MVA implemented changes to the eStore to enable CVV policy failure codes on its related banking services PCG merchant accounts to reject any credit card transaction with an invalid or missing CVV.
b. As of August 2013, MVA restricted critical privileges on its related banking services PCG user accounts to only those users who required privileges to perform their job duties.

Information Systems Security and Control

Finding 5
Monitoring and access controls were not sufficient.

Recommendation 5
We recommend that MVA

a. review all direct accesses to critical production files recorded on its mainframe security reports for propriety, investigate all suspicious or unusual entries, document these reviews and investigations, and retain this documentation for subsequent verification (repeat);
b. include security software rule changes over production files in its mainframe security reports;
c. perform and document reviews of critical database security logs, retain this documentation for subsequent verification, and log all critical audit events;
d. restrict direct file modification access to critical production data files and database tables to only those employees who require such access for their job duties; and
e. limit use of critical transactions to only those employees who require such use for their job duties (repeat).

Response:
The Administration concurs with the auditor's recommendations and has taken the following actions:

a. MVA established a process to ensure there is a record of accesses to critical production data and program files. This has been accomplished as of December 31, 2013, by reviewing the access log entries for these MVA critical production data and program files on a daily basis. The process and the review is documented and retained.
b. The program code for the rule changes report over MVA datasets was corrected in December 2012.

c. Since 2010, MVA had been reviewing the logs, however proper documentation of the review was not consistent. MVA reviewed the process and procedures and has implemented a documented review process as of July 1, 2013. On a monthly basis, MVA Management will confirm logs are being reviewed.
d. As of August 2013, MVA and OTTS immediately reviewed the list of users and removed access from all the users noted.
e. As of August 2013, MVA and OTTS reviewed the list of users and all the users were removed from these 2 groups. MVA and OTTS will implement by July 2014 a process to periodically review the list. The reviews will be documented and retained for audit purposes.

Information Systems Security and Control

Finding 6
Controls over the virtual server environment did not properly protect critical virtual servers.

Recommendation 6
We recommend that MVA
a. configure the software on its host servers to help ensure adequate security over the resident virtual servers (repeat),
b. locate its host servers and publicly accessible servers in separate network segments and appropriately restrict access to these segments (repeat),
c. restrict administrative access to the virtual server environment to individuals whose job duties require such access, and
d. regularly backup its host servers' configurations and store those backup files at an offsite, secure, environmentally controlled location (repeat).

Response:
The Administration concurs with the auditor's recommendations and has taken the following actions:
a. Previously recommended changes were not applied to the new eStore environment. This was due to the negligence of a vendor employee hired to support the virtualization infrastructure. Once deficiencies with the vendor employee's performance were identified, MVA took swift action to have the individual's duties removed. As of October 2013, all recommended changes were reapplied and additional procedures were put in place.
b. MVA applied the recommended changes as of September 2013. Again, this was due to the negligence of a vendor hired to support the virtualization infrastructure.
c. MVA created a new security group in September 2013 and only appropriate users have been added to the new group. MVA users have access to only the MVA environment.

d. The four internal eStore servers are identically configured. MVA is currently backing up 2 of the 4 servers in an effort to conserve space. The backup agent will be installed on the other 2 servers by October 2014.

Information Systems Security and Control

Finding 7
MVA customers' sensitive personally identifiable information was not properly protected.

Recommendation 7

We recommend that for the Driver Licensing and Point of Sale databases, MVA only retain needed sensitive personally identifiable information and encrypt the remaining records using approved encryption algorithms.

Response:

The Administration concurs with the auditor's recommendation.

MVA only retains needed information that is required to perform its business functions. MVA will implement FIPS-140-2 approved encryption algorithms for storage of sensitive personally identifiable information as part of a planned 2015 database server upgrade.

Insurance Compliance

Finding 8
Vehicle registrations were not always suspended for motorists that defaulted on payment plans with the Department of Budget and Management's Central Collection Unit for uninsured motorist penalty fees.

Recommendation 8

We recommend that MVA

a. investigate the cause of the aforementioned reporting and interface problems and take appropriate corrective action; and
b. in consultation with CCU, immediately flag driving records and suspend vehicle registrations for all motorists who are currently in default on payment plans.

Response:

The Administration concurs with the auditor's recommendations.

a. An investigation was conducted regarding the five (5) vehicle registrations that were not flagged for CCU. During the July 2012 time frame, CCU flags were sent weekly and due to the timing of the July 4th holiday, the new records to be flagged were sent one day earlier on a Tuesday and as a result were not processed. The file was over written on the CCU server by their next add file. As of July 16, 2012, all CCU flags are processed, archived and backed-up daily. If no file is received, an e-mail is sent to CCU that no file is present for processing.
b. Effective January 27, 2014, system enhancements were completed to ensure all appropriate action is taken with regard to a default CCU payment. The CCU notifies the MVA that a payment plan is in default. The MVA immediately suspends the vehicle registrations and generates a notification to the customer.

Contract Procurement and Monitoring

Finding 9
MVA did not properly procure a contract for facility security upgrades at numerous locations and did not modify the contract and seek Board of Public Works' approval for a significant change to the scope of the contract.

Recommendation 9

We recommend that MVA

a. comply with State procurement regulations with respect to procuring sole-source contracts and modifying contracts, and
b. prepare a contract modification and seek BPW approval for the aforementioned change in contract scope, as required.

Response:

The Administration concurs with the auditor's recommendations.

a. The MVA will follow the State procurement regulations regarding sole-source contracts and contracts modifications.
b. The MVA will prepare a contract modification to the current Alarm Services contract and seek BPW approval on or around July 31, 2014, that specifically addresses facility upgrade work and ancillary work.

AUDIT TEAM

William R. Smith, CPA
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

Karen J. Howes
Senior Auditor

Eric Alexander, CPA
Information Systems Senior Auditor

Megan A. Axenfeld
Mary K. Davis, CPA
Jaime A. DeWitt
Erin D. Erdley, CPA
Michael A. Klausmeier
Kelly M. McNemar, CPA
Staff Auditors