STATE OF CONNECTICUT

PERFORMANCE AUDIT
OF THE DEPARTMENT OF MOTOR VEHICLES'
INTERNAL CONTROLS OVER
DRIVERS' LICENSES AND IDENTITY CARDS

MAY 5, 2005

AUDITORS OF PUBLIC ACCOUNTS
KEVIN P. JOHNSTON ♦ ROBERT G. JAEKLE

TABLE OF CONTENTS

PERFORMANCE AUDIT
OF THE DEPARTMENT OF MOTOR VEHICLES' INTERNAL CONTROLS OVER DRIVERS' LICENSES AND IDENTITY CARDS

In accordance with the provisions of Section 2-90 of the General Statutes, the Auditors of Public Accounts has conducted a performance audit of the Department of Motor Vehicle's (DMV) drivers' license and identity card functions. Our audit was conducted in accordance with Generally Accepted Government Auditing Standards and included such procedures as we considered necessary to form an opinion about the controls in place over those functions.

Recent allegations that some of the DMV's employees issued driver's licenses to individuals who may not have met the State's eligibility requirements, including citizenship, led to the Governor's request that the Auditors of Public Accounts conduct a review of the DMV's licensing process. The results of that audit are presented in this report, which consists of the following sections: Comments, Results of Review, and Recommendations.

COMMENTS

Audit Objectives, Scope, and Methodology:

Our objective was to consider whether the DMV's internal controls over the credentialing function reduced to a relatively low level of risk the possibility that credentials could be issued in a manner that did not comply with applicable laws and regulations or failed to safeguard assets (including data) and not be detected within a timely period by agency employees in the normal course of performing their assigned functions. Specifically, we considered the following:

- Are front-line employees properly hired and trained to appropriately issue and renew credentials?
- Are data processing controls sufficient to monitor, issue, and renew credentials?
- Are credentials only issued to eligible applicants whose identities have been adequately established?
- Are controls over assets, such as data and supplies for producing credentials, adequate?

- Does legislation support adequate internal controls over issuing and renewing credentials?

To accomplish our objectives, we conducted interviews with staff and contractors and observed operations at the DMV's Central Office, Waterbury Branch, Wethersfield Branch, a Photo License Bus, and the Waterbury branch of the Connecticut Motor Club (AAA.) We based our conclusions regarding compliance on these interviews and observations. We also documented the DMV's policies and procedures over the credentialing process. We did not rely on computer-generated data to any material degree and therefore we did not assess its reliability. We obtained certain information from selected databases and considered the reasonableness of such data where possible.

Foreword:

The role and responsibilities of the Department of Motor Vehicles (DMV) are identified primarily under Title 14, Chapters 246 through 255 of the General Statutes. This audit focused on the Department's operator licensing and identity card functions that are codified by Sections 14-36 through 14-46g and Section 1-1h of the General Statutes, respectively.

Background and Recent Events:

One of the DMV's responsibilities is issuing credentials (identity cards and drivers' licenses) that have become widely regarded as a primary form of identification. As a result of the events of September 11, 2001, the DMV initiated procedures to strengthen its controls for issuing credentials to ensure that they are properly issued to individuals who meet the requirements as provided by law, such as citizenship, residency, and identity, as well as the applicable skill requirements for a driver's license.

Credentials issued by the DMV take the form of either identity cards or driver's licenses. Identity cards (IDs) are a widely accepted credential for banking and airline travel. They are only issued to individuals who do not already hold a valid driver's license or whose license is under suspension. Although a drivers' license is frequently used as an identification credential, its main purpose is to document whether an individual is authorized to drive either a commercial or a noncommercial vehicle. It also documents the class of vehicle that an individual is authorized to operate and whether there are any restrictions and endorsements. There are 16 different types of restrictions that can be recorded on a license that range from requiring the driver to wear corrective lenses to limiting the size of the vehicle that can be driven. Endorsements to licenses indicate that the driver has the authority to operate vehicles under specific circumstances such as to transport hazardous materials or public passengers.

The following table summarizes the number of active credentials at the beginning of February 2005. Noncommercial licenses represent over 85 percent of active credentials.

Driver's License	
Commercial	93,000
Noncommercial	2,300,000
Identity Cards	240,000
Total	2,633,000

Gary J. DeFilippo served as Commissioner of the DMV until January 31, 2005. Ralph J. Carpenter was appointed on February 1, 2005, and continues to serve as Commissioner.

We were told that the State Police began directing the DMV's confidential investigations into whether the DMV's employees were issuing fraudulent credentials during July 2003. To prevent suspected employees from altering their behaviors, the DMV did not revise its policies and procedures to correct any identified control weaknesses, instead it monitored the suspected employees' transactions. As a result of the investigations, three of the DMV's employees, along with private individuals, were arrested for allegedly participating in issuing credentials to individuals who may not have met the DMV's requirements. We do not provide any specific information relating to this alleged licensing fraud in this report because the investigations are ongoing.

RESULTS OF REVIEW

Our audit noted that the DMV's internal controls over the credentialing function did not reduce to a relatively low level of risk the possibility that credentials could be issued in a manner that did not comply with applicable laws and regulations or failed to safeguard assets (including data) and not be detected within a timely period by agency employees in the normal course of performing their assigned functions. We presented the following areas of concern to the DMV and included their responses to each item.

Item No. 1 - Hiring and Training of Employees and Contractors:

Criteria: Proper security procedures suggest that a thorough background check of an individual's criminal history should be completed for those individuals who handle cash and/or have access to confidential information. Federal Public Law 92-544 prohibits the Federal Bureau of Investigation (FBI) from executing a fingerprint-based national criminal history background check for the purposes of employment unless it is required by State legislation. Approximately 10 years ago the DMV proposed legislation that would have enabled them to obtain national criminal history background checks based on its employee's fingerprints. The bill was defeated in the Judiciary Committee.

The American Association of Motor Vehicle Administrators (AAMVA) has suggested that letting employees know that the Department is aware of and monitoring fraudulent activities is a significant deterrent to employee fraud. AAMVA has produced guides and reports of the best practices over employee fraud training, recommending that employees receive training on the potential temptations of fraudulent activities as well as the penalties for performing them. Fraud training should supplement business process training upon initial employment and should also be offered periodically thereafter. Employees should be able to report suspected fraud anonymously.

The DMV's contracts with the Connecticut Motor Club, Inc. and Automobile Club of Hartford (AAA) states that the DMV shall train and approve the AAA's employees to process license renewals.

Condition: Since the nature of issuing and renewing identity cards and drivers' licenses/learners' permits (credentials) results in access to cash and confidential information, the moral character of DMV's employees and contractors is critical. Currently the DMV screens its job applicants based on their driving history and a national criminal background check that is based on the individual's name and date of birth. There are no written policies and procedures regarding the evaluation of the results of these background checks. Also, the DMV does not have its employees' fingerprints examined by the State Police

and the FBI. The DMV has established a committee to recommend improvements to its current policies and procedures regarding criminal background checks of its employees. Also, AAA staff, including their summer interns, is authorized to process driver's license renewals. The DMV's contract with the AAA does not establish minimum standards for criminal background checks of their employees, and the DMV does not independently examine their employee's criminal backgrounds.

The process used by DMV to train employees and contractors did not include fraud awareness training. Also, The DMV's supervisors were only recently trained regarding identity theft and line employees have not been sufficiently trained to detect fraudulent documents submitted by applicants. The DMV has not been "training and approving" the AAA's employees as required by the contract. Also, there are no policies and procedures for employees of the DMV or AAA to report suspected fraud anonymously.

Effect: Weaknesses in the hiring and training of employees and contractors increase the risk of noncompliance with relevant laws and policies. The lack of a known mechanism to report suspected abuses anonymously may hinder such reporting and prevent timely action to correct problems.

Cause: A lack of administrative control contributed to these conditions. The DMV did not establish adequate policies and procedures based on an assessment of the risks associated with its employees and contractors' criminal backgrounds. The DMV employee responsible for the AAA's license renewal operations was unaware of the contractual provisions.

Recommendation: The DMV should consider seeking the necessary legislation to obtain fingerprint-based criminal history background checks and should establish formal policies and procedures for evaluating the results of employee's background checks. Appropriate standards for background checks should be established for the employees of DMV's contractors. Policies and procedures should be established to sufficiently train employees and contractors to identify fraud and to report it to management anonymously. (See Recommendation 1.)

Agency Response: "Proposed legislation, Senate Bill No. 1058, will require each applicant offered employment with the DMV to be fingerprinted and to submit to state and national criminal history checks.

The Document Integrity Unit (DIU) within the new Bureau of License and Registration Management will develop a thorough ongoing audit policy based on an organizational risk assessment. Additionally, DIU will be responsible for ensuring that all branch management and employees receive appropriate initial and refresher training in the

identification of fraudulent documents. DIU will also be responsible for providing an anonymous whistleblower line and for communicating its operation, confidentiality, and availability to all employees. In the meantime, while this new unit is getting off the ground, the Bureau of Customer Services and Relations (BCSR) has conducted training classes on identity fraud for all branch employees associated with licensing and their supervisors and managers and every employee has been given a manual. Additional classes are being scheduled through AAMVA for supervisors and managers and there is currently one DMV Lieutenant specifically assigned to fraud training. A form has been developed to anonymously report fraud and posters created for each branch office.

With regard to the AAA contracts and their hiring and training of employees to perform licensing activities, BCSR in conjunction with the Bureau of Legal Services will seek amendments to the agreements with the two AAA organizations, to include standards for background checks for their employees and the certification of all employees who process license renewals. We also expect that the contracts will be amended to state that the AAA organizations will train the individuals to process the renewals, but DMV personnel must certify and approve them prior to their receiving access to the DMV system. Again, a form has been created to anonymously report fraud."

Item No. 2 - Data Processing Access Controls:

Criteria: A properly designed Information System (IS) provides users with automated controls designed in part to prevent and detect errors. It also provides management with readily-accessible information about operations.

Proper security procedures would require that the DMV's employees' and contractors' system access should be terminated upon separation from the Department by removing both the logon identification and password.

Condition: The Information System does not provide management with sufficient oversight of its employees and operations. Throughout this report we make recommendations for improvements to the systems. In addition to those findings we also noted the following:

- Users of the systems cannot create their own reports. Each report must be created by the IS division. The systems have not been designed to include reports detailing such information as the number of licensees at a single address. There are limitations on the types of data analysis that can be done because the licensing,

testing, imaging and registration systems are not integrated and because individuals are not assigned a single identifier across the various databases.

- Our report on the examination of DMV's financial records for the fiscal years ended June 30, 2000, 2001, and 2002 recommended in part that the Department should terminate the system access rights of employees and consultants prior to separating. That audit noted approximately 120 instances in which the logon identifications (ID) of former employees or consultants remained on the system. We were told that it is currently the DMV's policy to leave the logon ID on the system and to remove only the password access.

- User's passwords are limited to three characters and are sometimes based on the employee's initials. These passwords do not expire.

Effect: The effectiveness of data processing access controls is reduced. The information system does not provide DMV with the necessary controls to prevent, detect, and report potential errors and abuses. Data on the system is not readily accessible for management oversight.

Cause: The system was originally developed to ensure data accuracy and recovery and was not designed to facilitate report writing.

The DMV believed that leaving separated employees and contractors' logon IDs on the systems did not increase the risks for unauthorized access significantly.

Passwords were limited to three characters because memory storage was expensive at the time the system was developed.

Recommendation: The DMV should improve its information systems to automate the licensing process while adequately preventing, detecting and reporting potential employee, contractor and customer abuses. This should include adequate user access controls. Also, the system should provide management with readily accessible reports. (See Recommendation 2.)

Agency Response: "DMV, through the draft Enterprise Technical Architecture Design, the new Drivers' License System project, and the new Registration System project, will be addressing these issues [going] forward. As new systems are built, we will be incorporating new report capabilities….

To clarify, in some instances, [we] suspend ACF2 access and Midrange access until the HR Monthly Separated Report is provided. Once reported, we delete the relevant Ids. … [a] request for termination of [a specific user's] access [is] handled immediately.

Note that by suspending access, this denies access to our mainframe systems until final documentation is provided.

There is an internal DMV password system, ACF2 that will be eliminated as we build new systems, [and] then only active users would know and/or use these passwords. We try to keep these up-to-date and will be more consistent and incorporate these as part of our larger data access process. As an example, our new Social Security On-Line Verification process ties ACF2 security into login activity and procedures reports for administration. This will be similar to our future plans for building new systems but with more capabilities in the future. The Driver Services Division has requested a list of all employees who have access to either issue a restoration or modify a driving record.

Finally, a project is underway to verify which employees have access to the various systems utilized within the agency, particularly those associated with the issuance, revocation, and restoration of drivers' licenses. Following the completion of each system within this review, DMV will cancel all access and reissue new access codes to those employees who have been authorized by their respective managers. This process has already been completed with respect to the Driver History system. We anticipate better control of these codes and will work with mangers to assure that the list of employees is kept current and access continues to be required for the individual employee's job function."

Item No. 3 - Data Processing Disaster Recovery Plan:

Criteria: Security over data includes provisions that organizations have current disaster recovery plans in place to enable critical operations to resume activity within a reasonable period after a disaster.

Condition: We noted the following conditions, which have not changed since they were included in our report on the DMV's operations for the fiscal years ended June 30, 2000, 2001, and 2002. The DMV's business contingency procedures did not include a current disaster recovery plan for data processing applications, including the credentialing function. Also, the DMV does not have arrangements in place for hot site/cold site utilization of its midrange applications housed within DMV facilities. With respect to DMV's major applications housed within the Department of Information Technology (DOIT), DMV had not entered into a formal agreement with DOIT specifying the responsibilities of each agency with regard to disaster recovery.

We were told that the DMV relies on DOIT for operation and disaster recovery for many of its systems, including credentialing; however, our report on DOIT's operations for the fiscal years ended June 30, 2002 and 2003, indicated that DOIT does not have a disaster recovery plan in place. In 2001, a recovery assessment was performed and numerous concerns were raised that included the lack of a documented disaster recovery process for some systems; the failure to test a hot site recovery; the lack of a tested recovery network infrastructure to provide needed connectivity; and the lack of agreement with other user agencies as to what data is expected to be recovered and the expected timeframes to accomplish the task. The assessment concluded that it was doubtful that DOIT would be able to recover its midrange processing function and network services within 72 hours of a disaster.

While it appears that DOIT is working with other State agencies to ensure their data and equipment in DOIT's Data Center is protected from disaster, it seems that the availability of hot site/cold sites for other State agencies to continue operations has not been addressed.

Effect: The DMV's lack of a comprehensive disaster recovery plan may lead to increased costs to the State due to service interruptions or loss of credentialing data from an actual disaster. Also, operations critical to the credentialing function may not be able to resume in a timely fashion.

Cause: DMV staff appeared to be aware of the need for a disaster recovery plan, but the task was not a high priority because the major applications were regarded to be the responsibility of DOIT. Despite the events of September 11, 2001, DOIT has not been compelled to elevate disaster recovery to a higher level of importance.

Recommendation: The Department of Motor Vehicles should expand efforts to create a comprehensive disaster recovery plan. A formal agreement should be entered into with the Department of Information Technology (DOIT) clarifying the division of responsibilities between DOIT and DMV. (See Recommendation 3.)

Agency Response: "Although DMV regards this as a high priority, we continue to depend on DOIT for coordination of Disaster Recovery Services. Information Systems Technology staff met with DOIT last summer and exchanged information in the fall of 2004 with a DOIT-hired vendor on our mainframe systems and the backup of our Midrange systems. We have setup a procedure to backup our servers but have run into network capacity issues. We will continue to seek DOIT's assistance in developing a comprehensive disaster recovery plan for the Agency"

Item No. 4 - Controlling Changes to the Record Associated with Credentials:

Criteria: Proper data security protects the data associated with an existing credential from unauthorized modifications. The DMV's information system requires a supervisor's password to make more than two changes at one time to an individual's record. Also, employees are prohibited by DMV policy from modifying their own records or executing transactions on their own behalf.

Condition: The information system is not designed to prevent or detect whether a DMV employee has made unauthorized changes to a record. Although the information system requires a supervisor's password to make more than two changes at one time, it does not require the password if those changes are made during separate sessions. Also, the system does not prevent employees from making changes to their own records. During the course of its investigation into suspected employee fraud, the DMV noted that two employees each had 16 photo images associated with their licenses. Although the system creates a log of all changes it would be cumbersome for the DMV to monitor it for suspicious activity. Also, the system has not been designed to generate reports of suspicious activity.

Effect: The DMV is not aware of whether its employees have inappropriately changed their own records or those of other individuals.

Cause: The data processing system in place at DMV did not have the capability to facilitate the review of changes.

Recommendation/ Conclusion: During January 2005, the DMV began reviewing monthly reports of changes to its employees' records to verify that any changes were properly executed. The information system should monitor and report suspicious changes to individuals' records. (See Recommendation 4.)

Agency Response: "Many procedural changes have been adopted by DMV, some after 9/11 and some after the license fraud was exposed. Since January 2005, the Bureau of Customer Services and Relations has been receiving from Information System Technology a report on any changes to an employee record. The report is reviewed bi-weekly by the division chief and division managers. Any questionable transactions are reviewed and appropriate personnel actions taken. The Document Integrity Unit will design and implement a more thorough, ongoing audit process that will ensure that the revised procedures are embraced and followed consistently. This type of audit must be supported by information system monitoring that reports suspicious activity. The current information systems were not designed to perform this type of monitoring and reporting. However, we are

building these requirements, point forward, into our new system developments. The new Social Security Online Verification incorporates some of these new functions. The new systems being designed will include such features as an automatic log out after a short time, fingerprint log on and fingerprint authorization to perform each transaction. DMV is currently extending an existing vendor contract to secure biofacial recognition capability, which will reveal multiple credentials and other types of fraud."

Item No. 5 - False Statement Penalty Provisions:

Criteria: Section 53a-157b of the General Statutes makes it a Class A misdemeanor to intentionally make a false statement intended to mislead a public servant in the performance of his duties, pursuant to a form bearing notice, authorized by law, that false statements are punishable by law.

Section 14-36, subsection (e), of the General Statutes requires that applications for a non-commercial driver's license be submitted under oath, stating such facts as the Commissioner requires.

Section 14-110 states that, "any person who swears or affirms falsely in regard to any matter respecting which an oath or affirmation is required by this chapter or by the Commissioner shall be guilty of perjury or false statement…."

Section 14-44c, subsection (a), requires applicants to certify the accuracy and completeness of the application, "subject to the penalties of false statement under Section 53a-157b."

Section 1-1h, subsection (a)(5), of the General Statutes requires the DMV to include a notice to the applicant that false statements on the identity card application are punishable under the false statement provisions of Section 53a-157b of the General Statutes.

Condition: The DMV relies on notices contained on its application forms regarding perjury and false statement to ensure that the applicant's statements on the application are factual. Some of the notices contained on DMV's application forms refer to the penalties for committing fraud, however, the language is inconsistent and only the application for an identity card refers to Section 53a-157b of the General Statutes.

Effect: The impact of DMV's notices to applicants regarding perjury and false statement is reduced without references to the penal code, specifically Section 53a-157b of the General Statutes.

Cause: The DMV's various applications do not consistently refer to the language contained in Section 53a-157b of the General Statutes regarding the penalties for making false statements.

Recommendation: The DMV's application forms should include language relating to the false statement penalty provisions of Section 53a-157b of the General Statutes. (See Recommendation 5.)

Agency Response: "DMV will include the correct language, referencing Section 53a-157b of the General Statutes, on the next revision and printing of its license application forms. That revision is in process and will be completed in the near future. In addition, DMV will seek a legislative amendment in this session, to include reference to Section 53a-157b within Section 14-36, [subsection] (e) [of the General Statutes.]"

Item No. 6 - Establishing an Applicant's Identity:

Criteria: The DMV is responsible for establishing an individual's identity when it issues, renews or replaces a credential. Section 1-1h of the General Statutes authorizes the DMV to issue identity cards to individuals who do not possess a valid motor vehicle operator's license based, in part, on the individual's birth certificate and "other pertinent information as the Commissioner of Motor Vehicles deems necessary." Section 14-36, subsection (e)(2), of the General Statutes requires that applicants must provide evidence of their date of birth and identity.

To obtain a new credential, the DMV requires applicants to submit a certified birth certificate, valid U.S. Passport, or proof of legal status along with one additional form of identification from a lengthy list of options.

The American Association of Motor Vehicle Administrators (AAMVA) recommends that motor vehicle offices implement one of the following four recommendations: 1) two employees should independently review an applicant's identification documents, 2) documents should be photocopied or scanned, 3) a centralized process should involve review by a document specialist, or 4) surveillance cameras should be utilized. Also, the AAMVA recommends that credentials should be verified to independent sources. For example, Social Security Numbers should be verified with the Social Security Administration.

Also, valid credentials should only be available to the individual originally identified by the DMV.

Condition: The DMV has not established adequate policies and procedures to verify the identity of applicants when issuing new credentials.

- Most states' birth records cannot be readily verified. The DMV relies on its employee's ability to identify fraudulent documents. Employees responsible for evaluating documents have not been adequately trained to verify the authenticity of each state's birth certificate or the approximately 30 different types of identity documents accepted by the DMV.

- According to AAMVA, there were 38 states verifying Social Security Numbers (SSNs) as of January 2005. The DMV is testing a system to verify SSNs. Also, the DMV has drafted legislation that requires an individual to provide a SSN as part of the application process and establishes the authority to verify the numbers with the Social Security Administration.

- Until November of 2004, the risk for fraud was increased because the DMV's procedures only required one individual to evaluate an applicant's identity documents.

The DMV's current system to renew a credential does not prevent an employee from issuing a fraudulent credential with an imposter's image. The process to verify an image relies on either a biometric system or a camera operator to compare an individual's current photograph against the last available image. We noted the following deficiencies regarding the current system:

- An employee may issue a credential to an imposter even though the automated biometric verification resulted in warnings of a mismatch. The system does not require supervisory oversight, it does not create a record of the mismatch, and no subsequent review is performed.

- Due to technological constraints, the automated system is not used to verify photo images taken on the DMV's buses and at the AAA Connecticut Motor Club offices. At those locations, the DMV relies solely on the camera operator to verify that the new image matches the image on the individual's old license.

- Until December 2004, the DMV's buses were permitted to issue a replacement document for a lost or stolen license. Because of the technological constraints noted previously, and the fact that the image relating to the missing document was not available for review, the DMV could not verify that the individual requesting the replacement credential was not an imposter. Also, the DMV did not perform automated verifications on the new images at a subsequent time. Beginning in January 2005, the DMV has stopped issuing replacement licenses from its buses.

Currently, the only way the DMV could detect that a credential was issued with an imposter's image would be if the correct person applies to renew the credential and the system rejects the request because either the credential is not expired, or biometric verification recognizes a difference in the image. An employee who has issued a fraudulent credential can prevent this method of detection by deleting the transaction.

As a result of its current investigations into suspected fraud, the DMV has determined that there are credentials that have the photographs of two or more individuals associated with them. Also, they have noted that there are images of a single individual associated with multiple credentials. Since the DMV has not established additional biometric systems to detect such credentials, they do not know how many fraudulent or duplicate credentials have been issued.

We noted that the DMV does not issue a new number when a lost or stolen credential is replaced, because in some rare cases it could enable an individual with bad credit to commit license-based credit fraud. This could result in two valid documents being held by two different individuals. Also, the DMV does not flag the credential as having been lost or stolen in its records. An evaluation of the credential's record would not suggest that there is any increased risk of its use by an imposter.

Effect: The DMV may not detect 1) fraudulent documents submitted by applicants for new credentials, 2) whether fraudulent credentials are being or have been issued to an imposter, or 3) whether it is renewing or replacing a lost or stolen credential.

Cause: The DMV did not adequately assess the risk that employees and contractors' employees would knowingly issue fraudulent credentials. We were unable to determine why the DMV did not fully train its staff to identify fraudulent documents. The DMV did not monitor its one-to-one image verification system for the renewal of credentials and did not implement additional systems that were available from the same vendor to detect both employee and customer fraud. Also, the DMV does not flag a credential as lost or stolen.

Recommendation/ Conclusion: The DMV should adequately train its staff to detect fraudulent documents submitted by applicants for credentials and should pursue the necessary legislation to verify Social Security Numbers for both the numbers currently in its systems and those submitted by applicants for new credentials. During November 2004, the DMV modified its policies and procedures so that identification documents submitted by an applicant are photocopied and reviewed by two different

employees, therefore, we are not recommending any changes to this process at this time.

The DMV should enhance its systems to biometrically verify facial images and should use those systems to detect, cleanse, and revoke fraudulent and duplicate records. Controls over credentials issued with mismatched facial images and subsequent deletions should be improved to ensure that an employee cannot issue a credential with an imposter's image.

The DMV should develop a system to record and report credentials as lost or stolen. (See Recommendation 6.)

Agency Response: "Please refer to our response to [Item No. 1] (Hiring and Training of Employees and Contractors) with respect to training on fraudulent document detection.

As of February 1, 2005, the Bureau of Customer Services and Relations checks social security numbers through the social security database. Since November 2004, at least two… examiners check the identity documents of licensing customers. In the event of a mismatch of biometric data, a report is being created by our Information Systems Technology (IST) staff to be reviewed [and acted upon] by the management staff. A new process has been created so that individuals who claim their credentials were lost or stolen must send a letter to our bureau where the information is reviewed and a new license number may be issued to the individual.

As noted previously, DMV is currently extending an existing vendor contract to secure biofacial recognition capability. The Document Integrity Unity is charged with the responsibility for setting up the capability and procedures to utilize the output of the matching and cleansing process to identify and revoke fraudulent and duplicate records. The same vendor will be providing proofing workstations to bolster the efforts of the DMV workforce to identify fraudulent documents. The proofing workstations are designed to verify the validity of out-of-state licenses, as well as U.S. and most other passports.

DMV through the draft Enterprise Technical Architecture Design and the new Drivers' License System and Registration System projects is addressing client identification issues from a point forward basis. As new systems are being built, we will be incorporating the creation and assignment of a single client identifier, including new reporting capabilities for use by the business units and IST staff alike."

Item No. 7 - Secure Handling of an Applicant's Identity Documents:

Criteria: Sound security practices should result in the return of an applicant's original identification documents to prevent those documents from being compromised.

Condition: The DMV's policies and procedures do not address how to handle documents that the DMV is unable to return to the applicant. We noted that one branch office had identification documents in a storage cabinet with various other lost and found items. We have been told that initially the DMV tries to contact the individual and then mails the documents to the address of record. These mailings are occasionally returned by the Postal Service.

Effect: Unsecured handling of an individual's identity documents puts those documents or information they contain at risk for theft.

Cause: The DMV has indicated that the return of an applicant's documents is common sense and does not need to be addressed by formal policies and procedures.

Recommendation: The DMV should consider establishing written policies and procedures for the proper return of customer documents that include: 1) sending a letter to the individual notifying them of the status of their documents; 2) only mailing documents at the customer's request; 3) questioning any returned correspondence as a possible fraud indicator; and 4) storing documents to prevent access by unauthorized individuals. (See Recommendation 7.)

Agency Response: "DMV, through the Document Integrity Unit (DIU), will establish, disseminate, and ensure compliance with written procedures for safeguarding any original documents that DMV is unable to return to the applicant. Compliance will be part of the DIU audit process. DMV branches will be provided with secure filing storage to safeguard all of the identity documents that come within the custody of DMV."

Item No. 8 - Controls over Issuing New Credentials:

Criteria: In accordance with Sections 1-1h and 14-36 of the General Statutes, the DMV is responsible for determining whether an individual qualifies for a credential. The standards for obtaining a credential include applicable age requirements, documented identity, physical ability, operator skills, and sufficiency of knowledge.

Condition: Since the DMV's system for issuing credentials is not fully automated, a DMV employee could circumvent the eligibility, identity, and testing requirements when issuing a new credential. The review of

identification documents and applicant testing for new drivers' licenses are not linked to the system that is used to issue credentials. The DMV does not reconcile the number of applications received with the number of tests administered and new credentials issued.

Beginning in November 2004, the DMV instituted manual compensating controls that require inspectors to perform a second review of an applicant's identification documents. Also, the camera operators responsible for producing new credentials began verifying that the applicant was tested. Finally, during the bookkeeping process, employees review each application for the applicable copies of identification documents and testing results. This system relies heavily on duplicate employee review rather than automated controls and reconciliations.

Effect: Prior to November 2004, the DMV could not readily detect whether employees issued credentials that did not meet the DMV's standards.

Cause: The DMV's controls were not designed to detect whether employees were complying with the Department's policies and procedures for verifying an applicant's identity or completion of the necessary testing requirements when issuing new credentials.

Recommendation: The DMV should consider automating its credentialing process so that its application, testing, and issuance processes are linked, thus helping to ensure that only individuals who meet all of the requirements are issued a credential. Until such an automated process can be developed, the DMV should consider reconciling the number of applications received, tests administered, and credentials issued to detect employee errors and fraud. (See Recommendation 8.)

Agency Response: "Since November 2004, the DMV has adopted significant procedural changes in the branch operations to address "Insider" Fraud. The Bureau of Customer Services and Relations (BCSR) now manually reconciles its applications received, tests administered, and credentials issued. The bookkeeper in each branch office doing the daily reconciliation monitors that the totals match and all discrepancies are reported to the manager of the branch and the division manager who has the responsibility of researching the incident for resolution. In addition, Fiscal and Administrative Assistants (FAA's) are being hired to oversee the reconciling of the documents and monies. The Agency has hired and trained five FAA's to date. Other procedural changes include:

- The Intake Examiner cannot also be the Document Examiner or do the image capture. This prohibition is monitored by the supervisory/management staff at each branch. With the new

system being designed, an employee will be prevented from performing more than one of these steps once their ID is recorded at one of the steps.

- With respect to new issues, the customer must bring a picture of him/herself, which accompanies their documents through the process to image capture. Staff compares picture to applicant at each step.
- A Ct. Non-Driver I.D. is not accepted as primary I.D. for a Driver's license.
- Inspection staff photocopies all documents and clips them to originals.
- An Immigration confirmation is performed.
- A Social Security number verification is performed.
- With respect to renewals, the existing image is verified prior to capturing new image….

In addition, as noted previously, DMV is in the process of adding biofacial recognition …, document proofing workstations, and the centralized issuance of new credentials. Full automation of the credentialing process will not be possible until the completion of the [new Driver's License System] project."

Item No. 9 - Expiration Dates for Non-Citizens' Credentials:

Criteria: The American Association of Motor Vehicle Administrators (AAMVA) recommends that the expiration date of a credential should be linked to a non-U.S. citizen's right to stay in the country.

Condition: Credentials issued by the DMV do not expire when an individual's right to stay in the United States expires.

Effect: An individual whose eligibility for a credential has expired will continue to hold a credential that appears to be valid.

Cause: The Connecticut General Statutes do not link the expiration date of a credential to an individual's right to live in the United States. Legislative amendments that were proposed during the last two sessions were not passed by the legislature.

Recommendation: The DMV should continue to pursue legislation to link the expiration date of a credential to the length of time that a non-U.S. citizen is authorized to stay in the country. (See Recommendation 9.)

Agency Response: "…DMV has pursued this legislation very actively in the past two sessions of the legislature. This proposal is now contained in the aforementioned [proposed] legislation sponsored by the Governor,

Senate Bill 1058. We will continue to urge the General Assembly to enact this type of legislation so that licenses will expire at the same time as the authorized presence of the license holder in the United States."

Item No. 10 - Criminal Background Checks for Endorsements to a Driver's License:

Criteria: Section 14-44, subsection (a), of the General Statutes prohibits individuals from providing transportation services without an appropriate endorsement to their license. The three types of endorsements are 1) a passenger endorsement to a commercial driver's license, 2) a school bus endorsement to a commercial driver's license or 3) a passenger endorsement to a noncommercial driver's license. Also, this section specifically provides nonresidents who drive passengers in commercial vehicles with the right to transport passengers in Connecticut as long as the individual has a similar endorsement issued by another state. The Statute is silent regarding the State's reciprocity for nonresidents wishing to operate school buses and noncommercial passenger vehicles. Also, Section 14-39, subsection (a), of the General Statutes permits licensed nonresidents to operate a motor vehicle in Connecticut but this section makes no reference to the school and passenger endorsements.

Section 14-44, subsection (c), of the General Statutes states that the Commissioner may issue, withhold, renew, suspend, cancel or revoke any passenger or school endorsement based, in part, on the individual's criminal record and moral character. Section 14-44, subsection (e), of the General Statutes, states that prior to issuing an operator's license bearing a school endorsement, the Commissioner shall require each applicant to submit to a fingerprint-based state and national criminal history records check. Section 29-17a of the General Statutes requires that the requesting party arrange for the fingerprinting, in this case DMV. Section 14-44-5, subsection (b), of the related regulations states that, "the commissioner may decline to issue any endorsement until the necessary checks are completed and an evaluation of their contents is made."

Condition: We noted the following weaknesses regarding DMV's criminal background checks on individuals who operate passenger and school vehicles in the State of Connecticut.

- Until June 2003, the DMV required individuals who held a valid out-of-state license to obtain a Public Passenger Endorsement Card (PPEC) before transporting passengers in the State of Connecticut. To obtain a PPEC, the individual was required to submit to a fingerprint-based criminal background check. The DMV stopped

issuing the cards when they determined that they conflicted with Federal legislation that prohibits an individual from holding more than one license. Also, the DMV had determined that the related information was not included in various DMV and law enforcement data systems. In lieu of modifying its controls to ensure compliance with the legislation that requires criminal background checks, the Commissioner of DMV has granted these drivers reciprocal driving privileges. Based on the most recent report available of PPECs, there were approximately 1,900 unexpired cards during August 2002.

The DMV does not monitor whether Connecticut's neighboring States require background checks for their passenger and school endorsements, therefore it does not know whether a nonresident driver meets Connecticut's standards. It appears that Connecticut's neighbors did require criminal background checks for school bus operators at one time, however, they may not currently require them and may not require criminal background checks to transport passengers in noncommercial vehicles. The Commissioner of DMV lacks the explicit legislative authority to grant nonresident driver's reciprocity to operate passenger and school buses in the State.

- The DMV's process for obtaining fingerprints from applicants seeking passenger and school endorsements does not ensure that the fingerprints actually belong to the applicant. Although the DMV purchased four electronic fingerprint machines that cost approximately $140,000, during April and June of 2002, we were told that the DMV does not use them to print applicant's fingerprints and also that the technology does not communicate with the State Police's system.

- Since it can take months for a fingerprint-based background check to be completed, the DMV issues the endorsement based on a background check determined through the applicant's name and date of birth, analysis of the individual's application, and other procedures. This increases the risk that an ineligible applicant is granted an endorsement. If the DMV subsequently determines that the individual does not qualify for the endorsement, they revoke it and notify the individual's employer.

Effect: There is reduced assurance that drivers meet Connecticut's requirements for operating school and passenger vehicles.

Cause: When the DMV stopped issuing the PPEC, it did not develop alternative policies and procedures to ensure that nonresident operators continue to meet Connecticut's standards.

We do not know why the DMV did not use its own equipment to ensure that fingerprints belong to the applicant.

The DMV has been issuing endorsements before completing their review of an applicant's criminal background.

Recommendation: The DMV should comply with Section 14-44, subsection (a), of the General Statutes by establishing policies and procedures to ensure that individuals who operate passenger and school vehicles within the State of Connecticut have an acceptable moral character and criminal history. (See Recommendation 10.)

Agency Response: "…Although there are a limited number of [out-of-state] drivers falling into this category, the DMV did check with neighboring states and confirmed the existence of background checks for those individuals licensed for the operation of school transportation vehicles. Additionally, the employers of these drivers are required under regulation to conduct routine checks on the criminal, driving and drug/alcohol status of those drivers employed by them. DMV regulations place an onus on employers of school bus… [and school transportation vehicle] drivers to perform inquiries and update driver files on an annual basis with regard to criminal and driver histories (Section 14-275c-53 [of the General Statutes]). This department's school bus inspectors conduct audits of driver files to ensure [compliance with] these requirements. To this end, the department does in fact have knowledge that school bus/STV drivers employed in this State are of moral character. However, we are examining alternatives to strengthen this process. … DMV's position continues to be that ideally we should do a background check on … [individuals] who hold a driver's license issued by another state, regardless of the elimination of the Public Passenger Endorsement Card. However, this has staffing and other cost ramifications that come into play. Another option being reviewed would be to seek legislation to mandate that only a Connecticut licensed driver could operate a passenger-carrying vehicle based with a Connecticut employer. However, there are legislative and possible legal issues associated with any such proposal. In addition, because Connecticut is a small state with borders on three other states, there would be an immediate and possibly significant impact on the availability of qualified drivers.

DMV agrees that reinstating direct electronic fingerprinting would improve on the reliability of the fingerprint process. DMV's fingerprint equipment was purchased from the same vendor used by the State Police Bureau of Identification (SPBI), but within two years, SPBI moved to a non-compatible technology. …this equipment was intended …for those individuals who had initial fingerprints returned as illegible … [not] for the agency itself to fingerprint the thousands of

individuals who annually apply for these endorsements. We did [not then] and still do not have sufficient resources to do so. We are examining securing equipment that will again be able to transmit fingerprints electronically to SPBI. However, the fact that DMV does not have adequate staffing to handle initial applicants has not changed. Currently … [the] DMV is using a fingerprint vendor for applicants for HazMat endorsements. We are [considering using] this vendor … to obtain reliable fingerprints for initial [applications for passenger endorsements.]

DMV agrees that waiting to issue the endorsement until completion of the fingerprint-based state criminal check by the State Police would be the most effective way to safeguard children who ride the school bus, but again, this would currently impact the provision of public passenger service. … All documents provided by applicants are reviewed and necessary action is taken, as it relates to each document submitted. Medical, criminal and driver background checks are made, as is necessary. A State Police Record Check (SPRC) is made and if no record exists for the applicant, and all other requirements are satisfied, the applicant is permitted to have the endorsement entered upon their license, pending the receipt of the fingerprint results. If the applicant has 'any criminal record at all', their application is not approved until such time as all information sought has been received. The issuance of an endorsement, once it has been determined that there exists no criminal record in the State of Connecticut, is believed to be reasonable. Seldom does the department receive information from the FBI that an applicant to whom we've authorized an endorsement has a criminal record when none exists in the State of Connecticut."

Item No. 11 - Controls over the Supplies and Materials Used to Produce Credentials:

Criteria: The American Association of Motor Vehicle Administrators (AAMVA) outlines several best practices regarding the physical security over the components of the system that produce credentials and the related supplies and materials. It suggests that the materials and equipment that produce credentials should be secured at all times and should not be readily available to consumers. Also, inventories should be tracked throughout the entire process, beginning with the time of manufacture, through shipment and delivery, and finally to card production. Each location should be accountable for its inventory and usage should be monitored centrally. Finally, AAMVA states that, "there should be an assigned serialized inventory of consumable stock card production materials assigned to each specific operator at a workstation to provide the necessary inventory and audit controls."

The DMV's policies and procedures require each location to maintain a perpetual inventory of all consumables and a physical inventory should be taken weekly. Based on the physical inventory of blank cards, the DMV reconciles the number of cards used in a week against the number of licenses issued.

Condition: The DMV does not adequately store and monitor the materials it uses to produce credentials (consumables), thereby reducing the likelihood of detecting inventory theft or loss, and increasing the risks for identity fraud.

Security: We found that consumables are generally not stored in secure cabinets and that card printers containing consumables are not always locked. Cabinets used to store consumables at the AAA Connecticut Motor Club (AAA) office were not locked during the day. Consumables stored on the DMV's bus were also in unlocked cabinets and the card printer was not attached to the counter that was within the public's reach. Consumables stored at branch offices were not always locked and the locking mechanisms were not sufficient.

Excessive Inventory Levels: We also noted that inventory levels seemed excessive. A DMV bus issuing approximately 300 credentials per day had enough cards to produce 5500 credentials and one AAA office issuing between 15 and 20 credentials per day had nearly 3,000 cards. Also, a busy branch office has been receiving duplicate shipments of consumables from the vendor. It should be noted that the DMV does not pay for the consumables in its stock; rather it pays a fee for each credential issued.

Monitoring: The DMV pays an additional six cents per license for a custom laminate with "Variable Information Personalization." This technology makes it difficult to produce counterfeit cards because it embeds custom information in the laminate that is nearly impossible to reproduce and can only be read with special equipment.

- The contractor that provides the laminate has established adequate controls over this consumable from the time of manufacture until its delivery to the DMV. Each package of laminate is marked with a unique serial number by the manufacturer that is used to track the package throughout the process. Also, the contractor has provided the DMV with a system to monitor its inventory through an aging report that would detect whether a box of custom laminate was lost or stolen. The DMV was not aware of this report and did not implement alternative procedures to monitor its inventory of laminate.

- Contrary to the DMV's policies, one AAA office did not keep a perpetual inventory of laminates by their unique identifier. The DMV was unaware that records were not being properly maintained.

- The DMV has not maintained sufficient accountability over the consumable by reconciling the amount of laminate it has used to the number of credentials it has issued.

Reconciliations: Since the number of cards in a box is inconsistent, we were told that employees are required to count the number of cards in a box each time one is opened and that any discrepancies should be recorded. We noted that two branch offices each had an open box of cards that had not been counted. The bus and AAA offices had counted the cards but they had not recorded the number of discrepancies for reconciliation between the number of cards used and the licenses issued. As a result, card reconciliations do not detect the theft or loss of small numbers of cards; only significant variances are reviewed further.

Photo License Bus: The DMV has not implemented additional controls over consumables stored on photo license buses. Such additional controls are necessary because the DMV rotates responsibility for bus operations daily. The consumables remain on the bus overnight locked in a secure indoor facility. Although the employee responsible for driving the bus is the first and last individual with custody of the consumables, the DMV's policies and procedures do not require that they take a physical inventory at either the beginning or end of the day. Instead, the DMV takes a weekly physical inventory similar to that done by other branches. If the reconciliation between the cards used and licenses issued detects a significant variance, the DMV cannot hold one employee accountable because it cannot know when the cards were removed from the inventory.

Effect: The DMV has not maintained adequate control over the materials used to produce credentials.

Cause: The DMV has not established adequate policies and procedures to prevent and detect the theft or loss of consumables used to produce credentials.

Recommendation: Internal controls over consumables used to produce credentials should be improved to prevent and promptly detect their loss or theft. (See Recommendation 11.)

Agency Response: "The Bureau of Customer Services and Relations (BCSR) has taken many steps to ensure the physical inventories in branch offices, AAA

offices and buses are secure. All Branch offices, buses and AAA offices must keep all cabinets and card printers where the [credentialing] …materials are stored locked during the day and at night and access to these materials is strictly limited. In addition, a new bookkeeping procedure has been initialized that requires a counting of chip cards in all locations (branches, buses and AAA offices) at the start and end of day. A report has been created for daily reconciliation as well as the weekly report already in use. Through this report, variances are reported to the management of the site for resolution. The … [contractor's] aging inventory report is being utilized by management for control of laminate. The AAA offices have all been put on the automated inventory system "SIMS" as of 2-28-05 to control inventory."

Item No. 12 - Individuals with Multiple Credentials:

Criteria: The Connecticut General Statutes do not prohibit an individual from having multiple credentials. To ensure a complete history for a credential, the DMV's policy is to issue one number throughout an individual's history with the DMV.

Condition: The DMV's investigation into suspected employee abuses noted many cases of individuals with multiple credentials. Unless all of the credentials that an individual possesses are known, it is unlikely that a review of their history will be complete. Since applicants frequently fail to report former credentials on their application form, the DMV requires its employees to review two separate databases to verify that a credential does not already exist. The DMV is currently testing a system to automate this process and plans to implement it during February 2005.

Effect: The DMV's policies and procedures do not always detect an applicant's existing credentials.

Cause: The DMV did not have an automated process in place to facilitate and record whether an individual was already issued a credential.

Recommendation/ Conclusion: The DMV has begun implementing an automated process to prevent individuals from obtaining multiple credentials. The DMV should identify individuals with multiple credentials. Multiple records associated with an individual should be linked so that inquiries result in a complete DMV history. (See Recommendation 12.)

Agency Response: "[Proposed legislation], Senate Bill 1058 as mentioned above also clarifies that individuals may hold only one Connecticut license or [identity] card. Further, the Commissioner may immediately revoke all

such documents if the person is detected as having multiple documents.

Again as discussed previously, DMV is currently extending an existing vendor contract to secure biofacial recognition capability, which will reveal multiple credentials and other types of fraud.

As part of the Driver's License System project, DMV is developing a status modification that will notify anyone looking at a credential history that there are other related credentials.

Additionally, the Bureau of Customer Services and Relations (BCSR) has implemented an automated process through a social security check to prevent individuals from acquiring two credentials. This process began February 1, 2005.

Finally, every week the Driver Services Division receives driving histories for individuals that appear to have more than one record. Sometimes it is only a number that has been changed. After a review of this information, the Division may combine records. However, when the review indicates that a person has two CT license or non-driver identification numbers, an inquiry is made to BCSR to determine the correct number and any actions that may be appropriate (i.e., canceling a credential, referring the matter to Document Integrity Unit and possibly law enforcement, etc.)."

Item No. 13 - Conflicting Statutes and Regulations:

Criteria: Section 1-1h, subsection (d), of the General Statutes requires the Commissioner of the DMV to adopt regulations for administering identity cards issued under Section 1-1h of the General Statutes.

Condition: The DMV's regulations have not been updated to reflect changes to the statutes made by Public Act 95-26 that eliminates a minimum age restriction to obtain an identity card. Section 1-1h-4 of the related regulations was not updated to reflect the change and therefore still requires that the individual be at least 16 years old.

Effect: The statutes and regulations regarding identification cards do not agree.

Cause: We were unable to determine why the DMV did not update its regulations when Public Act 95-26 became effective.

Recommendation: The DMV should update its regulations to eliminate conflicts with the General Statutes. (See Recommendation 13.)

Agency Response: "This regulation was not changed due to an oversight after the General Assembly eliminated the minimum age restriction. DMV is currently reviewing this issue and the necessary change in the regulation will be sought as soon as the agency's position in this matter is determined."

Item No. 14 - Revenue Accountability Reports:

Criteria: In accordance with the State of Connecticut's State Accounting Manual, accountability reports should be periodically prepared for all major sources of revenue to compare the amounts that were actually recorded with the amounts that should have been accounted for. In addition to providing assurance that all transactions requiring a fee have been properly performed, accountability reports can be useful in detecting unauthorized access to databases in which records were added or redacted without going through the established procedures.

Condition: As noted in our previous audit of DMV, the Department has a cash accounting system that appears to account for the transactions that are processed accurately. However, in order to produce an accurate accountability report for each revenue type, the transactions processed by the Department should be compared to the recorded change in the number of records in the various databases. Although each branch is responsible for reconciling the fees collected to its activity, a centralized process to perform these types of reconciliations was not in place during the audited period.

Effect: The failure to produce centralized accountability reports increases the risk that erroneous transactions will go undetected. Such a process would also serve to detect unauthorized changes that may be made to the various databases without the proper processing of a transaction.

Cause: The volume and the number of different transaction types that DMV processes can make the reconciliation process cumbersome. In addition, the lack of relational databases within the various licensing and registration databases prevents the ready accumulation of the necessary data.

Recommendation: The Department should prepare centralized accountability reports for the primary sources of revenue. (See Recommendation 14.)

Agency Response: "As we have stated previously in response to audit recommendations pertaining to this matter, each DMV location reconciles daily the cash accounting system transactions to the transactions updated daily to our registration and license systems. Unfortunately, the current registration and license systems do not hold transaction history records. This prevents DMV from running historical transaction reports. DMV has received funding and has begun the process to upgrade the registration

and license systems to relational databases that will provide far more flexibility for report generation and analysis. Upon completion of these systems, DMV will be able to produce the historical reports needed to verify system transactions to their related receipts."

RECOMMENDATIONS

1. **The DMV should consider seeking the necessary legislation to obtain fingerprint-based criminal history background checks and should establish formal policies and procedures for evaluating the results of employee's background checks. Appropriate standards for background checks should be established for the employees of DMV's contractors. Policies and procedures should be established to sufficiently train employees and contractors to identify fraud and to report it to management anonymously.**

   Comment:

   The DMV's policies and procedures do not provide for adequate verification of the criminal histories of its employees and contractor's employees; sufficient employee and contractor training; or anonymous reporting of fraud.

2. **The DMV should improve its information systems to automate the licensing process while adequately preventing, detecting and reporting potential employee, contractor and customer abuses. This should include adequate access controls. Also, the system should provide management with readily accessible reports.**

   Comment:

   Users of the information system cannot create their own reports, system access rights of separated employees and consultants are not completely removed from the system, and user's passwords are restricted to three characters that do not expire.

3. **The Department of Motor Vehicles should expand efforts to create a comprehensive disaster recovery plan. A formal agreement should be entered into with the Department of Information Technology (DOIT) clarifying the division of responsibilities between DOIT and DMV.**

   Comment:

   The DMV has not developed a sufficient disaster recovery plan for its data processing applications. Also, they are relying on DOIT for disaster recovery of its systems housed at the State Data Center, but the DOIT does not have a disaster recovery plan in place and there is no contract between the DMV and DOIT for this service.

4. **The information system should monitor and report suspicious changes to individuals' records.**

   Comment:

   The information system is not designed to prevent or detect unauthorized changes to records made to either a DMV employee's record or another individual's record.

5. **The DMV's application forms should include language relating to the false statement penalty provisions of Section 53a-157b of the General Statutes.**

   Comment:

   The DMV's notices contained on its application forms do not consistently refer to the penalties for committing fraud in accordance with Section 53a-157b of the General Statutes.

6. **The DMV should adequately train its staff to detect fraudulent documents submitted by applicants for credentials and should pursue the necessary legislation to verify Social Security Numbers for both the numbers currently in its systems and those submitted by applicants for new credentials.**

   The DMV should enhance its systems to biometrically verify facial images and should use those systems to detect, cleanse, and revoke fraudulent and duplicate records. Controls over credentials issued with mismatched facial images and subsequent deletions should be improved to ensure that an employee cannot issue a credential with an imposter's image.

   The DMV should develop a system to record and report credentials as lost or stolen.

   Comment:

   Policies and procedures over issuing new credentials are not designed to adequately establish an applicant's identity by sufficiently verifying the authenticity of an applicant's identity documents and by verifying those documents to available independent sources. The DMV does not adequately monitor deleted transactions. It also does not monitor that the photo images associated with credentials are appropriate. There are no policies and procedures to record or report lost or stolen credentials.

7. **The DMV should consider establishing written policies and procedures for the proper return of customer documents that include: 1) sending a letter to the individual notifying them of the status of their documents; 2) only mailing documents at the customer's request; 3) questioning any returned correspondence as a possible fraud indicator; and 4) storing documents to prevent access by unauthorized individuals.**

   Comment:

   The DMV's policies and procedures do not address how to handle identity documents that the DMV is unable to return to the applicant.

8. **The DMV should consider automating its credentialing process so that its application, testing, and issuance processes are linked, thus helping to ensure that only individuals who meet all of the requirements are issued a credential. Until such an automated process can be developed, the DMV should consider reconciling the number of applications received, tests administered, and credentials issued to detect employee errors and fraud.**

   Comment:

   Since the DMV's system for issuing credentials is not fully automated, the DMV implemented duplicate employee reviews to detect whether an employee has circumvented the eligibility, identity, and testing requirements when issuing a new credential. Also, the DMV does not monitor whether the requirements are met by reconciling the number of applications received with the number of tests administered and new credentials issued.

9. **The DMV should continue to pursue legislation to link the expiration date of a credential to the length of time that a non-U.S. citizen is authorized to stay in the country.**

   Comment:

   Credentials issued by the DMV do not expire when an individual's right to stay in the United States expires.

10. **The DMV should comply with Section 14-44, subsection (a), of the General Statutes by establishing policies and procedures to ensure that individuals who operate passenger and school vehicles within the State of Connecticut have an acceptable moral character and criminal history.**

    Comment:

    The DMV's policies and procedures over issuing endorsements to licenses for the operation of school and passenger vehicles do not ensure that the DMV has completely evaluated the applicant's criminal background. Although legislation is silent regarding whether nonresidents operating school and passenger vehicles must meet Connecticut's standards, the DMV has granted such individuals reciprocity to operate vehicles in the State.

11. Internal Controls over consumables used to produce credentials should be improved to prevent and promptly detect their loss or theft.

Comment:

The DMV is not adequately monitoring its consumable inventories for theft and/or loss, inventory levels may be excessive, and inventories are not consistently stored in secure locations.

12. The DMV should identify individuals with multiple credentials. Multiple records associated with an individual should be linked so that inquiries result in a complete DMV history.

Comment:

The DMV's policies and procedures to verify the existence of former credentials before issuing a new credential do no always result in the detection of the former credential that results in multiple records associated with a single individual.

13. The DMV should update its regulations to eliminate conflicts with the General Statutes.

Comment:

The DMV's regulations have not been updated to reflect changes to the General Statutes made by Public Act 95-26, which eliminates a minimum age restriction to obtain an identity card.

14. The Department should prepare centralized accountability reports for the primary sources of revenue.

Comment:

The DMV does not maintain accountability over revenue by reconciling the change in the number of records in its various databases with the transactions processed for each revenue type.

CONCLUSION

We wish to express our appreciation for the cooperation and courtesy extended to our representatives by the personnel of the Department of Motor Vehicles during this examination.

Ramona Weingart
Associate Auditor

Approved:

Kevin P. Johnston
Auditor of Public Accounts

Robert G. Jaekle
Auditor of Public Accounts