REPORT OF

THE

STATE AUDITOR

Driver's License and Identification (ID) Card Security
Department of Revenue

Performance Audit
May 2008

LEGISLATIVE AUDIT COMMITTEE
2008 MEMBERS

Representative James Kerr
Chair

Representative Dianne Primavera
Vice-Chair

Senator Jim Isgar
Representative Rosemary Marshall
Representative Victor Mitchell
Senator David Schultheis
Senator Gail Schwartz
Senator Jack Taylor

Office of the State Auditor Staff

Sally Symanski
State Auditor

Cindi Stetson
Deputy State Auditor

Jonathan Trull
Rosa Olveda
Julian Ouellet
Kara Trim
Legislative Auditors

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

May 22, 2008

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of Colorado's driver's license and identification card issuance process. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government, and Section 42-1-220(2), C.R.S., which requires the State Auditor to submit a report ". . . concerning the effectiveness of the security features that are part of the driver's license system in reducing the incidence of issuance of fraudulent driver's licenses and identification cards." The report presents our findings, conclusions, and recommendations, and the responses of the Departments of Revenue and Public Health and Environment.

Sally Symanski

This page intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

STATE OF COLORADO
OFFICE OF THE STATE AUDITOR **REPORT SUMMARY**

SALLY SYMANSKI, CPA
State Auditor

Driver's License and Identification Card Security
Department of Revenue
Performance Audit
May 2008

Authority, Purpose, and Scope

This performance audit was conducted under the authority of Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct performance audits of all departments, institutions, and agencies of state government, and Section 42-1-220(2), C.R.S., which requires the State Auditor to submit a report ". . . concerning the effectiveness of the security features that are part of the driver's license system in reducing the incidence of issuance of fraudulent driver's licenses and identification cards." The audit work was conducted between December 2007 and May 2008 and performed in accordance with generally accepted government auditing standards.

Our audit reviewed the security features that are part of the driver's license and identification (ID) card issuance system. We also conducted a review of the information technology controls over the Driver's License Information System (DLS), including controls over computer applications, operating systems, databases, and network infrastructure. We gratefully acknowledge the assistance and cooperation extended by the staff of the Departments of Revenue and Public Health and Environment.

Background

During the 1990s individuals and criminal organizations exploited weaknesses in the State's driver's license and ID card issuance system to obtain hundreds of fraudulent Colorado driver's licenses and IDs. The perpetrators used the fraudulently issued driver's licenses and IDs to commit a range of financial crimes, including mortgage fraud, racketeering, check fraud, and identity theft. These crimes cost businesses, taxpayers, and the State thousands of dollars and required significant government resources to investigate. In July 2000 the Department of Revenue (the Department) formed the Identity Fraud Working Group (the Group) to address the weaknesses that existed in the Department's issuance system. The Group made ten recommendations to the Department to reduce the number of fraudulently issued Colorado driver's licenses and IDs.

The Group's recommendations resulted in legislative change; specifically, House Bill 01-1125 became law and amended Colorado statutes to (1) require the Department to verify that a first-time applicant meet certain age, identity, and residency requirements before it issued a driver's license or ID; (2) authorize an additional $0.60 security surcharge per license and ID to cover the costs of improvements to the Department's processes and to the physical security features of the licenses and IDs; (3) require the use of "appropriate and accurate technology and techniques" to verify license and identification information; (4) require the Department to add an invisible security feature to Colorado driver's licenses and IDs; and (5) prohibit a Colorado resident from holding both a driver's license and ID. The Department complied with House Bill 01-1125 by making several changes to its policies and procedures, instituting additional verifications of applicants' identities and lawful presence status, and improving the physical security features of the Colorado driver's licenses and IDs.

The Driver and Vehicle Services Section (the Section), administratively located within the Department of Revenue's Division of Motor Vehicles, is responsible for licensing drivers and providing IDs to Colorado residents. During Fiscal Year 2007, the Section issued a total of approximately 620,000 original and renewal driver's licenses and IDs from its 52 offices. For Fiscal Year 2008, the Section was appropriated $25.7 million and 374.2 full time equivalent staff to carry out its statutory responsibilities.

Summary of Audit Findings

Our audit identified areas of improvement related to the security features that are part of the driver's license and ID issuance system and to the information technology controls over DLS. Specifically, we found:

- **Driver's license examiners and supervisors do not always follow required procedures.** From our site visits to 13 driver's license offices and examination of DLS records, we found that driver's license examiners do not always conduct the required verification checks of an applicant's identity, driving status, and lawful presence. For example, between August 2006 and January 2008, the Department did not verify the lawful presence of 76 of about 34,000 applicants (0.2 percent) that presented immigration documents. Also, we found that supervisors at 5 of the 13 offices (38 percent) we visited failed to review the applications and supporting documents for each driver's license and ID before issuance, as required by Department procedures. Finally, we found that one half of the 18 examiners we tested were not proficient at identifying fraudulent identification documents provided by applicants to obtain a Colorado driver's license or ID.

- **The Department's controls for protecting the personal information of deceased individuals from identity theft are inadequate.** We matched death records from the Colorado Vital Information System with DLS records and identified about 48,000 active motor vehicle records belonging to deceased persons. In 24 cases, we found that the

personal information of deceased individuals had been fraudulently used to obtain driver's licenses or IDs. For these 24 cases, the licenses and IDs were issued from 5 days to more than 30 years after the deceased individuals' dates of death.

- **The Department does not have adequate processes for mitigating the risk of employee-perpetrated fraud or measuring the effectiveness of its improvements to the issuance system.** Specifically, we found that the Department does not adequately monitor the issuance activities of its employees, perform comprehensive background checks on job applicants, or monitor recurring criminal history checks for its employees. The Department also lacks the ability to track employee activities in DLS, which makes it difficult for the Department to identify anomalous practices, such as examiners issuing licenses and IDs after business hours. Finally, the Department lacks a tracking mechanism for collecting and analyzing statistics on the effectiveness of its controls for preventing fraudulent issuances. As such, the Department cannot determine whether additional controls or system enhancements are needed.

- **The Department's management of information security is fragmented, disorganized, and poorly planned.** Specifically, we identified instances in which access to sensitive DLS data was not sufficiently restricted, system access was not revoked in a timely manner after users left employment or changed job duties, and data transmissions were not protected from unauthorized disclosure. For example, as of January 2008, we identified 33 former state employees who still had the ability to access the mainframe and DLS application to issue driver's licenses and IDs. We also found that the Department transmits personally identifiable information in approximately 100 large data batches in clear text, without encryption. These batch transmissions could be intercepted by unscrupulous individuals and expose Colorado residents to identity theft and other criminal activity.

- **The Department needs to improve its disaster recovery planning and testing related to DLS, restrict physical access to its data center, and improve its data center's fire suppression system and emergency procedures.** Specifically, we found that the Department could not fully restore DLS during the 2007 disaster recovery test because key production data were not being backed up. We also found that the DLS disaster recovery plan failed to include information required by State Cyber Security Policies and did not address the photo imaging system, which is managed by a third-party contractor. Finally, we determined that the Department needs to better monitor physical access to its data center, develop policies and procedures related to data center access and emergency procedures, and augment the data center's current sprinkler system with an inert gas-based fire suppression system.

Our recommendations and the responses of the Departments of Revenue and Public Health and Environment can be found in the Recommendation Locator and in the body of the report.

This page intentionally left blank.

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
1	24	Strengthen controls for ensuring driver's license examiners and supervisors comply with required procedures by updating the procedure manual, programming additional automated stops in the Driver's License Information System (DLS) computer application, providing relevant and timely training to examiners and supervisors, and monitoring compliance with issuance requirements.	Department of Revenue	Agree	June 2009
2	28	Strengthen controls over the motor vehicle records of deceased persons by verifying the status of applicants' social security numbers for renewal issuances, matching motor vehicle records to the death records maintained in the Colorado Vital Information System's database, and changing the status on the 48,000 records belonging to deceased individuals from active to inactive in the DLS database.	Department of Revenue Department of Public Health and Environment	Agree Agree	December 2008 June 2008
3	32	Strengthen controls for preventing and detecting employee-perpetrated fraud by tracking and analyzing data on driver's license and ID issuances and employee errors; programming audit trails in DLS to better track examiner activities; conducting fingerprint-based background checks on job applicants through the Colorado Bureau of Investigation, pursuing statutory change as appropriate; and defining the criminal background criteria that would disqualify an applicant from employment.	Department of Revenue	Agree	December 2008
4	34	Ensure compliance with statutory mandates for establishing Colorado residency by requiring applicants to furnish evidence of residency prior to issuing a Colorado driver's license or ID.	Department of Revenue	Disagree	--

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
5	37	Establish procedures and mechanisms to track the effectiveness of its controls over the issuance process for driver's licenses and IDs by tracking and quantifying the number of attempts to obtain a fraudulent driver's license or ID that were stopped by each internal control; developing a new case tracking database for the Motor Vehicle Investigations Unit and identifying and implementing procedures on the type and detail of data to be collected and summarized; and analyzing and using the information collected to improve internal controls, target staff training efforts, and support budget and planning decisions.	Department of Revenue	Agree	December 2008
6	44	Develop a comprehensive cyber security program that protects the data contained in crucial information systems, including DLS, against unauthorized access, disclosure, use, and modification or destruction. This should include establishing a centralized information security function managed by an Information Security Officer, as required by State Cyber Security Policies. In cooperation with the Governor's Office of Information Technology, correct the specific security deficiencies we identified during our audit, including developing a mechanism to manage user access to the DLS system, performing ongoing monitoring of user activities in DLS to identify anomalous activity and taking appropriate action, and encrypting all network transmissions of sensitive, personally identifiable information.	Department of Revenue	Agree	June 2009

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
7	48	Improve disaster recovery planning and preparedness for DLS by identifying and backing up all critical data sets necessary to fully recover DLS; developing sufficient, written disaster recovery test procedures; ensuring that disaster recovery tests include other DLS users and the Department's photo imaging system contractor in the testing procedures; and ensuring the disaster recovery plan includes all components required by the State's disaster recovery policy and tests connections to critical networks.	Department of Revenue	Agree	June 2009
8	50	Improve the physical access and environmental controls over the data center by restricting access to only those individuals who have an established and valid need to routinely access the data center; assigning a staff person to routinely review data center access records and follow up on unusual activity; developing policies, procedures, and training related to data center access and emergency procedures; and augmenting the current sprinkler system with an inert gas-based fire suppression system, once funding becomes available.	Department of Revenue	Agree	December 2008

This page intentionally left blank.

Overview of Driver's License and Identification (ID) Card Issuance in Colorado

Background

During the 1990s individuals and criminal organizations exploited weaknesses in the State's driver's license and identification (ID) card issuance system to obtain hundreds of fraudulent Colorado driver's licenses and IDs. The perpetrators used the fraudulently issued driver's licenses and IDs to commit a range of financial crimes, including mortgage fraud, racketeering, check fraud, and identity theft. These crimes cost businesses, taxpayers, and the State thousands of dollars and required significant government resources to investigate. In one such case, which occurred between October 1998 and June 2001, a single criminal enterprise passed more than 200 counterfeit payroll and business checks along the Front Range. Three perpetrators alone used approximately 60 fraudulently issued Colorado IDs to cash approximately 125 counterfeit checks. One victim (a local grocery chain) suffered losses in excess of $115,000.

The weaknesses that existed in the Department of Revenue's (the Department's) issuance system made it relatively easy to obtain multiple fraudulent driver's licenses and IDs. For example, the Department had few mechanisms for verifying the authenticity of applicants' identity documents or ensuring that an applicant's identity information was attached to only one photo record. Also, much of the Department's focus during this time was on improving customer service rather than strengthening the security of the driver's license and ID issuance process. Consequently, while individuals could receive a driver's license or ID with minimum inconvenience on the same day they submitted their applications, the same-day turn-around did not provide the Department sufficient time to verify each applicant's identity, age, and lawful presence.

In July 2000 the Department formed the Identity Fraud Working Group (Group) in response to the serious problems caused by identity theft and the significant economic loss and criminal activity associated with improperly-issued Colorado driver's licenses and IDs. The Group—consisting of representatives from financial institutions and financial services organizations, retail merchants, state and federal law enforcement agencies, and motor vehicle administrators—reviewed the processes and procedures involved in issuing motor vehicle documents and identified the extent and nature of the problems inherent in the licensing system. The Group

made ten recommendations to the Department for reducing the number of fraudulently issued Colorado driver's licenses and IDs. The Group's recommendations resulted in legislative change; specifically, House Bill 01-1125 became law and amended Colorado statutes to:

- Require the Department to verify that a first-time applicant for an instruction permit, driver's license, or ID meets certain age, identity, and residency requirements **before** it issues such license or ID.

- Authorize an additional $0.60 security surcharge per license and ID to cover the costs of improvements to the Department's processes and the enhanced security features incorporated on driver's licenses and IDs.

- Require the use of "appropriate and accurate technology and techniques" in verifying license and identification information.

- Require the Department to add to Colorado driver's licenses and ID cards an invisible security feature capable of authenticating the documents.

- Prohibit a Colorado resident from holding both a driver's license and an ID card.

The Department complied with House Bill 01-1125 by (1) identifying a set of credible breeder documents, which are documents that prove identity, age, and lawful presence; (2) instituting facial recognition technology, which compares an applicant's photo to all other photos in the driver's license database; (3) verifying each applicant's social security number with the U.S. Social Security Administration; and (4) moving to a central issuance process to allow time to verify an applicant's age, identity, and lawful presence before issuing a license or ID. The Department completed these improvements by November 2003. In August 2006 the Department also began verifying the authenticity of an applicant's immigration documents, as necessary, with the U.S. Citizenship and Immigration Services Agency.

Although the original impetus for reforming the driver's license system was the fraudulent issuance and misuse of Colorado licenses and IDs to perpetrate financial crimes, the events of September 11, 2001, and additional state and federal laws greatly increased the Department's responsibility for authenticating identity and lawful presence before issuing Colorado driver's licenses or IDs. For example, the Colorado Secure and Verifiable Identity Document Act (Act) [Section 24-72.1-101, C.R.S.], which became law in 2003, requires that the Department rely only on secure and verifiable identity documents to issue a Colorado driver's license or ID. Under the Act, a secure and verifiable identity document is "a document issued by a state or federal jurisdiction or recognized by the United States government and that is verifiable by federal or state law enforcement, intelligence, or homeland security

agencies." Additionally, the federal government passed the United States Real I.D. Act of 2005 which imposes certain security, authentication, and issuance procedure standards on the State's driver's license and ID cards in order for them to be accepted by the federal government for "official purposes," as defined by the Secretary of Homeland Security. States were originally required to implement the Real I.D. Act by May 2008; however, the U.S. Department of Homeland Security agreed to extend the implementation date for those states requesting more time. Colorado requested and received approval to extend the implementation deadline of the Real I.D. Act to January 1, 2010.

Fraudulent Driver's Licenses and IDs

Throughout this document we will be referring to fraudulently issued driver's licenses and IDs. As used in this report, a fraudulently issued driver's license or ID is either a license or ID issued by the Department of Revenue to someone who is not qualified for the type of license or ID issued (e.g., not lawfully present, habitual traffic offender, minor issued an adult license), or a license or ID issued by the Department in the wrong name and/or containing the wrong date of birth for the applicant. For the license or ID to be fraudulently issued, the person applying for the driver's license or ID must have **intentionally and willfully** provided incorrect information to the driver's license examiner. Fraudulently issued driver's licenses and IDs result from a single applicant defeating the controls and security features of the driver's license and ID issuance process, by acting either alone or in collusion with a Department employee.

The Department issued approximately 620,000 original and renewal driver's licenses and IDs during Fiscal Year 2007, some portion of which were likely issued fraudulently. There is no single authoritative source on the number of fraudulently issued driver's licenses or IDs in Colorado; neither are there reliable data on the costs associated with fraudulently issued driver's license documents. However, a 2008 Federal Trade Commission (FTC) report on identity theft ranked Colorado first in the number of fraud complaints per capita and eighth in the number of reported identity thefts per capita. According to the report, the average cost of an identity fraud nationally between 2005 and 2007 was $2,500. Of the roughly 4,300 Colorado complaints filed with the FTC in 2007 we estimate that approximately 1 percent, or about 40 cases, involved fraud related to Colorado driver's licenses and IDs. This rate is similar to rates reported for other states.

Driver's License and ID Issuance Process

The process of applying for a Colorado driver's license or ID has several steps and can be divided into five phases: (1) initial applicant contact / breeder document review; (2) drive and written tests; (3) input and instant verification of data; (4)

supervisory review and capture of the applicant's photo, fingerprint, and signature; and (5) driver's license / ID production. We explain each of these phases in more detail below.

Initial applicant contact / breeder document review. During the first phase, the examiner collects basic information from the applicant and determines whether the written and drive tests are required. Next, as required by statutes [Sections 42-2-107 and 42-2-302, C.R.S.], the applicant provides documentation (known as breeder documents) to prove (1) identity, (2) age, and (3) lawful presence in the United States. Through its rule-making authority, the Department has established a list of acceptable breeder documents (see Appendix A). As will be discussed in Chapter 1, although the Department has identified acceptable breeder documents for age, identity, and lawful presence, it has not identified acceptable breeder documents for establishing Colorado residency. Driver's license examiners physically inspect breeder documents for counterfeiting or altering. If fraud is suspected, the examiner will follow the Department's fraud procedures, including confiscating the breeder documents and referring the case to the Motor Vehicle Investigations Unit.

If an applicant cannot provide the required breeder documents, the examiner refers the applicant to the Motor Vehicle Investigations Unit for exceptions processing. Exceptions processing is a separate process whereby the Department conducts additional review to determine whether applicants without proper documents are qualified for a driver's license or ID.

Written and drive tests. Adult applicants without valid driver's licenses from Colorado or another state are required to pass written and drive tests. Applicants who have **valid** driver's licenses, including licenses from other states, as well as those requesting a Colorado ID, are not required to take the written and drive tests.

Input and instant verification of data. If the examiner is satisfied the breeder documents are authentic, he or she will input basic information about the applicant into the Driver's License Information System (DLS), such as the applicant's name, date of birth, and social security number. Depending on the breeder documents provided to the examiner, DLS will then automatically interface with and query the Commercial Driver License Information System (CDLIS), Problem Driver Pointer System (PDPS), the Social Security Online Verification (SSOLV) system, and the Systematic Alien Verification for Entitlements (SAVE) Program. The results from each query are displayed for the examiner to review. Additionally, if the applicant provides an out-of-state driver's license or ID, the examiner is required to manually query the state-to-state license system (SG) and review the results. These various systems provide information that will enable the examiner to independently verify that the applicant is actually the person standing before the examiner and that the person is qualified to receive a license.

Supervisory review and capture of the applicant's photo, fingerprint, and signature. According to Department procedures, the driver's license office manager or a supervisor is required to verify the accuracy of the information the examiner entered into DLS and to check DLS to ensure the applicant meets all requirements and qualifications. Once the supervisory verification is completed, a driver's license examiner captures the applicant's facial image, fingerprint, and signature. The applicant then receives a temporary driver's license or ID.

Driver's license and ID production. Overnight, an adult, first-time applicant's facial image is automatically compared to all other images contained in DLS. The system is programmed to identify possible matches based on a proprietary algorithm that quantifies the physical dimensions of a person's face. If an applicant's facial image is unique and is not connected to any other driver's license or ID record other than the applicant's, the Department transmits the information to its contractor, located in Washington State. The contractor produces the driver's license or ID and mails it to the applicant. By contrast, if the applicant's facial image is not unique and appears to match a facial image attached to another driver's license or ID, Department staff are required to analyze the images and determine whether or not the same facial image is attached to more than one driver's license or ID record. If a match is confirmed, issuance of the driver's license or ID is stopped, and the Motor Vehicle Investigations Unit investigates the case.

Driver and Vehicle Services Section

In accordance with Title 42 of the Colorado Revised Statutes, the Driver and Vehicle Services Section (Section), administratively located within the Department of Revenue's Division of Motor Vehicles (Division), is responsible for (1) licensing drivers and providing IDs to Colorado residents, (2) managing the State's motor vehicle records, and (3) regulating commercial driving schools. For Fiscal Year 2008, the Section was appropriated $25.7 million and 374.2 full time equivalent staff (FTEs) to carry out its statutory responsibilities.

The Department issues licenses and IDs at the Section's 52 offices (see Appendix B) for a listing of all offices and issuance data). Thirty-five of the offices are managed by the State, and 17 are managed by counties operating under a Memorandum of Understanding with the Department. The Section works closely with the Division's Motor Vehicle Investigations Unit (Unit). The Unit investigates crimes involving the fraudulent issuance of Colorado driver's licenses and IDs, administers the driver's license and ID exceptions process, and makes the final determination on image matches produced by the Driver's License Information System's facial recognition tests.

As the table below shows, the Section expended about $24.3 million in Fiscal Year 2007, a decrease of 1 percent from Fiscal Year 2006. Between Fiscal Years 2004 and 2007 expenditures increased 8 percent, and the Section lost 3.4 FTEs. In Fiscal Year 2008 the Section received an appropriation of $2.7 million to add three driver's license offices along the Front Range. The Section also received an appropriation for an additional 53 FTEs, an increase of 17 percent from Fiscal Year 2007.

Colorado Department of Revenue
Driver and Vehicle Services Section
Expenditures and FTEs
Fiscal Years 2004 through 2007

	Fiscal Year				Percent Change Fiscal Year 2004-2007
	2004	2005	2006	2007	
Personal Services	$13,650,000	$13,960,000	$14,465,000	$14,536,000	6%
Operating Expenses	$8,713,000	$9,589,000	$10,010,000	$9,725,000	12%
Total Expenditures	$22,363,000	$23,549,000	$24,475,000	$24,261,000	8%
Appropriated FTEs	324.6	324.6	323.3	321.2	-1%

Source: Colorado Department of Revenue.

The Driver and Vehicle Services Section is funded with general fund, cash fund, and cash fund exempt moneys. The Section's $25.7 million appropriation for Fiscal Year 2008 included $18.9 million in general funds, $5.4 million from cash funds, and $1.4 million from cash fund exempt sources. Of the $1.4 million in cash fund exempt moneys, almost $520,000 or 37 percent, will come from the Identification Security Fund (Fund). House Bill 01-1125 (previously discussed) created the Fund to receive the moneys generated by the $0.60 security surcharge. Moneys from the Fund, upon appropriation by the General Assembly, are to be used to cover the costs associated with improving the security of the driver's license and ID issuance system. The security surcharge was originally set to expire on July 1, 2006; however, Senate Bill 06-013 extended the $0.60 security surcharge to July 1, 2009. The following table shows revenue, expense, profit/loss, and fund balance data for the Fund for the past three fiscal years.

Colorado Department of Revenue Identification Security Fund Summary of Revenues, Expenditures, and Net Profit/(Loss) Fiscal Years 2005 through 2007				
	Fiscal Year			Percent Change Fiscal Year 2005 - 2007
	2005	2006	2007	
Beginning Fund Balance	$738,410	$595,550	$568,770	-23%
Revenues	$528,980	$593,270	$567,260	7%
Expenses	$671,840	$620,050	$561,430	-16%
Net Profit/(Loss)	($142,860)	($26,780)	$5,830	104%
Ending Fund Balance	$595,550	$568,770	$574,600	-4%
Source: Office of the State Auditor analysis of COFRS reports and Department of Revenue data.				

Partnering Governments and Organizations

The Driver and Vehicle Services Section partners with local governments, federal agencies, and private organizations to accomplish its mission with respect to the issuance of Colorado driver's licenses and IDs. These partners include:

- **Colorado counties**. Most Colorado licenses and IDs are issued by state employees located in either state-owned or leased properties. Although the State maintains responsibility for licensing drivers and issuing state IDs, some Colorado counties perform the licensing and ID issuance functions on behalf of the State. To issue driver's licenses and IDs, the counties must enter into a standard Memorandum of Understanding (MOU) with the Department. Counties can choose to either renew driver's licenses and IDs only, or act as a full-service driver's license office issuing first-time licenses and IDs as well as renewals. According to the MOU, the counties are required to provide the office space and staff to operate the driver's license office, maintain security for the equipment and documents, and send employees to state-provided training. The State provides the counties with the training, equipment, and supplies necessary to issue Colorado driver's licenses and IDs, including communication lines to the Driver's License Information System. According to statute (Section 42-3-114, C.R.S.), counties that issue driver's licenses and IDs are authorized to retain $8.00 of the $20.40 fee for each driver's license and ID issued.

  As the regulations and scrutiny over driver's licensing and ID issuance have increased in recent years, several of the counties that previously issued

driver's licenses and IDs have elected to return this function to the State. As of May 2008, 13 Colorado counties continue to issue driver's licenses and IDs at a total of 17 offices. These counties and the type of services they provide are listed in the table below.

Colorado Department of Revenue
County-Operated Driver's License Offices
As of May 2008

	County	Number of Offices	Type (Renewal or Full-Service)		County	Number of Offices	Type (Renewal or Full-Service)
1	Arapahoe	2	Renewal	8	Lincoln	1	Full-Service
2	Baca	1	Full-Service	9	Phillips	1	Full-Service
3	Cheyenne	1	Full-Service	10	Saguache	1	Renewal
4	El Paso	3	Renewal	11	Sedgwick	1	Full-Service
5	Kiowa	1	Renewal	12	Washington	1	Full-Service
6	Kit Carson	1	Full-Service	13	Yuma	2	Full-Service
7	Lake	1	Full-Service				

Source: Colorado Department of Revenue.

- **United States Citizenship and Immigration Services Agency**. The Section has entered into a Memorandum of Understanding with the U.S. Citizenship and Immigration Services Agency to access information contained in the Verification Information System database through the Systematic Alien Verification for Entitlements Program. The SAVE Program enables the Section to obtain the immigration status information necessary to determine whether a non-citizen applicant is lawfully present and thus, eligible for a Colorado driver's license or ID.

- **American Association of Motor Vehicle Administrators (AAMVA)**. Founded in 1933, AAMVA is a nonprofit organization that develops best-practice models for motor vehicle administration, law enforcement, and highway safety. Among these best practices are those designed to enhance driver's license and ID security. Additionally, AAMVA develops and maintains a number of information systems facilitating the electronic exchange of information among the states and between the states and the federal government. The Driver and Vehicle Services Section utilizes several of AAMVA's information systems, including the Commercial Driver License Information System, Problem Driver Pointer System, Social Security

Online Verification system, and the state-to-state license verification system. These systems and their purposes will be discussed in more detail later in the report.

Audit Scope and Methodology

Section 42-1-220(2), C.R.S., requires the State Auditor to evaluate "the effectiveness of the security features that are part of the driver's license system in reducing the incidence of issuance of fraudulent driver's licenses and identification cards" and submit a report to the Transportation Legislation Review Committee by July 1, 2008. To fulfill this mandate, we reviewed documentation and interviewed personnel in the Department of Revenue with respect to policies and procedures and security features for driver's license and ID card issuance; performed detailed analyses of the more than 3.4 million active records contained in the Driver's License Information System database; conducted a review of information technology controls, including controls over the DLS computer application, operating system, database, and network infrastructure; surveyed and interviewed driver's license examiners, supervisors, and managers; tested controls and security features of the issuance process; and collected best-practice information from the American Association of Motor Vehicle Administrators. We also collected and analyzed information related to identity theft and fraudulently issued Colorado driver's licenses and IDs from the Colorado Attorney General's Office, Federal Trade Commission, and the Colorado Judicial Branch.

Our review included site visits to 13 driver's license offices throughout the State. The offices we reviewed issued 40 percent of all Colorado driver's licenses and 54 percent of all IDs issued in Fiscal Year 2007. While at the driver's license offices, we interviewed 21 examiners and 12 supervisors, observed the issuance of 138 driver's licenses and IDs, and evaluated the physical security of the office locations. Appendix B provides issuance information about the driver's license offices statewide; offices visited during the audit are highlighted.

Our audit did not include a review of the security features over the issuance of instruction permits and commercial driver's licenses; nor did we go beyond the security features and controls intended to prevent the issuance of fraudulent driver's licenses/IDs to focus on other types of fraud that can involve a Colorado driver's license or ID, such as:

- **Counterfeiting:** The construction or production of driver's licenses or IDs by someone other than the Department of Revenue or its authorized agents. An example of counterfeiting would be a person using desktop publishing software to produce a fraudulent driver's license or ID from his or her home computer.

- **Forgery:** The fraudulent alteration of an authentic driver's license or ID. An example of forgery would be a person altering their name or age on an authentic driver's license.

- **Imposters:** The use of authentic driver's licenses or IDs by people falsely representing themselves as the legitimate document holders.

These types of fraud were not included within the scope of our audit because the driver's licenses and IDs were not fraudulently issued by the Department. Rather, the documents were either wholly created by the perpetrator, the perpetrator altered a properly-issued driver's license or ID, or the perpetrator attempted to misuse a properly-issued driver's license or ID.

Finally, our audit did not include a review of the Department's compliance with the Secure and Verifiable Identify Document Act. Statute requires our Office to conduct a review of state agencies' and institutions' compliance with the Act. That audit is underway and the report will be released in 2008.

Driver's License Security

Chapter 1

The Department of Revenue (Department) has been entrusted with taxpayer dollars, personnel, and other resources to design and implement a security framework to reduce the number of fraudulently issued Colorado driver's licenses and identification (IDs) cards. In total the Department reports spending about $3.2 million between Fiscal Years 2002 and 2007 to address the security mandates outlined in House Bill 01-1125. Since the passage of the legislation in 2001 the Department has improved the security features associated with both its driver's license/ID issuance process and the physical composition and design of Colorado's driver's licenses and ID cards. The improvements made by the Department provide greater assurance that the risks of fraudulently issued driver's licenses or IDs have been lessened.

The improvements the Department has made to the issuance process include the implementation of facial recognition analysis and electronic verification of social security numbers and immigration documents; a reduction in the types of documents that are acceptable for proving identity, age, and lawful presence; and the adoption of requirements for additional supervisory review. The Department also centralized the issuance system so that, rather than each driver's license office producing and issuing licenses and ID cards, all licenses and IDs are now produced at a single, secure, out-of-state location. In addition to these process improvements, the Department enhanced the physical composition and design of the Colorado driver's license and ID. The changes to the documents' physical attributes, such as watermarks, make it more difficult to counterfeit or alter them without detection.

Section 42-1-220 (2), C.R.S., requires the State Auditor to submit a report ". . . concerning the effectiveness of the security features that are part of the driver's license system in reducing the incidence of issuance of fraudulent driver's licenses and identification cards." In this chapter we provide the results of our review in accordance with this statutory charge. Overall, we concluded that the security features the Department has adopted are sound controls for reducing the risks for fraud, including the risks associated with fraudulently issued driver's licenses and ID cards. However, we identified areas in which these controls and other aspects of the issuance process need to be strengthened or brought into compliance with law. It is difficult to specifically quantify whether the Department's security features have reduced the incidence of fraudulently issued licenses and IDs. Complete data on the number of fraudulently issued documents are not available, and various factors, some of which are outside the Department's control, can affect whether or not fraudulently

issued driver's licenses and IDs are discovered and reported. Nonetheless, we believe the Department has a responsibility to provide assurances about the effectiveness of its efforts and to justify the expenditure of tax dollars intended to increase the security of Colorado's driver's license issuance system.

Issuance Security

A fundamental component of the Department's driver's license and ID card security framework is a system of integrated internal controls. These internal controls include specific procedures that Driver and Vehicle Services Section (Section) employees are required to follow when issuing licenses and IDs. Employee compliance is critical, because the procedures are designed to validate applicant qualifications, including age, identity, lawful presence, and driving record. When examiners and supervisors do not follow the procedures, the security of the issuance process is compromised, thereby reducing its effectiveness.

We reviewed staff compliance with the Department's required procedures for issuing driver's licenses and IDs. Overall, we found that the driver's license examiners and supervisors, who are directly responsible for processing and approving applications for Colorado driver's licenses and IDs, do not always follow required procedures. This lack of uniform and consistent compliance increases the risk that fraudulent driver's licenses and IDs will be issued by the Department's 52 driver's license offices. We identified several areas of noncompliance and other weaknesses that negatively impact the effectiveness of the Department's controls:

- **Verification of applicants' personal information**. Department procedures require driver's license examiners to electronically verify specific personal information about license and ID applicants. Examiners are to verify applicants' social security numbers with the U.S. Social Security Administration, out-of-state driver's licenses with the Association of American Motor Vehicle Administrators (AAMVA), and, if necessary, lawful presence status through the U.S. Citizenship and Immigration Services Agency. Also, examiners are to review applicants' driving records through AAMVA's Problem Driver Pointer System and its Commercial Driver License Information System.

  During our site visits to 13 driver's license offices, we found that driver's license examiners do not always conduct the required checks. Staff from one driver's license office we visited informed us that none of the examiners in that office perform the out-of-state license verifications. From a random sample of 39 records in which applicants presented out-of-state driver's licenses or IDs, we found that this problem is not confined to this one office. Rather, we found that examiners in seven other offices failed to perform the

out-of-state license verifications in 8 of the 39 cases (21 percent) we reviewed.

Furthermore, we found that examiners issue driver's licenses and IDs when the information systems supporting the electronic verification systems are not working. We identified a day in January 2008 when driver's license examiners issued 63 driver's licenses or IDs even though they were unable to complete the required verifications because the systems were not working.

Finally, we found that examiners do not always comply with Department procedures for verifying a person's lawful presence status. Our analysis revealed that, between August 2006 and January 2008, the Department did not verify the lawful presence of 76 of about 34,000 applicants (0.2 percent) who presented immigration documents. The verifications did not occur because examiners entered the immigration document information into the wrong field within the Driver's License Information System (DLS). Entering the data into the incorrect field circumvents the verification process and allows the driver's license/ID to be issued without lawful presence being established. We could not determine whether these data entry problems were intentional or erroneous. We provided the Department with the 76 records and the Department completed the lawful presence checks. In one case, the verification system rejected the immigration information. Consequently, Department staff report that they have requested this ID holder return to the office to resolve this problem.

- **Facial image verification.** Before they renew a driver's license or ID, examiners are required to verify that the facial image stored in DLS matches the applicant presenting himself or herself before the examiner. During our site visits, we observed that examiners did not verify facial images in 5 of the 93 cases (5 percent) in which such verification was required.

- **Supervisory review.** Department procedures require driver's license office supervisors to review the computer records of each driver's license and ID issued before the applicant leaves the office. Such reviews are intended to ensure that only qualified applicants are licensed and to deter examiner-perpetrated fraud. Supervisors should review the records for items such as data entry errors, verification of personal information, and whether examiners have properly reviewed and handled any holds or restraints on applicants' driver's license records. Through interviews and observations, we found that supervisors at 5 of the 13 offices (38 percent) we visited either never reviewed the computer records or reviewed the records sporadically. For example, the supervisor at the State's busiest driver's license office in Denver, which issued approximately 39,600 driver's licenses and 17,810 IDs in Fiscal Year 2007, told us that he never reviews the computer records. It

should be noted that this particular office has experienced employee-perpetrated fraud in the past. According to Department management, office supervisors are also required to periodically review the breeder documents presented to examiners. During our site visits, we observed that the supervisors at 7 of the 13 offices, or 54 percent, did not review any breeder documents.

- **Document identification.** Driver's license examiners are required to carefully review the breeder documents presented by applicants and to physically inspect the documents to confirm their authenticity. Physical inspections include verifying watermarks and seals and the texture or composition of the paper upon which the documentation is imprinted. In several instances, we observed examiners who did not perform these inspections. In addition, to test the examiners' competence in identifying fraudulent documents, we obtained both authentic and fraudulent breeder documents from the Motor Vehicle Investigations Unit. We provided 18 different examiners with 10 breeder documents and asked them to determine whether the documents were authentic or fraudulent. One half of the examiners failed to identify the fraudulent breeder documents in accordance with criteria set by the Department.

The failure of driver's license examiners and supervisors to comply with the Department's requirements is a concern and indicates the need for strengthened controls in several areas. Additionally, our analysis points to an absence of adequate oversight of driver's license offices on the part of the Department. Until we brought the areas of noncompliance to the Department's attention, management was unaware of these issues. The Department needs to make improvements in several areas to ensure the effectiveness of the security features that have been implemented over the issuance process.

First, the Department should adopt clear and complete written procedures for use by driver's license examiners and supervisors. Driver's license examiners and supervisors report that the Department's issuance procedures are sometimes unclear because not all procedures are included in the manual. For example, examiners report that they are to use AAMVA's state-to-state verification on both out-of-state driver's licenses **and** IDs; however, the procedure manual only requires the verification on out-of-state licenses. Written procedures should clearly describe how and when to perform each step of the issuance process, including all electronic verifications and supervisory reviews of computer records and breeder documents. The Department should also streamline the way in which it communicates procedural changes by simultaneously disseminating both the revised manual section and a memorandum detailing changes to examiners. Currently the Department's procedure is to issue only memorandums and then make changes to the manual at a later date.

Second, the Department should address the lack of automated computer stops within the electronic issuance system. An automated stop is a computer program that prevents actions, such as the issuance of a driver's license, from occurring unless specific conditions are met. Automated stops would act as transaction controls, ensuring that examiners meet predetermined conditions and that they cannot proceed without supervisory approval. Automated stops can prevent data entry errors and reduce the risks of employee-perpetrated fraud. With respect to all issuances, the Department should consider programming automated stops in DLS related to successful completion of (1) all verifications of personal information and (2) supervisor reviews. The Department should also implement automated stops for supervisor review of breeder documents for first-time issuances and verification of applicants' facial images for renewals.

Third, the Department could strengthen compliance with issuance requirements by providing more timely and relevant training to its driver's license examiners and supervisors. The Department provides examiners with training on issuance procedures and fraudulent document recognition soon after they are hired. However, the Department does not update or repeat the training. In addition, upon promotion, supervisors receive generic supervisory skills training. The Department should modify this training to include specific information on the supervisors' new duties related to overseeing the business operations of the driver's license offices and conducting document and computer record reviews.

Finally, the Department needs to improve its oversight of the driver's license offices by developing a comprehensive monitoring program. The Department does not conduct any regular reviews or internal audits of the operations of the driver's license offices. For example, the Department needs to conduct regular audits of each office, including bi-annual on-site audits of each county office as required by the Memorandums of Understanding with the counties. As part of each audit, the Department should evaluate employee and supervisor compliance with the procedural requirements, identify best practices, and note deficiencies. Problems and concerns should be addressed through corrective action plans with appropriate follow-up. Audit findings should be regularly reviewed by management to identify statewide areas of concern, needed improvements, and topics for refresher training.

Additionally, the Department should ensure that regional driver's license office supervisors regularly visit each office within their respective jurisdictions. During these visits, regional supervisors could conduct desk reviews, observe operations, and interview staff. The reviews should be documented and identified problems should be addressed. Records documenting the reviews should be maintained for future reference.

In addition to the weaknesses we identified in procedural controls, the Department reports that high turnover among license examiners contributes to compliance

problems. Specifically, according to Department personnel, attracting and retaining competent and dedicated driver's license examiners has become an increasingly difficult task. The responsibilities of driver's license examiners have expanded significantly as a result of the increased focus on document security and verification and the associated risks of identity theft. However, according to Department staff, there has been neither a corresponding increase in the status of the examiner position nor its pay. The Department indicates that an annual turnover rate in excess of 60 percent among driver's license examiners makes timely training and supervision difficult.

We recognize that problems associated with high turnover are a legitimate concern. If the Department believes that turnover contributes to compliance weaknesses then it should take corrective action in this area. One possibility is for the Department to evaluate the current position description for driver's license examiners to ensure the description is accurate and comprehensive with regard to all significant responsibilities. Correspondingly, market salary data should be analyzed in light of these responsibilities, and appropriate budget requests and salary adjustments made. Regardless of staffing concerns, the Department needs to take the steps we have outlined to ensure the security and integrity of the driver's license and ID issuance process.

Recommendation No. 1:

The Department of Revenue should improve the security of the driver's license/ID issuance process by strengthening controls for ensuring that driver's license examiners and supervisors are complying with required procedures. Specifically, the Department should:

a. Update the procedure manual to ensure that all requirements are clearly stated.

b. Program additional automated stops in the Driver's License Information System computer application to prevent issuance unless specified conditions are met.

c. Provide relevant and timely training to examiners and supervisors on an ongoing basis.

d. Monitor the operations of driver's license offices to assess compliance with issuance requirements, and follow up and resolve any problems identified.

Department of Revenue Response:

a. Agree. Implementation date: June 2008.

The Department of Revenue uses memoranda as a way to disseminate procedural changes quickly to all the driver's license offices. This form of communication can be disseminated the same day as the procedural change. The process to update the procedure manual can take up to three weeks from start to finish and includes: updating the document, reviewing and approving the changes, printing, and distributing the manual to all the offices. Due to Cyber Security, driver's license offices do not have access to the Internet and there is typically only one computer in the office with access to the Department's intranet site. Since system access is not readily available to all driver's license examiners, the Department produces and provides hard copies of the manual. The Department agrees the procedure manual should include all requirements in a clear fashion. The procedure manual will be updated by June 2008 to clarify that the out-of-state verification check also applies to IDs. In the future the Department will update the procedure manual as changes occur rather than waiting until there are numerous changes.

b. Agree. Implementation date: June 2009.

The Department will perform an application analysis by June 2009 to determine the extent to which automated stops can be incorporated into the Driver's License Information System computer application. Changes will be implemented to the extent they are justified based on costs and benefits.

c. Agree. Implementation date: June 2009.

The Department started a comprehensive training course for all examiners and supervisors in April 2008. The Department projects all employees will attend the training by June 2009. The Department will also provide refresher training classes each month.

d. Agree. Implementation date: June 2008.

The Department requires the regional managers to conduct monthly audits of each facility and submit the audit report to Driver's License Administration for review. The Department agrees the audit process could be improved and will update the audit procedures by May 2008.

Additionally, a reporting mechanism will be developed by June 2008 to track the report submittals and findings.

Death Records

The Department of Revenue has a responsibility to protect license holders' personal information. For example, Section 42-2-107 (3)(a), C.R.S., states that an application for a driver's license **shall include the applicant's social security number, which shall remain confidential**. This responsibility has become even more significant in recent years due to the increasing incidence of identity theft. Identity thieves often target the identity of a deceased individual because the fraud is less likely to be detected than when the victim is alive. To make the impersonation convincing, the perpetrator needs to obtain fraudulent identification documents, such as a driver's license, using the deceased's personal information. Best practices dictate that motor vehicle administrators implement processes to proactively identify, code, and protect the motor vehicle records of the deceased to prevent perpetrators from using these records to assume the deceased's identity. Additionally, state statute [Section 24-37.5-401 (1) (b), C.R.S.] provides that "state government has a duty to Colorado's citizens to ensure that the information the citizens have entrusted to public agencies is safe, secure, and protected from unauthorized . . . use . . . ."

We evaluated the Department's controls for protecting the personal information of deceased individuals and found the controls to be inadequate to sufficiently mitigate this type of identity theft. We arrived at this conclusion by comparing the more than 3.4 million active motor vehicle records in the Department's Driver's License Information System database with the death records in the Colorado Department of Public Health and Environment's Colorado Vital Information System's database. Our data match identified about 48,000 active motor vehicle records belonging to deceased persons. Working with Department staff, we determined that, for the vast majority of these records, no evidence of motor vehicle license-related identity theft had occurred. Rather, as will be discussed in more detail below, the records remained active because Department staff had not been notified by the document holders' families that these 48,000 individuals were deceased.

However, in 24 cases we found that the personal information of deceased individuals had been fraudulently used to obtain driver's licenses or IDs. Our comparison of the dates of death with the dates the licenses or IDs were issued for these individuals revealed that the Department had issued 24 driver's licenses or IDs after the dates of death. The periods between the dates of death and the dates the Department issued the licenses ranged from 5 days to more than 30 years. We provided the Department's Motor Vehicle Investigations Unit with the 24 records for further investigation. It is important to note that the Department of Public Health and

Environment's vital records database contains only the records for people who have died in Colorado. As such, it is possible that additional Colorado motor vehicle records belonging to individuals who died elsewhere remain active in the Department's motor vehicle database. Therefore, the identities of these deceased individuals could also be vulnerable to theft.

The Department's controls for preventing the theft of deceased individuals' identities are inadequate for two reasons. First, the Department does not verify social security numbers for license and ID renewal. As detailed previously, applicants for new licenses or IDs must provide their full names, social security numbers, and dates of birth. Prior to issuing the driver's license or ID, the driver's license examiners must electronically verify applicants' social security numbers with the U.S. Social Security Administration (SSA). If a social security number belongs to a deceased individual, the SSA electronically notifies the examiner and DLS automatically stops the issuance. By contrast, when an applicant applies for renewal, the Department does not re-verify the social security number. Therefore, if someone posing as a deceased Colorado license holder applies for license renewal, the Department would not identify the fraudulent use of the social security number.

The second reason controls in this area are inadequate is that the Department is not proactive in identifying deceased license or ID holders. Rather, the Department relies on family members of deceased individuals to notify it of document holders' deaths. For the motor vehicle record to be removed from the active license-holder category, the Department requires a family member to provide a certified death certificate. Upon receipt of the certificate, Department staff electronically indicate the deceased status of the license-holder on the electronic motor vehicle record. The system is programmed to prevent future issuance of a license or ID to this individual. Department staff report that they rarely receive death notifications from family members. Consequently staff estimate that DLS likely contains thousands of active records belonging to deceased Colorado license and ID holders, which was confirmed by our testing.

Verifying applicants' social security numbers for renewals and identifying active motor vehicle records belonging to deceased persons are two steps the Department should take to better fulfill its responsibility to prevent identity thieves from fraudulently obtaining Colorado driver's licenses and IDs. The first step the Department should take is to program its DLS computer application to verify social security numbers for renewals. Second, rather than relying on family members to notify it of the license and ID holders deaths, the Department should actively pursue this information. This should be done by periodically matching motor vehicle records against the death records maintained by the Colorado Department of Public Health and Environment and the Social Security Administration. We contacted staff at the Department of Public Health and Environment who indicated that periodic data matches could be conducted at minimal cost. Additionally, the Department should

immediately act on the 48,000 records we identified by changing the status in the motor vehicle record from active to inactive for these deceased individuals.

Recommendation No. 2:

The Department of Revenue should strengthen controls over the motor vehicle records of deceased persons by:

a. Programming the Driver's License Information System application to verify the status of applicants' social security numbers with the U.S. Social Security Administration for renewal issuances.

b. Working with the Colorado Department of Public Health and Environment to periodically match motor vehicle records to the death records contained in the Colorado Vital Information System's database.

c. Changing the status on the 48,000 records we identified as belonging to deceased individuals from active to inactive in the Driver's License Information System database.

Department of Revenue Response:

a. Agree. Implementation date: December 2008.

The Department agrees checking social security numbers for each renewal would strengthen controls over the issuance of driver's licenses. The Department estimates this additional check will cost approximately $30,000 annually. If funding is available, a decision item for Fiscal Year 2010 will be submitted.

b. Agree. Implementation date: June 2008.

The Department recognizes the weakness in the area of updating the DLS database for deceased individuals. The Department has made attempts over the past several years to work with the Colorado Department of Public Health and Environment to obtain this information, but these efforts were not successful. As a result of this audit, it appears that the Colorado Department of Public Health and Environment has identified a method to assist with identifying individuals in DLS that are deceased. In June 2008 the Department will start the process to provide the Colorado Department of Public Health and Environment with our records to check for deceased individuals.

The Intelligence Reform and Terrorism Prevention Act required changes to the definition of the Social Security Online Verification reply codes effective April 1, 2006. The Department was informed at that time the Social Security Administration (SSA) receives reports of death from multiple sources and it cannot always verify the source of the death report or the report itself. Therefore, further action will be needed by the Department to verify identity of the individual when the SSA reply indicates the person with the assigned Social Security Number (SSN) is deceased. While the check with the SSA will indicate if the SSN information sent shows an indication of death present, it does not provide absolute assurance the individual is deceased.

c. Agree. Implementation date: June 2008.

The Department will work with the Vital Records Section to run the entire DLS database against Vital Records' Mortality Data for Colorado to include all expired documents as well as active documents and will validate the information prior to updating the Department's records. Once the initial comparison is completed, the Department will further check the records for activity that occurred after the date of death and these cases will be referred to the Motor Vehicle Investigations Unit. The comparisons will begin in June 2008.

Department of Public Health and Environment Response:

(Parts a. and c. were not addressed to the Department of Public Health and Environment.)

b. Agree. Implementation date: June 2008.

The Colorado Department of Public Health and Environment (CDPHE) agrees with the desire to periodically match motor vehicle records to the death records contained in the Colorado Vital Information System's database. CDPHE will work with the Department of Revenue to negotiate a mutually agreeable process for CDPHE to conduct such matches. In addition to deaths occurring in Colorado, CDPHE will also match against death records from other jurisdictions within the limitations established by the Inter-jurisdictional Exchange Agreement of the National Association for Public Health Statistics and Information Services (NAPHSIS).

Risk of Employee-Perpetrated Fraud

The potential for driver's license and ID fraud is not limited to perpetrators from outside the motor vehicle system. The commission of internal fraud by Department employees who intentionally issue fraudulent Colorado driver's licenses or IDs is a real risk. Moreover, the costs and risks associated with employee fraud can be significant because Department employees can exploit their knowledge and access to issue countless fraudulent licenses as compared with the single fraud typically committed by an outsider. Although the Department's internal controls discussed earlier in this chapter are designed to act as deterrents to all fraud, including employee fraud, there are controls that specifically target the risk of fraudulent acts by employees. In this section, we discuss these additional controls and procedures.

On average, the Division of Motor Vehicles has experienced one employee-perpetrated fraud per year since 2000. In 2004 one case resulted in almost 400 fraudulently issued Colorado commercial driver's licenses, and required approximately 300 hours of investigation by the Department's Motor Vehicle Investigations Unit. The market value of fraudulently issued identification documents serves as a lucrative incentive for employees to commit fraud. Therefore, it is imperative that the Department develop strong controls focused on deterring, preventing, and detecting employee fraud.

As part of our audit, we reviewed the Department's controls related to the prevention of employee fraud and found that the Department needs to address the following weaknesses:

- **Employee issuance activities are not adequately monitored.** Our analysis of the DLS database identified three instances in which driver's licenses or IDs were issued on weekends when driver's license offices were closed. The Department was unaware of these issuances because it does not track and analyze data to detect anomalous employee behavior. In one case, the driver's license office manager issued the license to his wife, despite Department policy expressly prohibiting staff from issuing licenses and IDs to family members. We provided the records of all three issuances to the Department for further investigation. The Department should monitor and investigate driver's license issuances that occur during hours when driver's license offices are closed. The Department should also be concerned if an employee has a pattern of accepting a high volume of immigration papers or out-of-state birth certificates that cannot be verified electronically. Tracking the frequency of each type of breeder document that employees enter into the system would identify anomalous patterns and help to direct the Department's audit and investigative efforts. Finally, the Department does not track recurring employee errors. An important element of detecting employee

fraud is proactively identifying and investigating recurring and suspicious problems.

- **The Driver's License Information System does not track the actions taken by individual employees on license and ID applications.** That is, DLS does not have automated audit trails that record employee activities. This makes it difficult to determine if examiners are intentionally disregarding issuance procedures or issuing driver's licenses or IDs after business hours. For example, DLS does not maintain a record of the time of day that driver's licenses and IDs are issued. Additionally, DLS does not track whether or not an examiner performed the required verification with the U.S. Citizenship and Immigration Services Agency. The Driver and Vehicle Services Section staff should work with Department IT programmers to add audit trails to DLS, including information related to the electronic verifications performed by each employee, the results of the verifications, and the subsequent actions taken by examiners and supervisors.

- **Employee background checks are not comprehensive.** The Department's employee background checks are not current or comprehensive and lack the necessary criteria for identifying unacceptable criminal or ethical behavior. Background checks are limited to Colorado criminal and civil court cases and therefore do not provide comprehensive coverage, because crimes committed in other states or at the federal level are not identified. Additionally, the background data are often outdated. Also, the Department has no established criteria by which it disqualifies job applicants based on the results of the applicants' background checks. Rather, the Department makes hiring decisions on a case-by-case basis. This presents the risk that the Department may not apply background information uniformly when making hiring decisions and could therefore be exposed to legal action. Finally, the Department does not conduct periodic background checks on employees after they have been hired. Therefore, crimes committed during the period of employment are not identified and evaluated by Department management. For employees involved with the issuance of driver's licenses and IDs, the Department should begin conducting fingerprint-based background checks through the Colorado Bureau of Investigation (CBI), including flagging employee records for notification of future arrests. Background checks performed by CBI provide information on arrests and convictions in both Colorado and nationwide. To perform these checks, the Department will need to seek statutory authority. The Department should also identify criminal activities, such as convictions for fraud, forgery, or embezzlement, that might exclude an applicant from being hired, and should document those criteria.

The need for a comprehensive monitoring program, including the supervisory review and internal audits previously discussed in this chapter, is also specifically applicable to identifying and lessening the risk of employee fraud. Employee knowledge of ongoing Department monitoring through routine supervisory review and internal audits provides a sentinel effect and is an effective mechanism for reducing the incidence of employee fraud.

Recommendation No. 3:

The Department of Revenue should strengthen its controls for preventing and detecting employee-perpetrated fraud by:

a. Tracking and analyzing data on driver's license and ID issuances and employee errors to identify suspicious or irregular employee activities.

b. Programming audit trails in the Driver's License Information System to better track examiner activities.

c. Conducting fingerprint-based background checks on job applicants through the Colorado Bureau of Investigation, flagging employees' records for notification of future criminal activity, and pursuing statutory change as appropriate.

d. Defining the criminal-background criteria that would disqualify an applicant from employment.

Department of Revenue Response:

a. Agree. Implementation date: July 2008.

Due to the Department's current program structure, there is no systemic tool available to track and analyze this information. Managers currently manually review employees' issuances for errors and document such errors on performance management forms maintained in the employee's file. When errors appear to be recurring, the manager refers the employee to Driver License Administration for possible further corrective or disciplinary action. The Department will create a database to track employee errors by July 2008, which will allow for the analysis of suspicious or irregular employee activities.

b. Agree. Implementation date: July 2009.

The Department will perform an analysis of DLS to determine the extent to which the system can be modified to implement an audit trail and the related costs by July 2009. DLS is a mainframe system that does not lend itself to ad hoc reports. The requested audit trails could result in significant additions and modifications to the existing system. The Department will implement changes to the extent they are justified based on costs and benefits.

c. Agree. Implementation date: December 2008.

The Department agrees with the importance of performing fingerprint-based background checks on job applicants and believes checking the national database is most effective. The Department does not currently have funding to cover such an expense and will consider submitting a decision item for Fiscal Year 2010.

d. Agree. Implementation date: July 2008.

The Department will define the criminal background criteria that would disqualify an applicant from employment by July 2008.

Colorado Residency

By statute only a Colorado resident may obtain a Colorado driver's license or ID. Statute [Section 42-1-102(81), C.R.S.] defines a Colorado resident as "any person who owns or operates any business in this state or . . . has resided within this state continuously for a period of ninety days or has obtained gainful employment within this state, whichever shall occur first." Before the Department can issue a driver's license or ID, statute [Sections 42-2-107(1)(d) and 42-2-302(2)(c)(I), C.R.S.] requires the applicant to furnish "such evidence of residency as the department may require."

We found that the Department does not do enough to substantiate the Colorado residency of driver's license and ID applicants, and therefore, it is not fulfilling this mandate. The Department's procedures for establishing residency are twofold. First, staff ask the applicant whether he or she is a resident. Second, the applicant is asked to provide a Colorado-resident address. This address must be physically located in Colorado. Additionally, the applicant can provide a mailing address which can be in-state, out-of-state, or international. The Department requires no further proof of residency. We believe these procedures are inadequate for several reasons. In the

absence of additional verification, a verbal affirmation of Colorado residency is not sufficient "evidence of residency" as mandated by statute. Furthermore, even if the Colorado address is valid, it does not ensure the applicant is residing in the State, has resided in the State for the prescribed 90 days, or owns or operates a business in the State. Finally, the Department's acceptance of out-of-state and international mailing addresses raises obvious questions about the applicant's true residence.

We contacted 11 states and found that 7 require driver's license applicants to present written documentation of residency. Among the seven states, Utah requires applicants to provide one of several approved documents including: property tax notices, utility bills, non-expired vehicle registrations or titles, bank statements issued within the past 60 days, residential leases, recent mortgage papers, court orders of probation or release containing the applicant's residence address, school transcripts, or any other documents that unequivocally demonstrate proof of residency.

We believe the Department should strengthen its procedures for establishing residency and require applicants to furnish documentary evidence of such residency prior to issuing a Colorado driver's license or ID, as specified by statute. To do this, the Department should amend its rules to include a list of acceptable documents. To identify acceptable documents, the Department should review the documentation requirements of other states with similar residency requirements.

Recommendation No. 4:

The Department of Revenue should ensure compliance with statutory mandates for establishing Colorado residency by requiring applicants to furnish evidence of residency before it issues them a Colorado driver's license or ID. This should include identifying the specific types of documentation that will be allowed as proof of residency and amending its rules accordingly.

Department of Revenue Response:

Disagree.

The Department disagrees with this recommendation. Over the course of time, the Department has attempted to comply with this statutory requirement with little success. Compliance with this law by means of requiring some paper proof of a residence address is infeasible. The types of documents that can and are used to prove residency are difficult, if not impossible, for some applicants to obtain. Additionally these documents do not have security features nor can they be verified. Thus, under these circumstances, there is

little or no value-added to the integrity of the process using these documents. Such documents as apartment leases and utility bills are easily scanned and names changed. The Department has no means by which to assure the documents are valid. Also there are no available documents for people who live with friends, relatives with different last names, and others similarly situated, since they have no means by which to prove their residency.

While the Department agrees that it is important to process only applicants who are Colorado residents, we believe the most effective way to assure that people live in Colorado is through the central license issuance process, whereby the document is mailed to an address provided by the applicant. This method is not fool-proof, but is as effective as requiring provision of apartment leases, or bills mailed to a person at a given address. As a result, the Department believes this approach is functionally equivalent to having the applicant provide proof of residency by providing a piece of mail to him/herself at the address provided to prove residency.

Measuring Effectiveness

The Department has a responsibility to evaluate the effectiveness of its controls and to use its evaluations to identify and correct deficiencies that may have contributed to or resulted in the issuance of fraudulent driver's license or IDs. This information could also help identify changes necessary to improve the security of the issuance process and to support funding requests. Currently, however, the Department cannot answer basic questions about fraudulently issued Colorado licenses and IDs, including:

- How many fraudulently issued driver's licenses and IDs have been identified and confirmed by the Motor Vehicle Investigations Unit each year since 2001, the year House Bill 01-1125 became law?

- In the case of those fraudulently issued driver's licenses and IDs identified by the Motor Vehicle Investigations Unit, was the failure of the security of the issuance process due to: (1) absence of a specific control, (2) poor design of an existing control, or (3) failure to implement a well-designed control?

- For those fraudulently issued driver's licenses and IDs identified by the Motor Vehicle Investigations Unit, what was the outcome of each investigation (e.g., a finding of insufficient evidence, issuance of a citation, conviction)?

- How many attempts to obtain a fraudulently issued driver's license or ID has each internal control (facial recognition, breeder document inspection, and electronic verification of social security number and immigration documents) stopped?

Answers to these questions are vital for identifying areas where the security features are working effectively and areas where either features should be added or the features' design or implementation needs enhancement. Additionally, information is needed to assure the General Assembly that the Department is continually assessing the effectiveness of taxpayer dollars invested in driver's license and ID security improvements.

We reviewed the Department's data collection systems and found that the Department lacks a tracking mechanism for collecting and analyzing basic statistics on the effectiveness of its controls over the issuance process to prevent fraudulent issuances. For example, the Department does not track information on:

- The number of applicants who presented questionable social security information to examiners and thus, were prevented from obtaining driver's licenses or IDs.

- The number of instances in which the Department's facial recognition software successfully halted the issuance of a fraudulent driver's license or ID.

- The number of times examiners identified fraudulent breeder documents, thus preventing a fraudulent issuance.

We also found that the Department has not developed sufficient procedures and information systems to maximize the information available when a fraudulently issued driver's license or ID is detected. Specifically, the Motor Vehicle Investigations Unit (Unit) tracks the number of fraudulently issued, altered, and counterfeited driver's licenses and IDs that have been identified through its investigations or that have been referred to it by other state, local, and federal law enforcement agencies. However, we found that this information is difficult to retrieve and analyze from the Unit's database. The Unit's database uses an antiquated programming language and lacks the functionality to perform detailed data analysis. In addition, investigators do not enter into the database key data such as the types of breeder documents that are being used to obtain fraudulent licenses and IDs. This information is important because if patterns are identified, the Department can respond in a timely way and alert examiners or implement mitigating controls. Finally, the database does not include the dispositions of the investigations, thus preventing the Department from determining the types of fraud that are most or least prevalent.

Until it can establish a system for tracking and analyzing these basic data, the Department cannot know whether additional controls are needed or whether existing controls should be enhanced. For example, the Department is studying the feasibility of acquiring document scanners that would automatically verify the validity of breeder documents and save images of those documents if questions of fraud arise. The Department estimates the cost of the scanners to be approximately $600,000. If the Department could report data on the strengths and weaknesses of its existing controls and show why enhancements are needed, it would be better positioned to justify its request for additional taxpayer resources for the purchase of scanners.

The Department should work to establish procedures and mechanisms for tracking critical data regarding how effective the driver's license system's controls are at preventing the issuance of fraudulent licenses and IDs. To accomplish this, the Department should develop procedures to quantify the known number of fraudulent driver's license and ID issuances that were prevented by each security feature. This information should be maintained in a centralized database and periodically analyzed to determine whether controls are adequate and operating as expected. Additionally, the Department should work with the Unit to establish a new case-tracking database and to develop written procedures specifying the type and detail of the data to be collected by investigators, including the case disposition, type of fraud (separately tracking counterfeit, altered, and fraudulently issued driver's licenses and IDs), and the deficiency in the issuance process that allowed the fraudulent issuance to occur. The Department should utilize the information it collects to improve internal controls, provide training to staff, and make future budget and strategic planning decisions.

Recommendation No. 5:

The Department of Revenue should establish procedures and mechanisms for tracking the effectiveness of its controls over the process of issuing driver's licenses and IDs by:

a. Tracking and quantifying the number of attempts to obtain a fraudulent driver's license or ID that were stopped by each internal control.

b. Developing a new case tracking database for the Motor Vehicle Investigations Unit and identifying and implementing procedures on the type and detail of data to be collected and summarized.

c. Analyzing the information collected in Parts a. and b. on a regular basis and using the analysis to improve internal controls, target staff training efforts, and support budget and planning decisions.

Department of Revenue Response:

a. Agree. Implementation date: December 2008.

When a driver's license examiner identifies a counterfeit or altered document the case is referred to the Motor Vehicle Investigations Unit. The case is entered and tracked in the Convergent Technologies Operating System (CTOS). The Department performed an analysis of CTOS to determine the extent to which the system can be modified to track the additional information and has made all possible changes to the system at this time. The Department has begun exploring the development of a more detailed and sophisticated Access based tracking program and will implement changes to the extent they are justified based on costs and benefits by December 2008.

b. Agree. Implementation date: Implemented/Ongoing.

Based on the limited design of the antiquated CTOS system, the Department made some modifications in the system to increase the detail and classification of the cases in April 2008. Additionally, the Motor Vehicle Investigations Unit is currently exploring options that include the development of an Access based records management system that would provide even greater detail and more statistics and allow for the input of court/criminal disposition to cases.

c. Agree. Implementation date: December 2008.

Once the additional data are available, the Department will analyze the information collected on a regular basis to determine changes needed to improve internal controls, target staff training efforts, and support budget and planning decisions.

Driver's License Information System

Chapter 2

In carrying out its responsibilities related to issuing, renewing, and reinstating Colorado driver's licenses and IDs, the Department of Revenue (Department) handles and stores large amounts of electronic data. Specifically, the Department maintains data related to driver and motor vehicle records, traffic citations and fines, and associated accounting transactions. The Department also maintains sensitive, personally identifiable information on all persons holding a Colorado driver's license or ID, including their names, dates of birth, addresses, social security numbers, photos, signatures, and fingerprints. As of January 30, 2008, the Driver's License Information System (DLS) contained more than 3.4 million active Colorado driver's license and ID records.

To manage and store these large amounts of data, the Department designed and built the automated DLS in the 1990s. The automated system includes hardware (computer terminals, mainframe computers, and servers), software (individual computer programs, including the licensing application and supporting database), and network communications equipment (phone lines, routers, and switches). DLS is housed on the State's mainframe computer managed by the Division of Information Technologies (DoIT) located within the Department of Personnel & Administration.

A variety of users rely on the information contained in DLS. In addition to Department staff, county staff and employees from a number of state agencies are regular users of the system. State agency users include the Departments of Corrections, Health Care Policy and Financing, Human Services, Public Safety, and Transportation; the Secretary of State's and Attorney General's Offices; and the Judicial Branch. For example, the Colorado Bureau of Investigation, within the Department of Public Safety, periodically receives select data on driver records from DLS. The Departments of Human Services and Health Care Policy and Financing, and a number of state colleges and universities, regularly query DLS to determine whether an applicant for benefits or other services is lawfully present. At the time of our review, a total of more than 3,000 state and county employees had access to DLS.

According to Department staff, the performance of DLS is crucial to the Department's ability to carry out its responsibilities. As a result, strong IT system and security controls are vital to ensuring that the system performs as intended and information is safeguarded. If DLS fails, not only will Colorado residents be unable

to obtain driver's licenses and IDs, but agencies that regularly use the system will be hampered in conducting business. Additionally, if the system were to have a security breach, Colorado residents' personally identifiable information could be exposed to identity thieves.

We reviewed the Department's controls for protecting the data security and physical operations of DLS. We identified significant weaknesses in controls related to system security, disaster recovery planning, and the physical and environmental security of the data center, as described in this chapter.

Information Systems Security

In 2006 the General Assembly enacted House Bill 1157, which provided policy direction for the State with respect to protecting the security of information entrusted to it by its citizens. Specifically, the General Assembly stated that:

> Communication and information resources in the various public agencies of the state are strategic and vital assets belonging to the people of Colorado. Coordinated efforts and a sense of urgency are necessary to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information. [Section 24-37.5-401 (1) (a), C.R.S.]

The Bill also established the position of the State Chief Information Security Officer (CISO) and charged the CISO with developing information security policies, standards, and guidelines that apply to all state agencies. These policies, referred to as the State Cyber Security Policies, became effective in December 2006.

As set forth in the State Cyber Security Policies, agencies must have comprehensive cyber security programs in place to manage and protect all sensitive information—electronic and print—throughout the information's life cycle. A comprehensive cyber security program typically includes (1) a central security management structure to provide overall security guidance and strategic direction; (2) security policies and procedures that are designed to mitigate risk; (3) security awareness and training to inform personnel about information security risks and employees' responsibilities for complying with policies and procedures; (4) periodic assessments of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; and (5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices.

We evaluated the Department's information system controls that were designed to provide security over DLS and to protect the sensitive information it processes and stores. We found the Department lacks a comprehensive security management program as mandated by State Cyber Security Policies. Specifically, we identified instances in which access to sensitive DLS data and programs was not sufficiently restricted, system access was not revoked in a timely manner after users left employment or changed job duties, and data transmissions were not protected from unauthorized disclosure. These control weaknesses are detailed below.

System Access Controls

System access controls provide reasonable assurance that computer resources (data files, software, and computer-related facilities and equipment) are protected against unauthorized modification, use, loss, or impairment. Access controls include physical controls, such as keeping computers in locked rooms, and logical controls, such as using software programs that are designed to prevent or detect unauthorized access to sensitive files. State Cyber Security Policies require state agencies to establish access controls that permit users to gain access to only those IT applications and systems, and to perform only those tasks on the applications and systems, that are absolutely necessary for performing their jobs. Policies also require agencies to modify access privileges when an employee's job duties change and to revoke access privileges when an employee ceases employment.

To access DLS, individuals must have both a user ID and password for the State's mainframe computer and a user ID and password for the DLS application. Users receive access only to specific modules within DLS, depending on their job duties, and are assigned one of four levels of access to each approved module. The lowest access level allows a user to view records. The highest access level allows a user to view, create, modify, or delete records. As of January 2008 approximately 3,000 people had IDs that enabled them to access both the State's mainframe computer and DLS. Of these, 527 individuals also had the ability to issue and renew driver's licenses and IDs through the DLS licensing module.

We reviewed the Department's controls for documenting and monitoring user access to DLS. We found that overall, the Department lacks an effective mechanism for monitoring user access and for modifying or terminating access when employees change job duties or leave employment with the State. During our review, we identified 33 former state employees who still had both active mainframe and application-level IDs for the DLS system as of January 2008. The 33 employees had termination dates that ranged from 13 days to almost 500 days prior to the date of our review. All 33 former employees still had the ability to view and modify driver's licenses and ID information, and four of these former employees also had the ability to issue and renew driver's licenses and IDs.

We also identified 122 former employees who still had active IDs for the DLS application, even though their corresponding mainframe IDs were inactive or had been removed. Although the DLS application cannot be accessed without the corresponding mainframe ID, best practices and State Cyber Security Policies require that such access be revoked because it still represents an internal security risk.

In addition to the problems we identified with access privileges for former employees, we found that current state employees with active DLS user IDs had inappropriate levels of access for their job duties in some instances, and unauthorized levels of access in others. Specifically, of the 527 individuals with access to the DLS licensing module, we identified 14 users, or about 3 percent, whose levels of access appeared appropriate for their job duties, but the access level had not been authorized in writing, as required by Department procedures. We identified another 80 users who had express approval for access at a level that was inappropriate for their job duties. These 80 users had the ability to issue and renew driver's licences and IDs, but their job descriptions did not include these functions.

Transmission Security

State Cyber Security Policies require that when agencies transmit sensitive data, the data must be properly encrypted to prevent interception or corruption. We reviewed the Department's controls over large-batch data transmissions from DLS and found that the Department was transmitting the batches over the Internet and phone lines without encryption. As a result, unscrupulous individuals could use monitoring devices to intercept any personally identifiable information included in the batch transmissions and expose Colorado residents' personal information to identity theft and other criminal activity.

Currently the Department transmits 100 different large data batches from DLS to business partners located within and outside Colorado. These transmissions are not encrypted. Some of these transmissions occur daily; others occur on a weekly or monthly basis. We confirmed that most of these transmissions include personally identifiable data which, according to State Cyber Security Policies, must be encrypted.

In addition to the concerns related to batch transmissions, we identified a security risk related to the State's mainframe that houses DLS. We previously identified this issue during our Fiscal Year 2006 Statewide Single Audit and reported our concerns to the Department of Personnel & Administration under separate cover. The Department of Personnel & Administration has agreed to correct the problem by June 2008. We will be following up on implementation during our Fiscal Year 2008 Statewide Single Audit, which is currently underway.

System Monitoring

As previously discussed, the DLS database contains personally identifiable information on more than 3.4 million Colorado residents. According to reports prepared by the U.S. Department of Homeland Security, personally identifiable information has high market value. This increases the risk that DLS users could be motivated to obtain and sell personally identifiable information maintained in DLS.

State Cyber Security Policies require that all agencies monitor anomalous activities on their information systems and report suspicious activities to the agency's information security officer for investigation. Additionally, agencies are required to maintain records of these monitoring activities for their critical systems and applications for at least one year, in the event that a forensic investigation becomes necessary.

We reviewed the Department's controls to protect the sensitive information contained in the DLS database and found that the Department lacks a process for continuously monitoring DLS database activity. As a result, the Department is unable to identify unusual system activity or violations of the Department's acceptable use and data access policies. For example, the Department cannot detect certain anomalous activity, such as database administrators downloading the DLS database or DLS users attempting to exceed access authority or gain system access at unusual hours.

Improvements

Overall we concluded that the Department's management of information security is fragmented, disorganized, and poorly planned. The Department needs to take steps to correct the control weaknesses we identified by developing a comprehensive cyber security program, including a centralized structure managed by an agency Information Security Officer, as required by State Cyber Security Policies. Currently no single individual is accountable for security over the Department's information systems. Additionally, no centralized group or individual has been assigned responsibility for monitoring the Department's information security controls and investigating identified violations of Department procedures.

The Department also needs to take action, in cooperation with the Governor's Office of Information Technology, to address the specific control weaknesses identified during our audit. This should include developing mechanisms for documenting, monitoring, and updating user access levels for DLS; conducting an inventory of DLS data contained in batch transmissions and encrypting all transmissions of sensitive, personally identifiable information; and carrying out ongoing monitoring

of the activities of information system users to detect anomalous activity and following up on problems identified.

Recommendation No. 6:

The Department of Revenue should develop a comprehensive cyber security program that protects the data contained in crucial information systems, including the Driver's License Information System, against unauthorized access, disclosure, use, modification, or destruction. This should include establishing a centralized information security function managed by an Information Security Officer, as required by State Cyber Security Policies. Additionally, the Department, in cooperation with the Governor's Office of Information Technology, should correct the specific security deficiencies we identified during our audit, including:

a. Developing a mechanism for managing user access to DLS that includes documentation of user access privileges, regular review and monitoring of user access levels to determine whether access is still appropriate, and removal or revision of access privileges for users who cease employment or change job responsibilities.

b. Performing ongoing monitoring of user activities on DLS to identify anomalous activity or violations of Department procedures, and taking appropriate action to resolve the problems identified.

c. Conducting an inventory of DLS data contained in batch transmissions and encrypting all network transmissions of sensitive, personally identifiable information.

Department of Revenue Response:

Agree. Implementation date: December 2008.

The Department is currently reviewing and will update its cyber security policy by July 2008. The Department believes it has adequate information security expertise from various individuals now in place with such knowledge; however, we understand the importance of having one person responsible for this function. The Information Technology Division will evaluate and determine if the Information Security Officer duties will be the responsibility of an existing staff person or hire a person to specifically fulfill these duties by December 2008.

a. Agree. Implementation date: June 2009.

The Department is currently working on addressing the management of the user privileges and will perform an application analysis by June 2009 to determine the extent to which this can be incorporated into the DLS computer application and the related costs. Changes will be implemented to the extent they are justified based on costs and benefits.

b. Agree. Implementation date: June 2009.

Due to the current DLS program structure, there is no systemic tool available to track and analyze data on user activities. The Department will perform an application analysis by June 2009 to determine the extent to which this can be incorporated into the DLS computer application and the related costs. Changes will be implemented to the extent they are justified based on costs and benefits.

c. Agree. Implementation date: June 2009.

The Department will inventory the DLS data contained in the batch transmissions and encrypt the transmissions the Department has control over by June 2009.

Disaster Recovery

Information system disaster recovery refers to the process of identifying, testing, and evaluating all of the resources and procedures needed to make specific information system-based functions operational after services have been disrupted. Disaster recovery planning is essential if government is to continue providing services in the event of natural or man-made disasters or interruptions. In 2006 the Colorado Chief Information Security Officer (CISO) issued a disaster recovery policy that requires every state public agency, as defined in Section 24-37.5-102(5), C.R.S., to develop disaster recovery plans for information technology systems "to reduce the impact of a major disruption on key business functions and processes." According to the policy, agency disaster recovery plans must include the following components:

- **Roles, responsibilities, and contact information** for the individuals responsible for implementing the disaster recovery plan.
- **Recovery time frames** outlining both response and recovery requirements.

- **Recovery procedures** detailing the ways in which services will be restored and operations returned to normal.

- **Plan training,** to be conducted on a regular basis, for the individuals who have specific roles and responsibilities in implementing the disaster recovery plan.

- **Plan testing,** to be conducted on a regular basis, to ensure services can be effectively restored and any problems addressed.

- **Plan maintenance** to ensure the plan is updated or modified to reflect changes in recovery requirements, time frames, personnel, or other factors. The plan should also include procedures for distributing the plan to stakeholders and notifying them of any changes to it.

The Driver's License Information System uses computers, software, and network communications equipment to issue all Colorado driver's licenses and IDs. In Fiscal Year 2007 the system issued approximately 620,000 licenses and IDs. As with all information systems, DLS could be damaged or severely disrupted in the event of a disaster or an emergency, such as a fire or flood, or an act of terrorism or vandalism. Due to the critical nature of the licensing function and the importance of the data maintained in DLS, the objective of the Department of Revenue is to recover DLS within 24 hours after a disaster occurs.

We reviewed the Department's disaster recovery test, testing procedures, and planning documents for DLS and found problems in three areas. First, we found that the Department was unable to fully restore DLS during the 2007 disaster recovery test. From our review of the test results and interviews with Department staff, we learned that the reason the system could not be fully recovered was that key production data had not been identified and backed up in advance, and were thus unavailable during the test. Although the data sets are stored on the State's mainframe computer at the Division of Information Technologies' data center, the backup of these data remains the Department's responsibility.

Second, we found that the Department's procedures for testing the effectiveness of the DLS disaster recovery plan were insufficient. Specifically, the Department's testing procedures did not include such important components as test objectives, success criteria, participants' roles and responsibilities, and detailed test scripts (i.e., the specific functions that each test participant should undertake during the test). Without adequate testing procedures, the Department will not be able to evaluate the completeness and precision of the disaster recovery plan, including the performance of the personnel involved in the exercise, the coordination of the disaster management team, the ability and capacity of the recovery site, and the retrieval of production backups. Additionally, we found that the Department did not include

other DLS users, such as the Department of Human Services or the Colorado Bureau of Investigation, in the 2007 test. Because users from outside the Department depend on DLS to deliver essential state services, it is vital that they too participate in the disaster recovery tests. The Department also did not try to connect with the American Association of Motor Vehicle Administrators (AAMVA) network during the 2007 test. As previously discussed, DLS connects through AAMVA's network to verify an applicant's identity and to check the applicant's driving record before it issues a driver's license. It is important for the Department to test all aspects of DLS to ensure it can resume critical operations if a disaster strikes.

Finally, we found that the Department's disaster recovery plan lacked several key components. Both the State's disaster recovery policy and industry best practices indicate that disaster recovery plans should include procedures for connecting with the system's users. The Department's plan, however, does not include procedures for establishing connectivity with the 52 driver's license offices located throughout the State. It also does not address the photo imaging system, which is managed by a third-party contractor. The photo imaging system stores personally identifiable information on all Colorado drivers and ID holders and is used to perform facial recognition tests and produce the finished Colorado driver's licenses and IDs. According to the Department's contract, the company that owns the photo imaging system is required to develop and provide the Department with a disaster recovery plan for this system. We requested this plan from Department staff, but they could not provide it. Additionally, the Department did not include recovery of the photo imaging system during its 2007 disaster recovery test.

A comprehensive and well-tested disaster recovery plan is needed for the Department to be able to successfully resume the issuance of driver's licenses and IDs following a disaster or system disruption. It is also needed for other agencies that rely on DLS for their operations after such a disruption. The Department of Revenue is responsible for DLS and its recovery in the event of a disaster. Additionally, the Department has a responsibility to comply with the CISO disaster recovery policy. Therefore, the Department should ensure that its disaster recovery plan for DLS includes all required components and supporting information systems. This will require the Department to identify all data files necessary for the proper operation of DLS. Once the files are identified, Department staff will need to ensure that the key data files are backed up and stored offsite according to both the Department's data-retention requirements and the State Cyber Security Policies. Also, before it conducts the next disaster recovery test, the Department should develop sufficiently detailed, written procedures articulating exactly how it will adequately test the effectiveness of the plan. At a minimum, the testing plan should include test objectives, success criteria, test participants' roles and responsibilities, and detailed test scripts. Finally, the Department should include other DLS users in the testing procedures, and should, during each disaster recovery test, attempt to establish connections with critical networks and databases that support the issuance process.

Recommendation No. 7:

The Department of Revenue should improve its disaster recovery planning and preparedness for the Driver's License Information System by:

a. Identifying all critical data sets necessary to fully recover DLS and working to ensure the data sets are backed up and stored offsite according to Department data-retention needs and State Cyber Security Policies.

b. Prior to the next disaster recovery test, developing sufficiently detailed, written procedures for testing the DLS disaster recovery plan and assessing its effectiveness.

c. Ensuring that disaster recovery tests include other DLS users and the Department's photo imaging system contractor in the testing procedures. In addition, the Department should obtain the contractor's disaster recovery plan and review it to determine if it is sufficient.

d. Ensuring that the disaster recovery plan includes all components required by the State's disaster recovery policy and that it tests connections to all critical networks.

Department of Revenue Response:

a. Agree. Implementation date: June 2009.

   The Department will identify all critical data sets necessary to fully recover the DLS and ensure the data sets controlled by the Department are backed up and stored offsite in accordance with Department data retention policies and State Cyber Security Policies by June 2009.

b. Agree. Implementation date: December 2008.

   The Department will develop sufficient written test procedures by December 2008 for assessing the effectiveness of the DLS disaster recovery plan.

c. Agree. Implementation date: December 2008.

   The Department will include other DLS users and the Department's photo imaging system contractor in the testing procedures and in the next disaster recovery test. Additionally, the Department will work with

the photo imaging system contractor to obtain its disaster recovery plan and review it to determine if the plan is sufficient by December 2008.

d. Agree. Implementation date: December 2008.

The Department will review and update its disaster recovery plan by December 2008 to include all components required by the State's disaster recovery policy and test connections to critical networks prior to the next disaster recovery test.

Data Center

A data center is a facility used to house computing systems and associated components, such as telecommunications and storage systems. It typically includes redundant or backup power supplies, redundant data communication connections, and environmental controls such as air conditioning and fire suppression systems. The Driver's License Information System's critical computing components are hosted on the State mainframe computer located at the Division of Information Technologies' data center and on a computer server housed within one of the two data centers belonging to the Department of Revenue. The Department's data center housing DLS also contains computer equipment supporting online tax filing and processing.

The State Cyber Security Policies require that state agencies implement a system of physical and environmental controls at data centers to prevent unauthorized access to taxpayer information and to ensure the availability of key data and systems. The State Cyber Security Policies specifically require agencies to restrict physical access to computing equipment, infrastructure network devices, and data centers to authorized personnel only. Physical access to data centers must also be recorded and access records maintained for at least one year. Additionally, physical access records are to be reviewed on a regular basis for the purpose of detecting unusual activity. The State Cyber Security Policies also include requirements for protecting data centers from fire, including the use of smoke detection and fire suppression systems.

We assessed the effectiveness of the controls the Department has implemented to safeguard its data center from physical and environmental threats. Because we previously reviewed these controls at the DoIT data center (see *Division of Information Technologies Data Center and Technology Management Unit, June 30, 2007, Department of Personnel & Administration*), we limited this review to the Department of Revenue's data center. Overall, we found that the data center is neither adequately secured from inappropriate access nor properly protected from environmental hazards.

Physical Access

We found that the Department does not periodically review those individuals with access to the data center to determine whether they have a current, valid need for such access. Currently only two Department employees have computer operator responsibilities that require routine, day-to-day access to the data center. However, we found that, in direct conflict with State Cyber Security Policies, almost 70 people have unrestricted access to the data center. Although the Department electronically logs entry into the center by these individuals when they use their identity badges, no one within the Department reviews the access logs to identify unusual activity. We reviewed the electronic access logs for one week in February 2008 and found that one contractor entered the data center at 3:40 a.m. Although the contractor had authorization to access the center, the time of the access was unusual. Department management was unaware of the incident and could not explain why the contractor entered the data center at that hour.

Environmental Controls

We found that the data center's fire suppression system does not comply with State Cyber Security Policies or meet industry best practices. The Department's data center relies on a water-based fire suppression system. Using water on computing equipment can cause electrical shock. As required by policy, the Department should consider installing a Class C fire suppression system, such as an inert gas-based system, which is designed to extinguish electrical fires without threat of electrical shock. The Department is aware of the problem with its current fire suppression system and has, for several years, requested funding to replace it. The Department's requests have been unsuccessful.

Finally, we found that the Department has not developed procedures for handling emergencies at the data center. For example, procedures for handling smoke, fire, water leakage, flood, or power outage were neither documented nor posted. The absence of emergency procedures poses a potential risk to the safety of individuals working within the data center as well as to the equipment and data housed there.

Recommendation No. 8:

The Department of Revenue should improve the physical-access controls and environmental controls over the data center by:

a. Restricting access to only those individuals who have an established and valid need to routinely access the data center.

b. Assigning a staff person to routinely review data center access records and follow up on unusual activity.

c. Developing policies and procedures related to data center access and emergency procedures and training Department staff on these procedures.

d. Augmenting the current sprinkler system with an inert gas-based fire suppression system, once funding becomes available.

Department of Revenue Response:

a. Agree. Implementation date: May 2008.

The Department reviewed the existing list of individuals with access to the data center in May 2008 and determined the majority of the individuals do require access to the data center for valid reasons. The Department will monitor requests for obtaining access to the data center and will restrict access to only those individuals who have an established and valid need to routinely access the data center.

b. Agree. Implementation date: December 2008.

The Department will develop a process to routinely review data center access records and follow up on unusual activity by December 2008.

c. Agree. Implementation date: December 2008.

The Department will develop policies and procedures related to data center access and emergency procedures and train Department staff on these procedures by December 2008.

d. Agree. Implementation date: December 2008.

The Department received approval and funding for a FM2500 gas fire suppression system and the installation project is in progress. The Department is currently designing the system with building services and anticipates completion of the installation by the end of 2008.

This page intentionally left blank.

Appendices

This page intentionally left blank.

DR 2300 (03/12/08)
COLORADO DEPARTMENT OF REVENUE

IDENTIFICATION REQUIREMENTS

To be issued a Colorado Driver's License or Identification Card, you must prove the following elements: your full legal name, identity, age, and lawful presence in the United States. The chart below shows the documents that you may use to prove each of these elements. In some cases, a single document may prove all four elements. However, it may be necessary for some applicants to provide multiple documents in order to prove all the required elements. All documents presented must be certified originals or certified amended originals or true copies certified by the issuing agency.

If you can not prove each of the required elements with the documents set forth in the chart below, then you may request to go through "Exceptions Processing" in order to prove the required elements with additional/alternative documents.

Document	Elements			
Stand Alone Documents	**Identity**	**Age**	**Name[1]**	**Lawful Presence**
CO license (expired less than 1yr)	X	X	X	X
CO ID card (expired less than 1yr)	X	X	X	X[2]
US passport (expired less than 10 yrs)	X	X	X[3]	X
Out of State DL/ID from LP[3,4] state (expired less than 1 yr)	X	X	X[3]	X
Foreign passport w/ photo, US Visa, I-94[9]	X	X	X	X
Valid Military ID/Common Access Card[3]	X	X	X	X
Cert. of Naturalization w/ photo less than 20 yrs old[6]	X	X	X	X
Cert. of Citizenship w/ photo less than 20 yrs old[6]	X	X	X	X
Valid I-551	X	X	X	X
Valid EAD/Temporary Resident	X	X	X	X
Refugee/Asylee I-94 w/ photo less than 20 yrs old[6]	X	X	X	X
OR				
You must provide any combination of documents that prove identity, age, name, and lawful presence in the United States				
Lawful presence documents	**Identity**	**Age**	**Name[1]**	**Lawful Presence**
Social Security card verified by SSOLV				X
U.S. Birth certificate		X		X
Cert. of Citizenship from the Department of Interior		X[7]		X
U.S. Adoption Order w/ birth information		X		X
Asylee/refugee I-94, no photo		X		X
Name, Age, and Identity documents				
CO license (expired less than 10 yrs)	X	X	X	
CO ID card (expired less than 10 yrs)	X	X	X	
Out of State DL/ID (NLP[5],expired less than 10 yrs)	X	X	X[3]	
BIA ID Card w/ photo less than 20 yrs old	X	X	X	
Military ID/CAC (expired less than 10 yrs)	X	X	X	
VA Card w/ photo less than 20 yrs old	X	X	X	
Parent/Guardian affidavit if under 21[8]	X	X	X	
US school record less than 12 months old		X		

See reverse side for footnotes disclaimer.

Source:Colorado Department of Revenue.

[1] The applicant's full legal name is the name on the applicant's birth certificate, unless it has been changed by court order, marriage, divorce, or adoption. A marriage certificate, divorce decree, separation decree, or name change order issued by a state or federal court or government may be used to prove a name change.

[2] Applicants presenting a Colorado ID card with an issue date of 06/01/97 up to 07/01/98 must also present a document establishing lawful presence.

[3] Applicants who present U.S. passports, out of state driver's licenses and ID cards or Military IDs/Common Access Cards that do not contain the applicant's full name will be required to present an additional document (other than the US school record) that prove the applicant's full legal name.

[4] **LP =** lawful presence state, which are currently Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, West Virginia, Wyoming

[5] **NLP =** non-lawful presence state.

[6] Certificates of Naturalization or Citizenship, with photos over 20 years old, require an additional identity document.

[7] Only if the Certificates of Citizenship from the Department of Interior shows the applicant's date of birth.

[8] A parent/guardian providing an affidavit for a minor under 21 must also present identification and proof that they are the parent or legal guardian of the minor.

[9] Customers presenting a valid foreign passport with US visa and I-94 or valid Processed For I-551 stamp may be required to present documentation establishing a Colorado connection. Status F, J, H, and M, require verification of a Colorado connection through the sponsoring entity and original letter, by the Colorado employer, of Colorado employment or verification of education through the valid DS-2019 or I-20AB. Applicants with a B1, B2, WT, WB, CP, or NC status are not eligible for a Colorado Driver's License or ID Card.

This document is created solely to assist applicants in understanding the identification rules for obtaining a Colorado Driver's License or Identification Card. This document does not supersede, alter, or amend the rules promulgated by the Department of Revenue; those rules contain the complete requirements and are available on the Department's website at http://www.revenue.state.co.us/mv_dir/home.asp.

Per 1 CCR 204-13, 2.3.3.2, birth certificates must be issued by the United States, including any agency or department thereof, the District of Columbia, any state, county parish, or borough, and which has been certified by the issuing agency.

Appendix B

Colorado Department of Revenue Adult Driver's Licenses and IDs Issued by Colorado Driver's License Offices[1] Fiscal Year 2007				
	Driver's License Office (County)[2]	**State or County Run**	**Licenses Issued (FY 2007)[3]**	**IDs Issued (FY 2007)**
1	**Akron (Washington)**	**County**	**550**	**80**
2	Alamosa (Alamosa)	State	4,180	1,570
3	**Athmar (City and County of Denver)**	**State**	**39,600**	**17,810**
4	**Aurora (Arapahoe)**	**State**	**32,180**	**15,210**
5	**Boulder (Boulder)**	**State**	**26,680**	**3,980**
6	Broomfield (City and County of Broomfield)	State	23,600	5,130
7	Burlington (Kit Carson)	County	660	130
8	Canon City (Fremont)	State	5,100	1,030
9	Cascade (El Paso)	County	9,470	1,690
10	Centennial (Arapahoe)	County	2,550	300
11	Chapel Hills (El Paso)	County	16,280	640
12	Cheyenne Wells (Cheyenne)	County	180	20
13	**Colorado Springs (El Paso)**	**State**	**21,880**	**9,670**
14	Cortez (Montezuma)	State	2,850	710
15	Craig (Moffat)	State	1,440	290
16	**Delta (Delta)**	**State**	**3,070**	**600**
17	Durango (La Plata)	State	7,510	1,220
18	Eads (Kiowa)	County	90	20
19	Fort Collins (Larimer)	State	28,620	5,350
20	Fort Morgan (Morgan)	State	2,760	970
21	Frisco (Summit)	State	7,640	1,110
22	Fruita (Mesa)	County	1,250	70
23	**Glenwood Springs (Garfield)**	**State**	**9,890**	**2,120**
24	**Grand Junction (Mesa)**	**State**	**14,600**	**3,810**
25	Greeley (Weld)	State	15,220	5,820
26	Gunnison (Gunnison)	State	1,830	270
27	Holyoke (Phillips)	County	340	50
28	Hot Sulphur Springs (Grand)	State	1,640	190
29	Hugo (Lincoln)	County	820	130
30	**Julesburg (Sedgwick)**	**County**	**270**	**50**
31	**La Junta (Otero)**	**State**	**2,290**	**800**
32	Lakewood (Jefferson)	State	38,170	13,260
33	Lamar (Prowers)	State	1,070	270
34	Leadville (Lake)	County	680	210
35	Littleton (Arapahoe)	State	28,450	4,190

	Driver's License Office (County)[2]	State or County Run	Licenses Issued (FY 2007)[3]	IDs Issued (FY 2007)
36	Littleton (Arapahoe)	County	13,690	2,290
37	Longmont (Boulder)	State	15,490	4,760
38	Meeker (Rio Blanco)	State	310	40
39	Montrose (Montrose)	State	5,380	1,230
40	**Northglenn (Adams)**	**State**	**25,140**	**10,400**
41	Nucla (Montrose)	State	10	0
42	Pagosa Springs (Archuleta)	State	60	0
43	Parker (Douglas)	State	31,300	5,550
44	Powers (El Paso)	County	14,200	1,720
45	**Pueblo (Pueblo)**	**State**	**16,560**	**8,040**
46	Rangely (Rio Blanco)	State	190	30
47	Saguache (Saguache)	County	190	30
48	Salida (Chaffee)	State	2,180	250
49	Springfield (Baca)	County	440	80
50	Steamboat Springs (Routt)	State	2,900	470
51	Sterling (Logan)	State	1,910	530
52	**Trinidad (Las Animas)**	**State**	**1,770**	**470**
53	Walsenburg (Huerfano)	State	520	140
54	Wray (Yuma)	County	460	110
55	Yuma (Yuma)	County	350	100
	Total in Sample[1]		**194,480**	**73,040**
	Driver's Licenses and IDs issued by all offices		**486,460**	**135,010**
	Sample as percentage of total licenses/IDs issued		**40%**	**54%**

Source: Office of the State Auditor analysis of information from the Department of Revenue.

[1] The 13 Driver's License Offices visited by Office of the State Auditor staff are listed in bold. The total in sample are the driver's licenses and IDs issued in Fiscal Year 2007 by the 13 driver's license offices we visited. We did not test each of these issuances during our audit work.

[2] There were 55 offices open for at least part of the year during Fiscal Year 2007. However, the Fruita, Nucla, and Pagosa Springs offices closed, and as of May 2008, only 52 offices remained open.

[3] Licenses issued include only licenses issued to adults and does not include Commercial Driver's Licenses, Motorcycle, Minor, Provisional, Duplicate, or Reinstated Licenses.

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 1912