STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Arizona Department of Transportation
Motor Vehicle Division
Information Security and E-government Services

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Subject

The Motor Vehicle Division's (MVD) two major computer systems contain sensitive customer information, including names and social security numbers that MVD's employees, third parties, and other government users need to perform their jobs. This audit discusses information security for these two systems, and the status of ServiceArizona, MVD's e-government program.

Our Conclusion

ADOT should improve information security controls related to user access, computer program changes, policies and procedures, and disaster recovery. Due to ServiceArizona's growth and significance, MVD should require IBM Corporation, which hosts ServiceArizona, to have an information security control assurance review.

2004

September • Report No. 04-10

ADOT Should Strengthen MVD's Information System Security

Thousands of people have access to MVD's title, registration, and driver's licensing data as part of their jobs. Some work for MVD or provide MVD services, such as third-party processors. Many others work for other state, county, and local agencies, including law enforcement agencies, who can access MVD data as part of normal operations in accordance with state and federal statutes. For example, the Department of Economic Security's Child Support Enforcement employees can access MVD data to locate parents. These users account for more than 8 million transactions or queries on the systems each week.

Because so many people can access MVD's two major information systems as part of their jobs, ensuring system security is of the utmost importance.

Weaknesses in data security

Although ADOT and MVD have taken steps to assess security risks, auditors found deficiencies in four security control areas:

- Access controls—Limit users' access to only the data and functions they need.
- Computer program change controls—Permit only authorized changes to programs and ensure that the changes work.
- General policies—Ensure security for the whole system.
- Disaster recovery—Ensures that critical services can continue if hardware or software fails or is destroyed.

Access to systems not adequately controlled—We found a variety of weaknesses in access controls. For example:

- ADOT and MVD have placed some employees in the wrong user groups. A sample of 30 customer service representatives (CSRs) found an enforcement officer incorrectly placed in the CSR user group. This gave him the ability to change records when he should be able to review information only.
- Some user account groups' access levels have not been reviewed for appropriateness.
- CSRs had access to a transaction that should be reserved for technical support.
- MVD's list of non-MVD employees who can access its systems is out of date. Thirteen former employees of two other agencies still had access rights, and MVD also had an outdated list of third-party user accounts.

During the course of our audit, ADOT's IT Group and MVD reported that they had made or were making some changes. For example, ADOT has eliminated the CSRs' ability to perform inappropriate transactions, and MVD is taking steps to maintain an accurate list of third-party processors.

Computer program changes not adequately controlled—The process for changing a computer program should be to:

- Request the change.
- Design the change.

- Test the change.
- Give final approval if it passes tests.
- Implement the change.

Auditors reviewed 30 program changes between March 2003 and March 2004. MVD's programmers could not adequately document 83 percent (25 of 30) of the changes. Several changes did not have any documentation. When documentation was available, it showed that changes were often implemented before they were tested and approved.

General policies and procedures are inadequate—ADOT and MVD lack or do not enforce general policies, ranging from a general comprehensive security program to training. However, some progress is being made. ADOT has hired a security analyst to develop policies and procedures, and should have a priority list developed by the end of 2004. Also, ADOT is developing a Web-based computer security training program that MVD employees will be able to take to increase security awareness.

ADOT's disaster recovery plan not completed—Implementation of a disaster recovery plan has three steps:

- Assessment of the system failure's impact on critical business processes.
- Recovery strategy.
- Implementation.

The Department of Administration, which houses MVD's data in the State Data Center, has a disaster recovery plan to recover MVD data. However, ADOT needs to complete its own disaster recovery plan, since it is responsible for bringing all its computers and network equipment back up at ADOT administrative and field offices in the event of a service disruption. ADOT reports that it should have a plan implemented by February 2007.

Turnover has contributed to inaction

ADOT has had four different chief information officers (CIOs) since June 2000. The current CIO has been in his position since February 2003. In addition, there have been vacancies in the data security group. As of March 2004, two of ADOT's five data security positions were vacant.

Recommendations

ADOT should:

- Evaluate and appropriately define and limit the access of all user accounts.
- Develop policies and procedures for a comprehensive security program.
- Implement a disaster recovery plan.
- Better ensure that user accounts are removed when an employee leaves or no longer needs access.
- Periodically review its list of third-party processors.
- Better control the implementation of program changes.

Oversight of ServiceArizona More Important with Its Growth

MVD provides 26 services over the Internet, including vehicle registration renewals, driver's license address changes, and voter registration. This e-government program is called ServiceArizona, and MVD and IBM Corporation (IBM) jointly operate it under MVD's direction. ServiceArizona consists of a Web site, an interactive voice recognition system, and walk-up kiosks at several field offices.

MVD is a national leader in providing motor vehicle-related services over the Internet. Further, ServiceArizona is very popular with its users. According to MVD reports, for fiscal years 2001 through 2004, customer satisfaction ratings exceeded 99 percent.

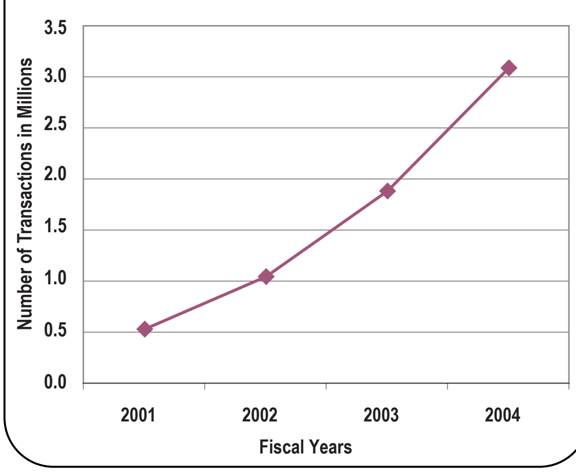
ServiceArizona

- Created, financed, and jointly operated by both MVD and IBM.
- IBM receives fees as allowed and defined in statute.
- IBM receives revenues for 18 of the 26 types of transactions it provides.
- In fiscal year 2004, IBM processed more than 3 million transactions.
- In fiscal year 2004, IBM received $6.3 million for its services.

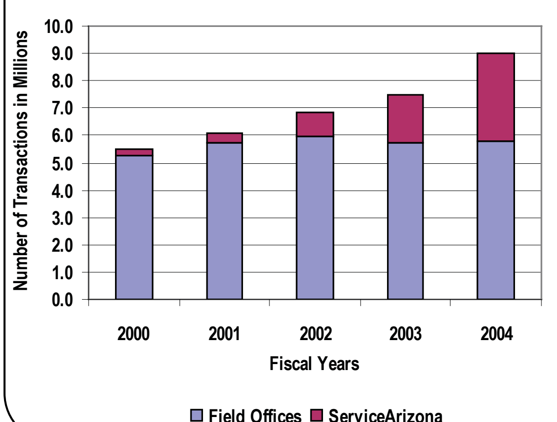
ServiceArizona is growing—Given its number of services and popularity with users, ServiceArizona has grown significantly since 1997, its first year of operation. In fiscal year 2004, it handled more than 3 million transactions.

ServiceArizona's growth has helped MVD absorb the increase in its workload caused by the State's population growth. As shown in the chart, although the total number of transactions has increased between field offices and ServiceArizona, field office transactions have largely leveled off while ServiceArizona transactions have increased.

ServiceArizona Transactions



Field Offices vs. ServiceArizona Transactions



Effective monitoring is critical. ServiceArizona's continued growth increases the importance of MVD's monitoring of the program. IBM must comply with MVD security directives, laws, and rules. We found that:

- MVD appears to follow policies and procedures it has established to monitor the revenues that ServiceArizona collects and remits to MVD.

- IBM reports that it provides numerous controls and security methods to protect the privacy and security of customers' personal information. For example, IBM protects confidential records by encrypting them while transmitting between its system and MVD's system.

MVD should require an assurance review to improve oversight—Although policies and procedures are in place, MVD's current agreement with IBM does not require that IBM obtain an independent assurance review. Assurance reviews provide a way for organizations to help ensure that controls are in place to help protect their data. An independent auditor would conduct such a review to determine whether adequate controls are in place and operating effectively.

MVD's current agreement with IBM expires on December 31, 2005, providing an opportunity to negotiate a provision in the next agreement to include an assurance review at IBM's expense.

MVD should ensure that it receives source code—MVD should also work with IBM to amend the current agreement to ensure that if IBM is no longer the ServiceArizona administrator, the State will receive the programmable source code. This source code is the computer software in its original form as written by the programmer. If IBM no longer administers ServiceArizona, MVD will need the source code so that its programmers can change the program as needed to either improve services or add new services.

Recommendations

MVD should:

- Add a provision to its next agreement with IBM to require IBM to obtain an independent third-party assurance review.
- Amend its current agreement with IBM to ensure that the State receives the programmable source code if IBM no longer administers ServiceArizona.

TO OBTAIN MORE INFORMATION

A copy of the full report can be obtained by calling **(602) 553-0333**

or by visiting our Web site at: www.auditorgen.state.az.us

Contact person for this report: Shan Hays