



**New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor**

**Motor Vehicle Commission
Data Security**

May 15, 2013 to June 30, 2014

**Stephen M. Eells
State Auditor**



LEGISLATIVE SERVICES COMMISSION

ASSEMBLYMAN
VINCENT PRIETO
Chairman

SENATOR
THOMAS H. KEAN, JR.
Vice-Chairman

SENATE

CHRISTOPHER J. CONNORS
NIA H. GILL
ROBERT M. GORDON
JOSEPH M. KYRILLOS, JR.
JOSEPH PENNACCHIO
STEPHEN M. SWEENEY
LORETTA WEINBERG

GENERAL ASSEMBLY

JON M. BRAMNICK
ANTHONY M. BUCCO
JOHN J. BURZICHELLI
THOMAS P. GIBLIN
LOUIS D. GREENWALD
ALISON LITTELL MCHOSE
SCOTT T. RUMANA

OFFICE OF THE STATE AUDITOR
(609) 847-3470
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

GREGORY PICA
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES

OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

DAVID J. ROSEN
Executive Director
(609) 847-3901

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Vincent Prieto
Speaker of the General Assembly

Mr. David J. Rosen
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Motor Vehicle Commission, Data Security for the period of May 15, 2013 to June 30, 2014. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
March 16, 2015

Table of Contents

Scope.....	1
Objectives	1
Methodology.....	1
Conclusions.....	2
Findings and Recommendations	
Data Integrity	3
Social Security Numbers – Deceased Individuals	4
Invalid Social Security Numbers	5
Non-Expiring Licenses and Identifications	5
Incomplete Records	6
Corporate Records	6
Duplicate Social Security Numbers	7
General Controls	8
Auditee Response.....	9

Scope

We have completed an audit of Data Security for the Motor Vehicle Commission (MVC) for the audit period May 15, 2013 to June 30, 2014. We reviewed data security, data integrity, and selected information technology general controls that we considered necessary for data security.

The MVC relies on the Office of Information Technology (OIT) for much of its network infrastructure, as well as for select general controls such as logical domain access and physical security. However, IT Circular Letter 08-01-NJOIT - Information Security Program states, "Each Agency has ultimate responsibility for the protection of its information from disclosure, loss or misuse. As such, each agency must maintain thorough knowledge of these assets and understand and manage risks associated with the use of these assets." Therefore, all data security issues found during the audit are being reported to the MVC in either this report or a management letter which will be issued in conjunction with this report. The MVC should work with relevant OIT personnel to address our recommendations.

The MVC was in the process of replacing the existing Comprehensive (COMP) system which handles almost all motor vehicle transactions. The replacement, the Motor Vehicle Automated Transaction (MATRX) system, did not have an implementation date that was within reasonable proximity to the audit period and, as reported in our separate report *Motor Vehicle Commission, Revenue*, dated December 22, 2014, has had production suspended. Therefore, the scope of our audit specifically excludes the MATRX system. The data security issues in the report and management letter need to be addressed in the context of the current system and architecture because the risks cannot remain outstanding during the time frame needed to implement MATRX.

Objectives

The objective of this audit was to determine the adequacy of controls in place to protect the confidentiality, integrity, and availability of confidential data and other resources owned by the MVC.

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

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

In preparation for our testing, we studied legislation, MVC and statewide policies and procedures, internal technology documentation, and industry and government standards for computer security and operation. Provisions we considered significant were documented and compliance was verified by interviews of key personnel, observations, access to the MVC's information technology resources, and performance of tests we considered necessary.

A non-statistical sampling approach was used. Our samples were designed to provide conclusions on our audit objectives as well as internal controls and compliance. Sample items were judgmentally selected for testing.

Additional guidance for the conduct of the audit was taken from the *Federal Information Systems Control and Audit Manual (FISCAM)* issued by the Government Accountability Office, benchmarks issued by the Center for Internet Security, *Control Objectives for Information and Related Technology (COBIT)*, and the International Organization for Standardization's *ISO/IEC 27002:2005*, which is utilized by the OIT as their standard for security practice.

Conclusions

The MVC recognizes the importance of data security in their organization and has implemented controls to maintain the confidentiality, integrity, and availability of the confidential data and other resources they own. However, we noted certain control weaknesses requiring management's attention that, if remedied, would strengthen the data security control environment.

The audit found conditions meriting management's attention within controls over select areas of data security operations and within associated general controls that were deemed confidential to the MVC. These items were communicated in detail under a separate cover that was provided only to MVC management and appear in this report in summary form only. Although these items are not included in this report, they are still subject to a post-audit compliance review by the State Auditor as set forth in Title 52:24-4 of the New Jersey Statutes.

Data Integrity

Data integrity is defined as the accuracy and consistency of stored data. Data integrity is imposed within a database at its design stage through the use of standard rules and procedures and is maintained through the use of error checking and validation routines. Our audit procedures focused specifically on the Driver Owner database, which is one of the primary databases in the Comprehensive (COMP) system and contains all records related to individuals and businesses that either have a MVC license of some type, are a vehicle owner, or have committed a motor vehicle violation in the state.

Because of the eventual implementation of the MATRX system, our audit work focused primarily on the existing data at rest in the COMP system databases. Select error checking and validation routines that currently exist in the COMP system were tested, where appropriate, to verify issues found in the data at rest. This data will eventually be migrated into the MATRX system databases, so integrity issues with the current data should be addressed now to avoid migrating erroneous or incomplete data into the new application.

Our analysis of the Driver Owner database found 8,373,621 active records, which are defined as records that are all of the following: complete, not designated as deceased or canceled, not corporate records, and having an expiration date after the date of the data extract obtained from the MVC. This total consists of 5,905,228 automobile drivers license records; 2,126,851 identification, owner-only, and violator-only records; 261,056 commercial drivers license records; 76,479 drivers permit records; 3,123 handicap identification records; 552 moped-only license records; 216 motorcycle-only license records; and 116 agricultural machinery-only license records.

According to the MVC, an automated check of the validity of the Social Security number (SSN) for individuals with a license or identification document was implemented in November 2003. All records that existed in the COMP system prior to that date were matched with the Social Security Administration's (SSA) records off-line and their validity flagged in the COMP system based on the results. From November 2003 to August 2005, the COMP-to-SSA check was optional and had to be manually initiated by an MVC employee. Since 2005, license and identification documents are issued only after a real-time automatic check of the SSN is done to the SSA database. Based on the result of this check, the record is labeled as valid or invalid. The MVC has the ability to override an invalid result based on further evidence. The SSA verification check that is run on a SSN is done the first time the number is entered into the COMP system, and is not rechecked periodically. Therefore, once a SSN is validated, it is not re-verified each time a license is renewed, nor is a periodic check done to identify invalid SSNs. Specific reportable conditions follow.

Social Security Numbers – Deceased Individuals

The Driver Owner database contains active records with Social Security numbers belonging to deceased individuals.

We performed an independent match from the Driver Owner database to the Social Security Administration's (SSA) VERIS system and found 6,814 licenses or identification documents that were issued and recorded in the COMP database where the SSN was reported by the VERIS system as belonging to a deceased individual. These records were classified in four different categories based on two factors: whether the last name on the Driver Owner database record matched the VERIS system record for the same SSN and whether the date of issue was before or after the date of the individual's death as reported by the VERIS system. The following were the results.

- There were 5,844 documents issued where the last name on the Driver Owner database record matched the VERIS system record and the date of issuance was prior to the VERIS system record date of death.
- There were 644 documents issued where the last name on the Driver Owner database record did not match the VERIS system record and the date of issuance was prior to the VERIS system record date of death.
- There were 56 documents issued where the last name on the Driver Owner database record matched the VERIS system record and the date of issuance was after the VERIS system record date of death.
- There were 270 documents issued where the last name on the Driver Owner database record did not match the VERIS system record and the date of issuance was after the VERIS system record date of death.

The effect of each of these categories is slightly different, though in all cases there is an increased risk that a license or identification document may be in the hands of someone other than the intended person. Of greater concern are the license and identification records issued after the date of death.

Recommendation

We recommend the following.

- Driver Owner database records where the last name matches and the date of issuance was before the date of death should be flagged as deceased.
- Driver Owner database records where the last name does not match and the date of issuance was before the date of death should be investigated by the MVC and labeled as deceased if necessary.

- Driver Owner database records where the name matches and the date of issuance was after the date of death should be investigated to determine if licenses are being maintained for deceased individuals.
- Driver Owner database records where the last name does not match and the date of issuance is after the date of death should be investigated to determine if a false document was issued and these records turned over to the Division of Criminal Justice, if necessary.
- The Driver Owner database be rechecked periodically.

»»<<««

Invalid Social Security Numbers

The Driver Owner database contains active records with invalid Social Security numbers.

Our analysis of the active records in the Driver Owner database found 1,364 records where the Social Security number (SSN) was invalid per our independent match with the VERIS system and is not associated with an individual reported as deceased. Of these records, 953 had SSNs that were overridden by MVC personnel to validate the SSN, 34 records have not been validated by the MVC, 11 records were previously labeled in the database as valid, and 366 records were flagged as invalid in the Driver Owner database. Based on our discussions with MVC personnel, any record that returns an invalid SSN flag will not allow a document to be issued.

License or identification documents tied to invalid SSNs weaken the integrity of the data and increase the risk of a fraudulent document being issued. MVC overrides of SSNs that return as invalid could also increase this risk.

Recommendation

We recommend the MVC validate the 34 records that have not been validated and review the 953 overridden records as well as the 11 records currently returned as valid. Records found to be incorrectly overridden should be corrected.

»»<<««

Non-Expiring Licenses and Identifications

The Driver Owner database contains license or identification records that do not expire.

Our analysis of the active records in the Driver Owner database found 32 records with no expiration date. Of these, 30 are identification documents, one has no vehicle class and may be a driver permit, and one is an automobile drivers license. Discussions with MVC personnel

revealed that all license and identification documents should have an expiration date with a maximum of four years.

License or identification documents that do not expire increase the risk of the documents containing incorrect information, bypassing data integrity controls, or being used fraudulently.

Recommendation

We recommend the MVC investigate the 32 records with no expiration date and cancel the associated documents if necessary.



Incomplete Records

The Driver Owner database contains records that should be expunged from the database.

Our analysis disclosed 1,688,311 incomplete records in the database which exist because of a conversion error from the previous system 25 years ago. Records that were not properly converted were labeled as “VIOLATOR ONLY – NO D/L” in the name field. For many of these records, the only information was the drivers license number. It was thought these records could be repopulated as individuals came in to renew documents or perform other tasks. Analysis of these records found that they belong to either non-license documents or expired license documents.

Incomplete or inaccurate records increase the risk of duplicate records existing in the database, increase the storage space needed and, with the development of the replacement for the COMP system, would increase the chance of a conversion error to the new system because of possible data validation rules in the new system.

Recommendation

We recommend the MVC expunge the 1,688,311 incomplete records from the Driver Owner database prior to migrating to the new system.



Corporate Records

The Driver Owner database contains corporate records without valid Employer Identification numbers.

There are 725,264 active corporate records in the Driver Owner database that appear to have the company’s Employer Identification number (EIN) in the SSN field. Based on a match to known valid EIN prefixes, we found that 621,321 of these records contained an invalid EIN number.

Of the 725,264 records, almost all had a SSN value flag in the database indicating the record had not been validated, and the remaining records had an SSN value flag indicating that the field was overridden by the MVC. The current MVC SSA validation process is only able to validate an individual's SSN, and does not include EIN numbers. The MVC has not performed an independent match to valid EIN prefixes to identify this issue. Incorrect or fraudulent information in the database increases the risk that an unauthorized document could be issued.

Recommendation

We recommend the MVC perform a match of the EIN numbers in the corporate records to a reliable reference to identify companies registered with the MVC under an invalid EIN and investigate these exceptions.



Duplicate Social Security Numbers

The Driver Owner database contains multiple records with the same Social Security number and vehicle class.

The Driver Owner database contains active records with a SSN that is duplicated on at least one other record of the same vehicle class. There were 1,070 records associated with a SSN that was duplicated only once and the license class is the same on both records. Of these, 564 were automobile drivers license records, 352 were identification records, 152 were permit records (no license class), and 2 were commercial license records. There were also 1,594 records associated with a SSN that was duplicated more than twice and the license class is the same on at least two of the records. Of these records, 1575 were owner or violator-only records and 19 were automobile drivers licenses.

Although the check against the SSA is performed to test the validity of the SSN, the SSN does not represent a unique field which cannot be repeated in multiple records. As such, the COMP system does not currently check existing records for a matching SSN. Multiple unique records with the same license class and SSN, but a different drivers license number, could indicate that one person may be in possession of two unique drivers licenses or identification cards, or that more than one individual has a unique drivers license or identification card that is tied to the same Social Security number. Either of these situations increases the risk of fraudulent licenses being issued and impacts the integrity of the database.

Recommendation

We recommend that the MVC investigate the records that share a SSN to determine if one or more of the records can be canceled. In addition, the new MVC system should perform real-time checks for duplicate SSNs, or the MVC should perform this analysis outside the system on a periodic basis.



General Controls

The Motor Vehicle Commission does not have a business continuity plan for the Trenton Office Complex and field offices.

The MVC does not have a business continuity plan (BCP) which covers the MVC's Trenton Office Complex and field offices. A BCP should be developed to restore critical functions, including arrangements for alternative processing facilities in case the regular facilities are significantly damaged or cannot be accessed. Agency-level policies and procedures define the contingency planning process and documentation requirements. Furthermore, an entity-wide plan should identify critical systems, applications, and any subordinate or related plans. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations.

The MVC's IT operations were once under the Department of Transportation, who handled both the disaster recovery and business continuity planning. The MVC is no longer part of the department, and their IT hardware has been moved to the Department of the Treasury, Office of Information Technology, who handles the disaster recovery aspect only. The MVC has recently completed a Request for Proposal for a full risk assessment from which to develop the BCP.

In the event of an incident, although the hardware and applications should be restored successfully, the disruption of service would be longer than necessary without a proper BCP in place to guide MVC staff and operations.

Recommendation

We recommend the MVC continue the steps toward completing the BCP in order to prevent a disruption of services if an incident were to occur.

»»<<««



New Jersey Motor Vehicle Commission

P.O. Box 160
Trenton, New Jersey 08666-0160

STATE OF NEW JERSEY

Chris Christie
Governor

Kim Guadagno
Lt. Governor

Raymond P. Martinez
Chairman and Chief Administrator

March 3, 2015

Mr. Stephen Eells
State Auditor
Office of the State Auditor
P.O. Box 167
Trenton, New Jersey 08625-0067

Dear Mr. Eells:

The Motor Vehicle Commission (MVC) has prepared their response to the Data Security Audit performed by your staff. As you know, our core mission is ensuring the security and integrity of all motor vehicle documents. The data security issues that you have identified have been preliminarily reviewed by my staff and addressed as follows:

→ **Social Security Numbers – Deceased Individuals**

Finding: *The Driver Owner database contains active records with Social Security Numbers belonging to deceased individuals.*

MVC Response: The Commission concurs with the audit finding; however, a preliminary review indicates that many of those records that were reported as “active” in the audit report are now in the Comprehensive System as “deceased.” The Commission believes that the periodic update from the National Technical Information Service (NTIS) within the Department of Commerce occurred after the extraction of data by the Office of the State Auditor. As for the names that do not match, there may have been subtle name formatting, such as Sr., Jr. II, or a dash between the maiden and married names that caused the files not to match. The Commission will work with the Office of Information Technology (OIT) and the MVC business units to correct any discrepancies. The process within MVC will be a manual process, which is time-consuming and will require access to the federal Social Security Number verification system. Should the MVC suspect fraudulent activity on any of these records, it will be referred to the MVC’s Division of Security and Investigations for further review.

On the Road to Excellence
Visit us at www.njmvc.gov
New Jersey is an Equal Opportunity Employer

→ **Invalid Social Security Numbers**

Finding: *The Driver Owner database contains active records with invalid Social Security Numbers.*

MVC Response: According to MVC policy, employees at the Motor Vehicle Agencies are permitted to perform overrides on Social Security Numbers in certain situations. All overrides are tracked by the Commission and when each agency is audited, the focus is on these transactions. In reviewing the file provided by the Office of the State Auditor, the bulk of the data revealed all zeros in the Social Security Number (SSN) field, which is not an acceptable override scenario. The MVC will review these records and take any necessary corrective actions.

→ **Non-Expiring Licenses and Identifications**

Finding: *The Driver Owner database contains license or identification records that do not expire.*

MVC Response: A preliminary review by the Commission indicates that all but one record are paper photo documents, which are no longer valid as a form of identification; however, the MVC will develop a plan to remediate this issue.

→ **Incomplete Records**

Finding: *The Driver Owner database contains records that should be expunged from the database.*

MVC Response: A portion of the nearly 1.7 million records in the MVC database cannot be expunged by the Commission. While there is no driver license number associated with these records, a driver history record could have been created due to the incurred violation. These records have historical and legal value to the Commission. On the other hand, those records without any associated driver history could be expunged. The MVC will discuss the finding with the Office of Information Technology to see if there is a possible solution for these records.

→ **Corporate Records**

Finding: *The Driver Owner database contains corporate records without valid Employer Identification Numbers (EIN). We recommend the MVC perform a match of the EIN numbers in the corporate records to a reliable reference to identify companies registered with the MVC under an invalid EIN and investigate these exceptions.*

MVC Response: The MVC issues corporation codes (corpcode) to businesses located in New Jersey. These numbers allow businesses, organizations and government agencies to conduct motor vehicle transactions such as titling and registering vehicles under a business or entity name, deal in motor vehicles, or obtain information from the Commission regarding registrations and titles, such as insurance companies. This identifier is used solely for the purpose of conducting motor vehicle transactions and cannot be used as an identifier for any other purpose. Before a 15-digit corpcode can be issued, the business must be registered with the Division of Revenue and Enterprise Services (DORES) and request a valid Employee Identification Number.

The Commission currently has a manual process in place to verify and correct the EIN as business licenses are renewed. In addition, the Commission is in the process of proposing regulations that would establish procedural requirements in order to strengthen the controls for the issuance of an EIN. At this time, the MVC cannot undertake this business process change; however, it will consider changes with the development of any new system by the Commission.

→ **Duplicate Social Security Numbers**

Finding: *The Driver Owner database contains multiple records for the same Social Security Number (SSN) and vehicle class. We recommend that the MVC investigate the records that share a SSN to determine if one or more of the records can be canceled. In addition, the new MVC system should perform real-time checks for duplicate SSNs, or the MVC should perform this analysis outside the system on a periodic basis.*

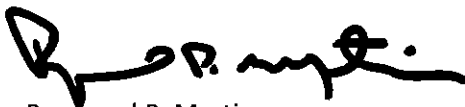
MVC Response: The MVC agrees with the finding and will develop a strategy for reviewing all of the records to ensure that the proper SSN is associated with the right person. This will be a manual process for the Commission since the current system does not provide the flexibility to check existing records for a matching SSN.

→ **General Controls**

Finding: *The Motor Vehicle Commission does not have a business continuity plan for the Trenton Office Complex and field offices. We recommend the MVC continue the steps toward completing the BCP in order to prevent a disruption of services if an incident were to occur.*

MVC Response: The MVC concurs with this finding and is in the process of developing a Request for Proposal (RFP) to be issued by the Department of the Treasury in order to secure a highly qualified vendor to develop a business continuity plan. The completed product will identify our organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the Commission while continuing operations.

Sincerely,



Raymond P. Martinez
Chairman and Chief Administrator

RPM/CH/rmg

cc: Jeanne D. Ashmore, Deputy Chief Administrator
Richard Miller, Deputy Administrator of Finance and Administration
Selika J. Gore, Deputy Administrator of Operations
Edward Lally, Director of Information Technology
Carol-Ann Hollows, Director of Financial Management