Secretary of State Audit Report

Kate Brown, Secretary of State

Gary Blackmer, Director, Audits Division

# Drivers System Data was Secure but Controls Could be Improved

## Summary

The mission of the Oregon Department of Transportation (department) is to provide Oregonians with a safe, efficient transportation system that supports economic opportunity and livable communities. One of the department's major divisions is the Driver and Motor Vehicle Services Division (DMV). DMV's mission is to promote driver safety, protect financial and ownership interest in vehicles and collect revenue for Oregon's roads.

In 2007, the Oregon State Legislature passed Senate Bill 583, known as the Oregon Consumer Identity Theft Protection Act, to protect personally identifiable information contained in both private and public information systems. One of the major information systems involved in collecting and maintaining personally identifiable information at DMV is the Drivers System (system).

The purpose of this audit was to evaluate the effectiveness of key computer controls governing the system. Specifically, we evaluated controls governing input, processing and output; programming changes; backup and recovery; and security.

We found that:

- System controls provided reasonable assurance that system data remained complete, accurate and valid during input, processing and output.
- System computer code modifications followed appropriate system development processes and change management procedures, but weaknesses existed in securing program source code.
- It is uncertain whether the system and its data could be fully recovered in a timely manner after a major disruption.
- DMV provided adequate controls to protect the system, but State Data Center security weaknesses increased the risk the system could be compromised.

## Recommendations

To resolve these issues, we recommend department management improve program change management processes, improve its disaster recovery strategies, and better define and manage its security requirements with the State Data Center. Our detailed audit recommendations follow in the Audit Results section below.

## Agency response

The agency response is attached at the end of the report.

## Background

The mission of the Oregon Department of Transportation (department) is to provide Oregonians with a safe, efficient transportation system that supports economic opportunity and livable communities. One of the department's major divisions is the Driver and Motor Vehicle Services Division (DMV). DMV's mission is to promote driver safety, protect financial and ownership interest in vehicles and collect revenue for Oregon's roads. DMV licenses drivers, registers motor vehicles, and administers motor vehicle laws. There are 64 DMV offices statewide serving more than 13,000 walk-in customers each day. In addition, DMV personnel process more than 10 million transactions and respond to over 1.8 million phone inquiries each year. Law enforcement agencies access DMV computer information files more than 41,000 times each day, and businesses and individuals make about 4 million DMV record requests each year.

DMV uses several computer systems to support its mission. One of these is the Drivers System (system), which stores and manages information such as a driver's name, Oregon driver license number, and license status. This system runs on a mainframe computer at the State Data Center, which is operated by the Department of Administrative Services.

In 2007, the Oregon State Legislature passed Senate Bill 583, known as the Oregon Consumer Identity Theft Protection Act, to protect personally identifiable information contained in both private and public information systems. According to this legislation, personally identifiable information includes a person's name in combination with his or her Oregon driver license or Social Security number. The requirements in this legislation directly affect DMV because it collects and retains personally identifiable information, such as Social Security numbers, as part of the process to issue driver licenses and identification cards.

The purpose of this audit was to evaluate the effectiveness of key computer controls governing the Drivers System. Specifically, we evaluated controls governing data input, processing and output; programming changes; backup and recovery; and security.

# Audit Results

## Management Ensured System Data was Reliable

The first objective of our audit was to determine whether DMV had implemented controls to ensure Oregon driver license information remained complete, accurate and valid during input, processing and output. This is particularly important because driver licenses are widely accepted as proof of identity.

Good controls consist of both manual and automated processes. They include data validity checks, error detection and correction processes, transaction balancing routines, transaction authorization and separation of critical duties.

We found that the system included controls designed to ensure that system data remained reliable. These controls included manual reviews of critical data input, data error detection and correction processes, policies and procedures for controlling distribution of sensitive data, and various automated and manual routines to ensure statutory requirements were satisfied.

We tested these controls to determine whether they were working as intended and concluded that DMV provided reasonable assurance that system data was complete, accurate and valid. Specifically, we found:

- verification procedures for system input were performed as directed, and were effective;
- staff adhered to established policies and procedures relating to data confidentiality;
- during our testing period, controls ensured licensees met selected requirements, such as having a valid Social Security number;
- selected fields in system database tables contained valid data;
- errors identified during data validation procedures were corrected in a timely manner; and
- selected automated input routines prevented entry of invalid data.

## Change Management Processes Were Sufficient, but Weaknesses Existed in Securing Program Source Code

Our second audit objective was to determine whether computer code modifications follow appropriate system development processes and change management procedures. These processes and procedures should ensure that only approved program modifications are implemented.

We reviewed department processes, policies and procedures relating to program change management and concluded that department staff applied reasonable controls to manage changes to program code. However, we identified some improvements to better ensure only approved changes are made to the system.

Department controls included formal procedures for ensuring changes were authorized, documented, tested and approved. In addition, department management relied on software to track movements and status of source code modules. When established controls were followed, this software alerted managers when program changes occurred so that they could investigate any unauthorized instances. However, programmers could circumvent these controls and make unauthorized changes to source code that could affect the integrity of the system.

We identified similar issues relating to controlling access to program source code during our audits of other state agency computer systems. We concluded that this weakness is widespread at state agencies and could be resolved with program change control software or other controls. Robust program change management software is commercially available that could resolve this weakness.

After we completed our fieldwork, department managers indicated they were considering procuring comprehensive change management software to provide more robust version control of system source code modules.

**We recommend** department management implement comprehensive change management controls that protect source code and track its movements throughout the system. This may be accomplished by modifying existing systems and processes or procuring a commercially available solution.

## Disaster Recovery Strategies Need Attention

Our third audit objective was to determine whether the system could be restored in a timely manner after a major disruption. Organizations should ensure usable backups are regularly performed in accordance with a defined back-up strategy. This strategy should ensure all critical files are copied as frequently as needed to meet business requirements and are securely stored at both on-site and off-site locations. In addition, disaster recovery procedures should be well-documented to facilitate proper and timely system reconstruction in the event of a major disruption. These procedures should also be tested periodically to ensure that they will function as planned.

We reviewed the department's backup and recovery procedures and found that staff ensured regular backups of system and data files were created at the State Data Center. Department managers indicated they were relying on the State Data Center to create backup tapes designated for off-site storage, to store the tapes securely, and to recover the system from the tapes in a disaster recovery scenario. However, neither the department nor the State Data Center had developed detailed procedures that defined how the system would be recovered, and neither party had conducted tests to determine whether full recovery could occur. As a result, the department did not have sufficient assurance that the system could be recovered in the event of a disaster.

These weaknesses existed in part because the department had not assigned responsibility for ensuring that disaster recovery capabilities were available.

**We recommend** that department management assign responsibility to ensure that disaster recovery strategies include detailed procedures for recovering the system, and that recovery capabilities are tested.

## The Department Provided Adequate Security for the System, but State Data Center Weaknesses Posed Risks

Our final audit objective was to determine whether system information was protected against unauthorized use, disclosure, modification, damage or loss. To achieve this objective, we evaluated the controls DMV used to secure the system, and considered security measures provided for systems hosted at the State Data Center.

The integrity of computer systems and other information assets is preserved by controls that protect the environment in which systems operate, as well as controls that protect individual systems. In addition, when an organization relies on an external service provider to host its computer systems, it should formally define each party's responsibilities and specific expectations regarding security. It should also obtain assurance that critical security requirements are fulfilled.

We concluded that the department took adequate measures to protect the Drivers System against unauthorized use, disclosure, modification, damage or loss. Specifically, the department provided security for the system by:

- demonstrating strong commitment and support for the security function;
- implementing adequate security policies and procedures;
- assigning an individual to lead DMV's Information Security Program and ensure its compliance with the Oregon Consumer Identity Theft Protection Act;
- ensuring user accounts were appropriately closed when no longer needed;
- ensuring secure data transmissions between DMV users and the State Data Center; and
- periodically confirming compliance with policies and procedures governing required confidential record disclosures.

A separate audit of controls at the State Data Center that we conducted concurrently with this audit identified security weaknesses that increased the risk that DMV's system could be compromised. Although the security weaknesses at the State Data Center were not the direct responsibility of the department, we found that the department had not adequately defined its security requirements with the State Data Center or confirmed its security expectations were met.

**We recommend** that the department better define its security requirements with the State Data Center and establish a mechanism for ensuring those expectations are fulfilled.

## Objectives, Scope and Methodology

The objectives of this audit were to determine whether the Oregon Department of Transportation, Driver and Motor Vehicle Services Division had implemented information system controls to provide reasonable assurance that the Drivers System:

- information remained complete, accurate and valid during input, processing and output;
- computer code modifications followed appropriate system development processes and change management procedures;
- could be restored in a timely manner in the event of a major disruption; and
- information was protected against unauthorized use, disclosure, modification, damage or loss.

Our review covered both the Drivers System and portions of associated systems that could be used to create or modify information stored on the two database tables primarily associated with the Drivers System. This included portions of the Driver's Registration Issuance Verification System and the Customer Information System.

We conducted interviews with appropriate DMV and other department personnel and observed department operations and processes. In addition, we examined technical documentation relating to the Drivers System and its architecture.

To evaluate system controls we reviewed whether:

- verification procedures for Drivers System input were being performed as stated;
- errors noted during verification procedures for certain types of transactions were corrected; and
- input controls in the Driver's Registration Issuance Verification system prevented entry of invalid data.

We also evaluated data elements from selected database tables to determine whether conditions were met based on logical relationships or legal requirements, including:

- whether individuals who were issued licenses from June 2008 through June 2009 met certain criteria, such as having verified Social Security numbers and meeting age restrictions; and
- validity of data in selected database fields, including those with key dates and status codes.

To test program change management controls, we evaluated the department's change management policies and procedures, reviewed logical access to file locations, and performed a limited review of supporting documentation for selected changes.

We tested backup and restoration controls by reviewing backup procedures and logs of backups performed and by observing demonstrations of virtual tape identification.

To determine whether the system and its data were reasonably secure, we:

- reviewed department security policies and procedures;
- tested whether access was provided in accordance with department policies and best practices; and
- verified that data transmissions were encrypted between DMV and the State Data Center.

We used the IT Governance Institute's (ITGI) publication, "Control Objectives for Information and Related Technology," (CobiT) and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 27002:2005 to identify generally accepted and applicable internal control objectives and practices for information systems.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Oregon
Theodore R. Kulongoski, Governor

**Department of Transportation**
Office of the Director
Room 135
355 Capitol St NE
Salem, OR 97301

March 9, 2010

Gary Blackmer, Director
Oregon Secretary of State, Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310

Dear Mr. Blackmer:

Thank you for the opportunity to review the Driver and Motor Vehicle Services Division (DMV) computer controls audit report. The Oregon Department of Transportation (ODOT) agrees with the report contents and recommendations.

We appreciate that the audit recognized ODOT for efforts in using computer controls to meet business needs. At this time, ODOT is committed to resolving all of the findings identified in the report and is working on all three recommendations.

***Audit Recommendation:***

*We recommend department management implement comprehensive change management controls that protect source code and track its movements throughout the system. This may be accomplished by modifying existing systems and processes or procuring a commercially available solution.*

**Response:**

The DMV/Information Systems group is implementing a two-pronged strategy to better manage and control programming source code through the full migration lifecycle. The first initiative is nearly complete with implementation of comprehensive manual change management processes that clarify roles and responsibilities and formalize workflows and migration reviews. The second initiative will procure a best of breed software configuration management tool. The ODOT Procurement Office is reviewing the statement of work for a Request for Proposal that will be issued later this spring.

***Audit recommendation:***

*We recommend that department management assign responsibility to ensure that disaster recovery strategies include detailed procedures for recovering the system, and that recovery capabilities are tested.*

**Response:**

Two DMV/IS employees are assigned to support the Disaster Recovery planning activities within the department and the State Data Center (SDC). The department will ensure that future Disaster Recovery exercises include DMV applications with detailed recovery procedures and testing of recovery capabilities at designated SDC sites. The existing Service Level Agreement with the SDC will be updated with more detailed needs and expectations specific to disaster recovery of DMV records. The department will continue to demand better support from the SDC in the area of Disaster Recovery services and participate in the SDC-sponsored activities that promote and protect the department's business interests.

***Audit Recommendation:***

*We recommend that the department better define its security requirements with the State Data Center and establish a mechanism for ensuring those expectations are fulfilled.*

**Response:**

DMV/IS has an active project to improve on its internal and external security measures. To assure that proper security requirements at the SDC are clarified for ODOT and DMV/IS (as a division of ODOT), DMV/IS will assign a resource to work with the ODOT Information Systems Branch team addressing security concerns at the SDC in the next revision of the Service Level Agreement between ODOT and the SDC. To further assure our expectations are met we will request that the ODOT ISB Security officer have audit capabilities that allow the department to determine when someone accesses DMV data. In addition we will strive to get automated audits of access to DMV data and application at the SDC run on a regular basis (quarterly).

Sincerely,

Matthew L. Garrett
Director

## About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of the Executive, Legislative, and Judicial branches of Oregon government. The division audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

| Audit Team |
| --- |
| William K. Garber, CGFM, MPA, Deputy Director |
| Neal E. Weatherspoon, CPA, CISA, CISSP, Audit Manager |
| Erika A. Ungern, CISA, Principal Auditor |
| Glen D. Morrison, MBA, Staff Auditor |
| Teresa L. Furnish, Staff Auditor |

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained from:


internet: http://www.sos.state.or.us/audits/index.html

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310



The courtesies and cooperation extended by officials and employees of the Oregon Department of Transportation during the course of this audit were commendable and sincerely appreciated.