A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit

Arizona Department of Transportation

Motor Vehicle Division—
Information Security and
E-government Services

SEPTEMBER • 2004
REPORT NO. 04 – 10

STATE OF ARIZONA
OFFICE OF THE
AUDITOR
GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Representative **John Huppenthal,** Chair	Senator **Robert Blendu,** Vice Chair
Representative **Tom Boone**	Senator **Gabrielle Giffords**
Representative **Ken Clark**	Senator **Peter Rios**
Representative **Ted Downing**	Senator **Thayer Verschoor**
Representative **Steve Yarbrough**	Senator **Jim Weiers**
Representative Jake Flake *(ex-officio)*	Senator Ken Bennett *(ex-officio)*

Audit Staff

Shan Hays, Manager and Contact Person

Monique Cordova, Team leader	**Aaron Cook**
Pamelia Eck	**Joe McKersie**

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:
www.auditorgen.state.az.us

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

September 29, 2004

Members of the Arizona Legislature

The Honorable Janet Napolitano, Governor

Mr. Victor Mendez, Director
Arizona Department of Transportation

Transmitted herewith is a report of the Auditor General, A Performance Audit and Sunset Review of the Arizona Department of Transportation, Motor Vehicle Division—Information Security and E-government Services. This report is in response to a November 20, 2002, resolution of the Joint Legislative Audit Committee. The performance audit was conducted as part of the sunset review process prescribed in Arizona Revised Statutes §41-2951 et seq. I am also transmitting with this report a copy of the Report Highlights for this audit to provide a quick summary for your convenience.

As outlined in its response, the Arizona Department of Transportation agrees with all of the findings and plans to implement all of the recommendations.

My staff and I will be pleased to discuss or clarify items in the report.

This report will be released to the public on September 30, 2004.

Sincerely,

Debbie Davenport
Auditor General

Enclosure

SUMMARY

The Office of the Auditor General has conducted a performance audit and sunset review of the Arizona Department of Transportation (ADOT), Motor Vehicle Division (MVD) pursuant to a November 20, 2002, resolution of the Joint Legislative Audit Committee. This audit was conducted as part of the sunset review process prescribed in Arizona Revised Statutes (A.R.S.) §41-2951 et seq and is the second in a series of three reports on the Motor Vehicle Division. The first report addressed several MVD functions that produce or affect the revenue generated for the State (Auditor General report No. 04-09). This report focused on the security of MVD information systems and the status and performance of ServiceArizona, the e-government program that MVD implemented in November 1997. The third report will be an analysis of the 12 statutory sunset factors.

The security of MVD computer systems is important because MVD maintains confidential information about Arizona's residents including names, addresses, and social security numbers. Thousands of workers, both in MVD and other state and local agencies, have access to all or part of this information as they update records or use the data for law enforcement and other functions. In addition, MVD has moved aggressively to provide its services through third parties that provide services similar to field offices and "e-government," such as creating a way to renew vehicle registrations using the Internet. These new approaches are another reason to ensure that good information security systems are in place.

ADOT should strengthen MVD's information system security controls (see pages 9 through 17)

The Arizona Department of Transportation (ADOT) and its MVD need to take steps to strengthen the security of its two major information systems and data. The sensitive nature of the stored data, the large number of MVD employees, other government and third-party users accessing MVD's data as part of their daily business, and the high volume of inquiries and adjustments made to the data each day all increase the risk of improper access or misuse of data. Auditors reviewed several areas of data

security to determine if (1) access to data is appropriately restricted, (2) computer program changes are controlled, (3) necessary policies and procedures are in place, and (4) a plan for bringing services back online if service is interrupted is in place. Auditors identified deficiencies in four areas:

- Access controls—ADOT has not reviewed for appropriateness the specific access levels for some user groups managed by ADOT's access control system.

- Changes made to computer programs—MVD could not provide adequate documentation to show the need for and appropriate implementation of 25 of 30 computer program changes that auditors reviewed.

- Policies and procedures—ADOT has not developed an entity-wide security program that would detail all aspects of data security, including policies and procedures such as background check requirements for people who access MVD data.

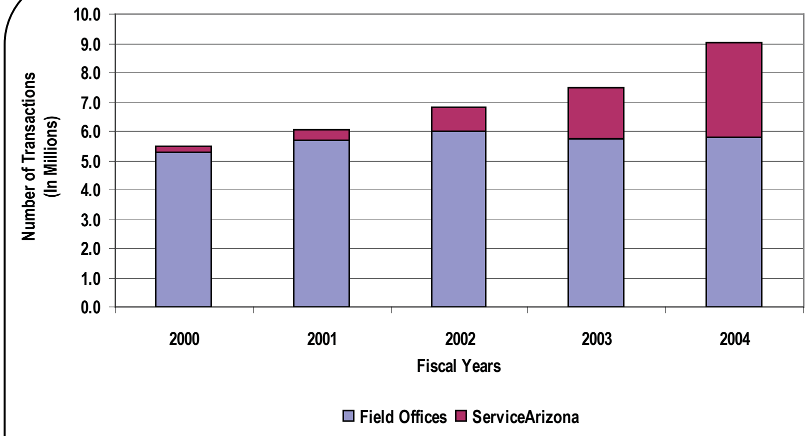
- Data recovery—The Department of Administration, which houses MVD's data in the State Data Center, has a disaster recovery plan to recover MVD data. However, ADOT needs to complete the development of its disaster recovery plan, which it began working on as early as October 2001. MVD reports it should have a plan implemented by February 2007.

During this review, auditors did not find security breaches, but the review was designed more to examine security controls and not to identify instances of improper access or misuse. Even without any evidence of security breaches, the current situation exposes MVD's data to an unnecessary amount of risk, making improvements essential.

ADOT has been aware of a number of these deficiencies for some time, through reviews that Deloitte & Touche auditors conducted in 1997 and 2000. Staffing issues appear to have contributed to the lack of progress in addressing the security weaknesses. Specifically, there has been turnover at the ADOT chief information officer (CIO) position, vacancies in other key positions, and a lack of staff expertise. For example, Deloitte & Touche auditors reported in their 2000 security assessment that ADOT's data security group "lacked the time and expertise to function from an enterprise-wide view of information security." ADOT's CIO believes it is making progress in the staffing area. It hired a qualified data security manager in 2003. It also recently restructured the data security group and hired a new security analyst who has expertise in network security and other areas in which the group had little experience.

Growth in ServiceArizona makes better oversight more important (see pages 19 through 27)

In October 1997, MVD and IBM Corporation (IBM) formed a partnership to operate an “e-government” program known as ServiceArizona. ServiceArizona provides MVD’s customers a convenient way to complete a wide array of MVD services by Internet and telephone, and over 90 percent of the customers who use it and complete the accompanying survey report being very satisfied with it. ServiceArizona has become integral to MVD operations. Every year since its inception, ServiceArizona has grown in the types of services offered, the number of transactions handled, and in revenues collected. As shown in the figure below, ServiceArizona transactions have continued to grow since fiscal year 2000, while field office transactions have remained relatively level. In fiscal year 2004, the Web site gave customers the opportunity to perform 26 different transactions online, and they completed more than 3 million transactions online. In contrast, customers completed just under 2 million transactions in fiscal year 2003. Fiscal year 2004 transactions collected $168.4 million in state revenue. IBM, which underwrote its development costs and hosts the system, earned approximately $6.3 million in fees in fiscal year 2004.



Source: Auditor General staff analysis of ADOT Motor Vehicle Division Director's Update to the Strategic Plan, Fiscal Years 2000 through 2004.

MVD can strengthen its program oversight by renegotiating its current third-party agreement to require that IBM hire an independent outside party to conduct an independent assurance review of IBM’s information security controls. IBM officials report that they have adequate controls to protect customer information, but an assurance review would enable an independent auditor to issue an opinion on IBM’s description of its controls. Further, MVD should amend its third-party agreement with IBM to ensure that MVD receives ServiceArizona’s programmable source code if the agreement expires. Programmable source code is computer software in its original form as written by the programmer. Amending the current third-party agreement to ensure that MVD receives the source code if the agreement expires ensures that MVD’s IT staff could modify the software to meet MVD’s future needs. According to an MVD official, both MVD and IBM have already indicated that they are willing to modify their current agreement to clarify that MVD would receive the source code if the agreement expires.

TABLE OF CONTENTS

continued

TABLE OF CONTENTS

Figures:

Tables:

concluded •

INTRODUCTION & BACKGROUND

The Office of the Auditor General has conducted a performance audit and sunset review of the Arizona Department of Transportation (ADOT), Motor Vehicle Division (MVD) pursuant to a November 20, 2002, resolution of the Joint Legislative Audit Committee. This audit was conducted as part of the sunset review process prescribed in Arizona Revised Statutes (A.R.S.) §41-2951 et seq and is the second in a series of three reports on the Motor Vehicle Division. The first report addressed several MVD functions that produce or affect the revenue generated for the State (Auditor General Report No. 04-09). This report focused on the security of MVD information systems and the status and performance of ServiceArizona, the e-government program that MVD implemented in October 1997. The third report will be an analysis of the 12 statutory sunset factors.

Alternative service delivery methods expand

Since the early 1990s, MVD has been offering customers different ways to obtain motor vehicle services. Typical MVD services include issuing driver's licenses, vehicle titles, and vehicle registrations; enforcing commercial transportation laws and agreements through driver testing and licensing; and collecting a significant amount of state tax revenues such as vehicle license and fuel taxes. In the early 1990s, MVD began providing its customers with alternatives to visiting a local MVD field office for some of these services. For example, customers could obtain several services through private companies called third parties that provide vehicle title and registration services, driver's licensing testing, and some inspections. The use of third parties allows customers to obtain MVD services at more locations and at different hours of the day. MVD reports that it has 488 contractors with agreements to provide MVD services to the public and businesses.

In 1997, MVD significantly expanded its delivery methods with the introduction of electronic, or e-government, services. MVD entered into an agreement with IBM Corporation (IBM), in which IBM agreed to work with MVD to develop the e-government program, now known as ServiceArizona. Currently, the ServiceArizona agreement allows MVD's customers to conduct transactions through three methods:

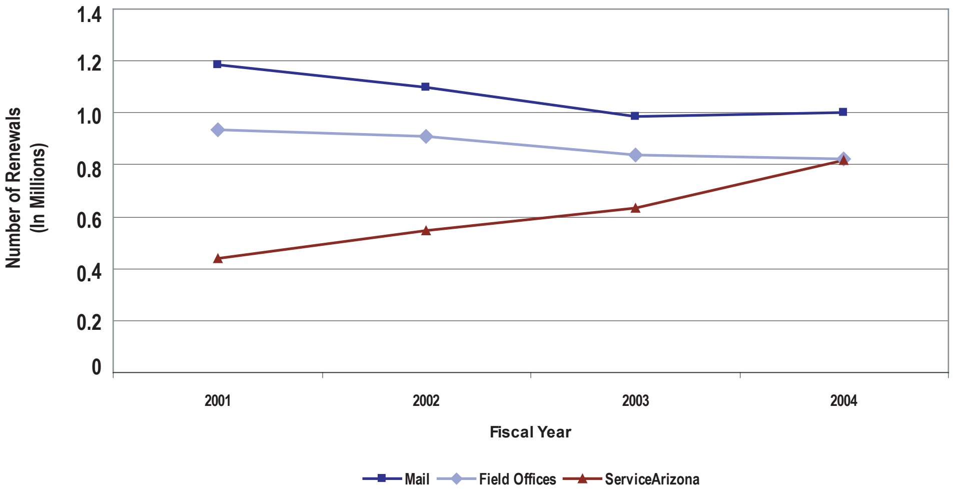
- **Internet**—As of May 2004, customers can conduct 26 different transactions via the ServiceArizona Web portal (www.servicearizona.com), including vehicle registration renewal, driver's license reinstatement, and address changes, as well as voter registration.

- **Telephone**—Customers can conduct vehicle registration renewals via an automated Interactive Voice Response (IVR) system. ServiceArizona's IVR system differs from the informational services that customers receive when they contact an MVD call center.[1]

- **Kiosks**—Customers can also now access the ServiceArizona Web site at MVD field offices through kiosks. In fiscal year 2004, MVD expanded kiosks to15 field offices throughout the State. Kiosks allow customers to complete limited transactions via the ServiceArizona Web site instead of waiting in line for a customer service representative.

MVD's customers have increased their use of ServiceArizona in recent years. Figure 1 shows the vehicle renewal transaction trends for the three main service methods from fiscal years 2001 through 2004. As the figure shows, more renewals have been completed through ServiceArizona each year, while renewals completed using mail and field officers have declined or leveled off.

Figure 1: Vehicle Registration Renewals[1]
Fiscal Years 2001 through 2004



[1] The figure shows the vehicle registration renewals for the three main services. Other service methods, including third parties, account for fewer than 10 percent of the transactions.

Source: Auditor General staff analysis of ADOT Motor Vehicle Division Director's Update to the Strategic Plan, Fiscal Years 2001 through 2004.

[1] MVD operates call centers to answer questions that customers might have about MVD services and to obtain information about a variety of MVD-related issues and services. MVD's call centers allow customers to speak to individuals and ask general or specific questions, whereas the ServiceArizona IVR system allows customers to conduct transactions.

Number of users accessing data through various methods increases importance of information security

MVD's ability to offer services through a variety of methods has heightened the importance of ensuring that it has adequate security controls in place to protect its information systems and customer data. For example, as MVD makes more services available over the Internet, adequate controls are important to protect the electronic information that customers transmit. In addition, MVD's current service environment allows thousands of individuals to access its data. These individuals are not only MVD employees but also employees of third parties that provide MVD services.

Further, employees of other state, county, and local agencies access MVD data as part of normal operations for a variety of reasons in accordance with federal and state statutes. For example, the Department of Economic Security's Child Support Enforcement program employees access MVD data to locate parents. Many of these users have access to sensitive information about MVD's customers, such as names, addresses, and social security numbers, which is necessary in order to perform their jobs. It is important to ensure that MVD's employees as well as external users such as other government employees and third parties have their access restricted to the specific systems, programs, and data they need to perform their jobs.

Information security management

MVD reports that it uses 29 systems to carry out its duties. Its two main systems, the Title and Registration System and the Drivers Licensing System, were introduced in 1973 and 1977, respectively. MVD relies on the following groups to manage and secure its data and information systems:

- ADOT Information Technology Group (167 FTEs)—Responsible for broad computer and network support issues regarding MVD data such as configuration management, access controls, and database administration (see text box on page 4 for definitions of these terms). The IT Group also performs these same tasks for the rest of ADOT, as well as system development and support for all non-MVD systems and programs.

- MVD Custom Systems Solutions (19 contractors and 13 MVD employees)—Performs system development and support for MVD systems. This group reports directly to the MVD director and works closely with both MVD and ADOT IT Group personnel.

- **Arizona Department of Administration (DOA)**—Maintains ADOT's mainframe. MVD houses its data on ADOT's mainframe, located in the DOA State Data Center, and therefore DOA is responsible for the security of the mainframe environment.

Configuration management—Control and document changes made to a system's hardware and software throughout the development and operational life of the system.

Access controls—Protect computer resources from unauthorized modification, loss, or disclosure.

Database administration—Administer the data used throughout an organization by identifying, cataloging, controlling, and coordinating the needs of the entity.

The Legislature granted MVD $2.75 million per year in fiscal years 2002 and 2003 for security and computer upgrade issues. As of July 2004, MVD still had about $2.3 million of the nonlapsing funds available for use. MVD reports that to date it has focused on providing the Office of Special Investigations with tools to investigate cases for prosecution. For example, it is developing an enhanced audit trail and fraud investigation database at a cost of about $780,000. MVD plans to use the remaining monies for a variety of projects, such as additional security enhancements, replacing old servers, and purchasing software. For example, MVD expects to spend about $968,000 on a document imaging and retrieval system; approximately $200,000 on software for commercial driver's license testing; and about $1.2 million on replacing desktop computers, software, printers, and servers.

Followup to 1997 audit

In 1997, the Auditor General conducted a review of customer service issues at field offices and telephone call centers (see Auditor General Report No. 97-13). Although these offices have since instituted some changes to improve efficiency, followup conducted during this audit showed that customers visiting some field offices still have to wait an hour or longer, and that callers also continue to experience significant wait times.

- **Field office wait and transaction times**—The 1997 audit found that customers experienced average service times of 28.6 minutes (including wait and transaction times). Urban offices generally took longer to complete the customer's transactions. Since 1997, the ServiceArizona program has provided an alternative to visiting field offices, and may have helped keep wait times from lengthening despite Arizona's population growth (see Finding 2, pages 19 through 27). In addition, MVD has improved the way it monitors customer wait and transaction times by installing its computerized Q-matic system in more offices.

Q-matic—A computerized system that records how long customers wait in the lobby to be serviced and how long it takes to process their transactions at the window.

For this audit, auditors reviewed wait times in the 32 field offices that had the Q-matic system for all of 2003 and the first 4 months of 2004. Based on Q-matic data, service times are about 22 minutes, with wait times typically of about 14 minutes, and transaction times approximately 8 minutes. However, customers visiting some offices can experience maximum wait times of over 60 minutes. While many of these offices are in the Tucson and Phoenix areas, other offices around the State may have occasional wait times of an hour or longer.

- **Call center access and wait times**—The 1997 audit also found that customers had difficulty accessing MVD for information via the telephone. MVD operates five call centers to assist residents in obtaining information. Customers wishing to speak to a customer service representative are first routed to one of three call centers staffed by Arizona Department of Corrections' inmates. If the customer's request requires the exchange of personal information, then the call is transferred to an MVD employee. In 1997, auditors found that many customers could not get through at all because of busy phone lines, while others experienced long hold times or gave up rather than waiting on hold.

  Since the 1997 audit, MVD has increased the number of inmate call centers from two to three, added more inmate workers, and reorganized its staff call centers to have two MVD call centers in Phoenix and Tucson instead of three MVD call centers housed in Phoenix. In the current audit, auditors still had difficulty accessing MVD call centers. When calling the Phoenix and Tucson call center numbers over a 7-week period from March to May 2004, auditors found that the Phoenix number was busy 67 percent of the time, while the Tucson number was busy 45 percent of the time. In addition, over a 3-week period in April and May 2004, auditors recorded the time they waited to speak to an MVD employee and found that they waited on average about 22 minutes.

Audit scope and methodology

This audit focused on the security of MVD information systems and the status and performance of the ServiceArizona Web site. Auditors also conducted a followup on field office and phone center wait times (see pages 4 through 5). This audit includes two findings and associated recommendations:

- To strengthen the security of information systems, ADOT should improve security controls related to access, changes to computer programs, entity-wide security, and disaster recovery.

- Use of the ServiceArizona Web portal has grown significantly since its inception. MVD can improve oversight of the Web site by requiring IBM to hire an independent third party to complete an assurance review of information security controls. In addition, MVD should amend its agreement with IBM to ensure that the company transfers programmable source code should the agreement terminate.

Source code—A program in its original form as written by the programmer.

Auditors used a variety of methods to review and study the issues addressed in this audit. Audit methods include interviews with the management and staff of MVD, the ADOT IT Group, and IBM; and review of applicable statutes, regulations, policies, and procedures. To perform more specific audit steps, auditors used the following methods:

- To assess the adequacy of information security for MVD's two major systems, auditors reviewed a 1997 Network Review and a 2000 Information Security Assessment, both conducted by Deloitte & Touche. Auditors also reviewed ADOT's internal documents indicating the status of compliance with recommendations made in those and other audits or reports, which it updates on a quarterly basis. To evaluate access management practices and their effectiveness, auditors analyzed summaries of user accounts and user groups and reviewed other mainframe reports produced in March 2004. In addition, auditors reviewed security practices in greater detail by conducting case file reviews, for four samples of 30 user accounts each, as provided in March 2004. Auditors also reviewed documentation relating to program changes implemented between March 2003 and March 2004 in the two main MVD systems—Title and Registration and Drivers Licensing—in order to review control procedures. In addition, auditors reviewed information security standards as defined by the Arizona Government Information Technology Agency (GITA) as well as other national sources, such as the U.S. Government Accountability Office, the National Institute of Standards and Technology, and the Information Systems Audit and Control Foundation.

- To assess the ServiceArizona program, auditors reviewed third-party statutes, IBM's third-party agreement, the program's Web site, transaction data and revenue information for fiscal years 1998 through 2003, and reports by MVD and the American Association of Motor Vehicle Administrators (AAMVA). Auditors also interviewed MVD, IBM, and AAMVA personnel. To determine whether MVD used sound procedures for reconciling transactions and revenues, auditors reviewed MVD's policies and procedures, interviewed the personnel responsible for the process, observed a daily reconciliation process for 6 of the 18 applications for which IBM is allowed to retain a portion of the revenue, interviewed outside consultants currently helping MVD review and improve its procedures, and interviewed personnel from Deloitte & Touche regarding the firm's audit of ADOT. To assess the program's customer satisfaction rates, auditors interviewed IBM personnel about the customer satisfaction survey.

Auditors also reviewed customers' comments for the week of March 1, 2004 through March 7, 2004, and reviewed updates to MVD's Strategic Plan for fiscal years 2000 through 2003. To assess the data security system, auditors interviewed MVD, IBM, and GITA personnel, and reviewed IBM's security policy and other pertinent literature regarding data security, assurance reviews, e-business, and e-government.

- To review customer service wait and transaction times in the field offices, auditors analyzed 16 months of wait time data spanning calendar year 2003 and the first 4 months of calendar year 2004 for MVD's offices equipped with Q-matic monitoring software. Auditors also interviewed supervisors in the East Mesa, Scottsdale, Tempe, and Tucson Regional Field Offices, and reviewed daily transaction reports for the Scottsdale, Tempe, and Tucson Regional Field Offices for selected months in calendar year 2004. To review the accessibility of the call centers, auditors called local access numbers for the Phoenix and Tucson call centers over a 10-week period from February to May 2004. Auditors used 7 weeks of this time period from March through May 2004 to evaluate the frequency of busy signals versus being able to speak to a customer service representative. For 3 weeks during this period, auditors also measured the length of time they had to stay on hold before a level 2 (MVD employee) customer service representative answered the call. Auditors also reviewed MVD call center reports produced using software called Symposium. To assess the validity of these reports, auditors recorded any unusual data, such as 8-hour hold times for callers, and determined from staff if they could explain the unusual findings. Auditors also conducted interviews with Nortel, the company that produces the Symposium software.

The audit was conducted in accordance with government auditing standards.

The Auditor General and staff express appreciation to the director of the Department of Transportation, the director of the Motor Vehicle Division, and their staff for their cooperation and assistance throughout this audit.

FINDING 1

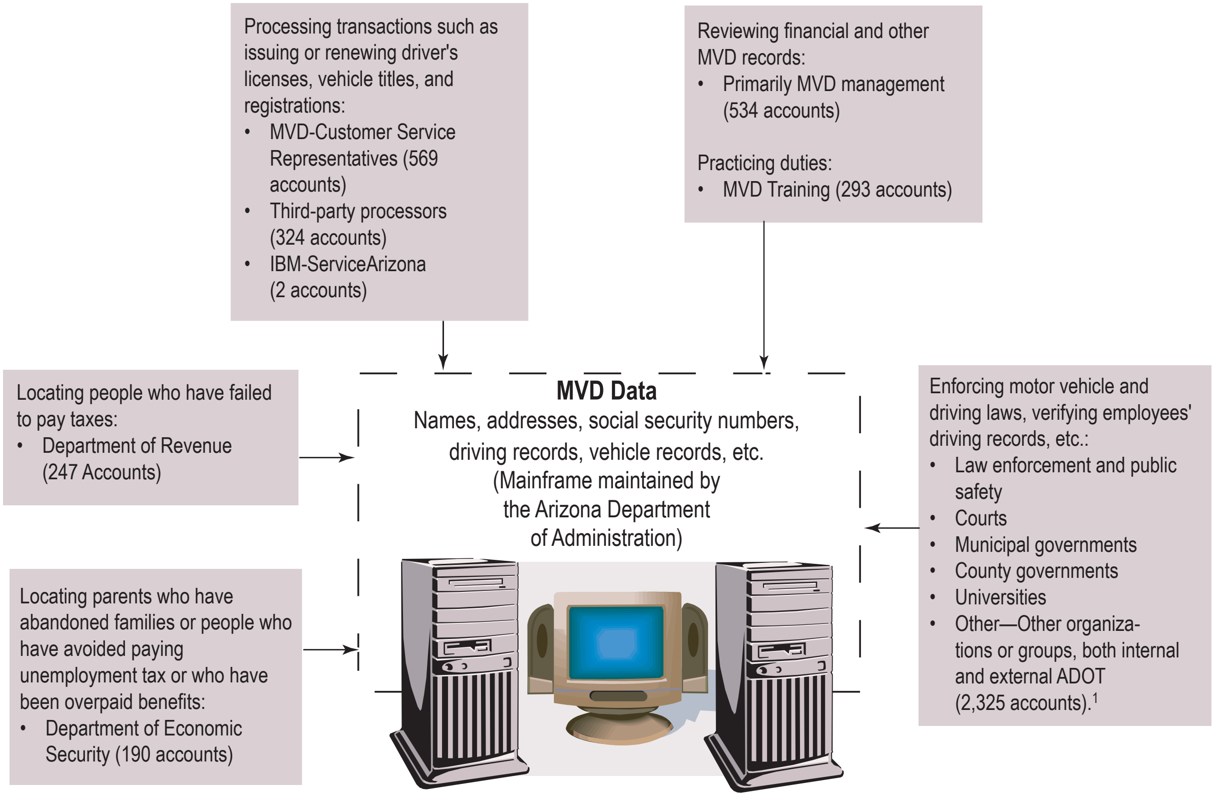
ADOT should strengthen MVD's information system security controls

ADOT and its MVD need to secure MVD's information systems and data. The data's sensitive nature, the large number of users, and the high number of transactions all increase the risk of improper access or use. However, auditors reviewed MVD's two major systems and found that they currently lack effective controls over access, program changes, and disaster recovery. During this review, auditors did not find security breaches, but the review was designed more to examine security controls and not to identify instances of improper access or misuse. The current situation exposes MVD to an unnecessary amount of risk, making improvements necessary. Staff turnover and vacancies help explain why ADOT has not made these improvements.

Many people access MVD data

Thousands of people have access to MVD data as part of their jobs. ADOT controls access to MVD and other ADOT data through user accounts, and as of March 2004 there were nearly 4,500 such accounts, some of which were for more than one person. Some of these accounts are for MVD groups, such as MVD supervisors, customer service representatives (CSRs), and third-party processors. Many other accounts are for other agencies, including state, county, and local agencies involved in law enforcement, parking enforcement, or other functions that use MVD information as permitted by federal and state statute (see Figure 2, page 10). Collectively, these user groups conduct more than 8 million transactions or queries each week, including accessing records that contain MVD customers' personal information (names, addresses, and social security numbers). According to ADOT officials, approximately 3,000 users had access to MVD data as of July 2004.

Figure 2: User Groups Managed by ADOT's Access Control System As of March 2004



Processing transactions such as issuing or renewing driver's licenses, vehicle titles, and registrations:

- MVD-Customer Service Representatives (569 accounts)
- Third-party processors (324 accounts)
- IBM-ServiceArizona (2 accounts)

Reviewing financial and other MVD records:

- Primarily MVD management (534 accounts)

Practicing duties:

- MVD Training (293 accounts)

Locating people who have failed to pay taxes:

- Department of Revenue (247 Accounts)

MVD Data
Names, addresses, social security numbers, driving records, vehicle records, etc. (Mainframe maintained by the Arizona Department of Administration)

Enforcing motor vehicle and driving laws, verifying employees' driving records, etc.:

- Law enforcement and public safety
- Courts
- Municipal governments
- County governments
- Universities
- Other—Other organizations or groups, both internal and external ADOT (2,325 accounts).[1]

Locating parents who have abandoned families or people who have avoided paying unemployment tax or who have been overpaid benefits:

- Department of Economic Security (190 accounts)

[1] Some users may not have access to MVD data. According to ADOT officials, approximately 3,000 users had access to MVD data as of July 2004.

Source: Auditor General staff analysis of ADOT's user account and group summaries provided on March 18, 2004, and interviews with personnel from certain municipal, county, and state entities.

Given the large number of individuals accessing the data, the large transaction volume, and the information's sensitive nature, ensuring the security of MVD systems and data is important. Protecting the computer systems and its data is critical to prevent individuals with malicious intent from intruding into systems, obtaining sensitive information, committing fraud, and disrupting services. Given the wide range of users, this risk comes from both employees internally and others outside of the agency.

ADOT officials have taken some steps to assess these security risks. For example, Deloitte & Touche performed a comprehensive security assessment of the entire agency and released their report in June 2000. ADOT completes quarterly audit follow-up reports to monitor its progress in implementing Deloitte & Touche's recommendations and other audit recommendations. ADOT also performs an annual information security risk assessment with the intent to identify areas for improvement.

Several types of weaknesses exist in protecting division data

Although ADOT and MVD have taken steps to assess security risks, controls over several key elements of security planning and management are weak. Auditors reviewed controls affecting MVD's two main systems—the Title and Registration System and the Drivers Licensing System. Auditors identified deficiencies in four areas, indicating that data in MVD's two major systems is exposed to an unnecessary amount of risk.

Major Security Control Areas Examined

Access controls—Ensure that lists of authorized users are accurate and up-to-date, and that users have access only to the data they need.

Computer program change controls—Ensure that only authorized changes are made to computer programs, and that the changes are reviewed to ensure they work as designed.

General policies and procedures—Ensure that the organization has policies and procedures for keeping entity-wide security levels achievable and sustainable.

Business continuity and disaster recovery—Ensure that an organization can protect and recover its assets while maintaining critical services in the event of a major hardware or software failure or destruction of facilities.

ADOT does not adequately restrict access to MVD systems—Access controls should provide reasonable assurance that access to systems and data is limited to authorized users for purposes related to their function and responsibility. Data should be protected against unauthorized modification or inappropriate disclosure. For instance, access controls should include procedures for reviewing and defining who can access the data, maintaining adequate documentation to monitor access, and monitoring the status of user accounts to ensure improper access does not occur. However, ADOT lacks several controls to help ensure that data is adequately restricted. Table 1 (see page 12) explains these controls and describes the situations that the auditors found regarding them.

Such weaknesses in access controls can impact data security. If access controls are inadequate, then users may be able to access data inappropriately, commit fraud, or otherwise compromise the system. Because auditors were primarily assessing system controls, they did not attempt to identify actual cases in which a breach of security occurred. However, auditors did observe situations that illustrated the potential for such occurrences. For example:

- In reviewing a random sample of 30 CSR user accounts, auditors discovered that one employee in the CSR user group was actually an MVD enforcement officer. Placing the enforcement officer in the CSR group means that the

Table 1: Deficient Access Control Areas in MVD's Two Major Systems
As of March 2004

Necessary Controls	Conditions Found
Access rights: Users should be restricted to the specific systems, programs, and data they need to perform their duties.	• Despite Deloitte & Touche's recommendation in a 1997 network review to define security levels for each user group, as of March 2004, some user groups still had security levels that had not been reviewed for appropriateness. Although ADOT has reviewed access for many user groups, it still needs to review access for the remaining groups.
Extent of access authority: Users should not be able to create, delete, or modify records if their functions do not require them to do so.	• Customer service representatives (CSRs) could correct certain errors that can occur when data is shared with other states' motor vehicle departments—an ability that MVD programmers indicated should be reserved for technical support. • Programmers reported that about 20 percent of the transactions CSRs are allowed to conduct in the system are obsolete and should be removed.
Assigning access rights: Those responsible for granting levels of access need information that will allow them to grant access at the proper level.	• The current access request form does not show a new employee's position. Therefore, there is insufficient information to grant the proper level of access. Granting too much access can allow employees to modify, create, or delete records when they do not have authorization to do so.
Maintaining documentation about users: Those granting access to systems should ensure that users receive appropriate access by receiving and maintaining access request forms and help ensure that users understand their responsibilities by receiving and maintaining access agreement forms.	• Auditors reviewed the presence of access request forms in four different samples. Request forms could not be located for 10 of 27 (37 percent) user accounts in a random sample of all user accounts, including 1 of 9 (11 percent) among accounts created in the past 3 years; 1 of 29 (3 percent) user accounts of CSRs hired in the last 3 years; 1 of 29 (3 percent) third-party processors hired in the last 3 years; and 4 of 27 (15 percent) user accounts belonging to a user group composed primarily of MVD management, including 1 of 8 (13 percent) created in the past 3 years. • Computer access agreements could not be located for 12 of 27 (44 percent) user accounts in a general user sample, including 1 of 9 (11 percent) among accounts created in the past 3 years; 3 of 29 (10 percent) user accounts of CSRs hired in the last 3 years; and 10 of 27 (37 percent) user accounts belonging to a user group composed primarily of MVD management, including 2 of 8 (25 percent) among accounts created in the past 3 years. All 29 user accounts belonging to third-party processors hired in the last 3 years were located. • The IT Group, which creates new user accounts, does not have a list of persons authorized to grant access, and, therefore, cannot ensure that access is properly authorized before establishing a new account.
Controlling accounts with outside parties: Those controlling outside parties' access to data should ensure that access is appropriately granted and restricted.	• MVD's Electronic Data Services Unit, which oversees the access of employees from other government agencies, does not maintain a centralized list of users from other agencies who can access MVD data. • Information on employees from other agencies is out of date. Auditors' review of 437 names listed as having access from the Arizona Department of Revenue and the Arizona Department of Economic Security showed that 13 no longer worked for those agencies. • MVD's Title and Registration Partnerships Group, which oversees the access of third-party employees, had an outdated list that showed only 292 of the 317 third-party user accounts as of March 2004.
Updating passwords and removing unused accounts: Users should have to change their passwords at regular intervals, and unused accounts should be removed from the system as appropriate.	• Some accounts assigned to individuals and many accounts for more than one person do not require users to change their passwords at regular intervals. • Many accounts had not been used for more than 1 year.

Source: Auditor General staff analysis of ADOT's user summary report as of March 18, 2004; case file reviews for four samples of 30 user accounts each; Deloitte & Touche's *ADOT TCP/IP and Third Party Network Review* (July 1997); U.S. Government Accountability Office's *Federal Information System Controls Audit Manual* (Jan. 1999); and the National Institute of Standards and Technology's *An Introduction to Computer Security: The NIST Handbook* (Oct. 1995).

enforcement officer, who should be allowed to look at records only to verify information, inappropriately has the ability to create, delete, and modify records.

- According to MVD system programmers, CSRs had access to a transaction allowing them to correct certain errors that can occur when they share data with other states' motor vehicle departments. This authority should be reserved for technical support.

- Thirteen former employees of other agencies did not have their access revoked after they terminated their employment with their agencies, allowing a situation in which records could be inappropriately accessed or modified. ADOT's security system deactivates any user account that is not accessed for a certain period of time. However, until that period of inactivity lapses, a user account that is no longer needed, either because the employee was terminated or the employee no longer needs access, can pose a security risk.

- The presence of unused accounts potentially increases the risk of unauthorized access, and therefore only unused accounts that meet specific criteria should be retained. For example, training accounts with restricted access may be appropriate to retain even when unused. However, ADOT has not developed criteria to determine which user accounts should be maintained despite inactivity.

In some cases, ADOT and MVD personnel indicated that changes have been made or were underway to address the control weaknesses. For example, ADOT has eliminated CSRs' ability to have access to the inappropriate transactions. In addition, in order to keep the list of third-party processors with access to MVD systems up-to-date, MVD transferred responsibility for maintaining the list to an employee who has more direct contact with third-party processors, and gave the person who oversees third parties the ability to review their account status to detect when an account is no longer in use. In addition, according to MVD management, MVD plans to begin providing other government employees access through a Web-based application. According to MVD management, once this is done, MVD will develop a centralized list of users. MVD should periodically review the lists of third-party processors and other government employees to ensure that they are up-to-date and accurate.

Nevertheless, the weaknesses identified indicate that ADOT and MVD need to take action on a number of fronts in the area of data security. ADOT should ensure that access request forms provide sufficient information, such as new employees' positions, and are properly authorized; access request and computer user agreements are submitted and maintained; and criteria are documented for keeping old user accounts or accounts without passwords. For its part, MVD should ensure that access for employees of other government agencies is removed in a timely fashion when these users no longer need access. Finally, ADOT and MVD should collaborate to review the access of all user groups in order to ensure they are appropriately defined and limited. In doing this, ADOT and MVD should document the rationale for access and authority level given to each user group. In addition, ADOT and MVD should ensure that users are placed in the appropriate user group. Access rights should also be reviewed on a periodic basis to ensure that they remain appropriate.

Computer program changes are not adequately controlled—This type of control helps ensure that only authorized modifications to computer programs are implemented. Documentation for changes should include five items: 1) request for the change, 2) design of the change, 3) testing the change, 4) approval given if the test results were satisfactory, and 5) implementation. However, MVD does not have written policies requiring this documentation and cannot demonstrate that only authorized changes have been made. Auditors reviewed 30 known program changes made between March 2003 and March 2004, and MVD could not provide adequate documentation for 25 of 30 program changes (83 percent). In several instances, programmers had no documentation at all, and when documentation was available, it indicated that programmers often implemented changes before they were tested and approved. In addition, when the documentation included a formal written request, it did not always have appropriate signatures and dates from those requesting the modification. MVD should develop policies and procedures to ensure that it maintains proper documentation for all program changes. In addition, it should develop controls to help ensure that programmers cannot make unauthorized system changes.

Adequate documentation was missing for some program changes.

General policies and procedures not adequate—Clear and adequate policies help an agency's personnel ensure that appropriate security levels are achievable and sustainable.[1] Currently, ADOT and MVD lack or do not enforce policies in several areas, ranging from a general entity-wide security program to training (see Table 2, page 15). The absence of these general policies and procedures lessens the likelihood of carrying out a thorough and consistent approach to computer security. However, ADOT is making some progress. For example, one weakness is that employees accessing MVD data are typically not receiving computer security awareness training. According to an ADOT official, ADOT is developing a Web-based computer security training program that should help increase the number of personnel who take the course. The training should be available by September 2004. Further, ADOT recently hired a new security analyst whose responsibility is to develop policies and procedures for an entity-wide security program. ADOT's chief information officer believes that by the end of 2004 the agency should have developed a priority list for formulating policies and procedures and will have begun creating them.

ADOT should ensure that general policies and procedures adequately protect MVD data. Specifically, it should document an entity-wide security program; establish policies to require background checks at initial hire and on an ongoing basis for employees accessing and securing data; and ensure that the new Web-based

[1] Arizona Government Information Technology Agency (GITA). *State of Arizona Target Security Architecture Information Technology (IT) Technical Document,* Revision 1.0. Phoenix GITA, May 6, 2003.

Table 2: Deficient General Policy and Procedure Controls
As of March 2004

Necessary Controls	Conditions Found
Entity-wide security program: A set of written policies and procedures helps ensure that appropriate security levels are achievable and sustainable. Such policies should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.	• Deloitte & Touche's June 2000 report noted that ADOT had not developed policies and procedures for most of its information security program. Specifically, ADOT lacked policies in important areas such as the overall purpose and organization of the IT group, network security, classifying data according to criticality and sensitivity, and responding to security-related incidents. • These policies and procedures were still not developed when this audit was conducted.
Background checks: Should be conducted on all persons accessing and securing data to protect against hiring untrustworthy individuals who could commit fraud or otherwise compromise data.	• Written policy requires that only MVD peace officers have a background check. • An MVD Office of Special Investigations official said it also performs background checks on customer service representatives (CSRs) in accordance with a 1999 verbal agreement. However, a review of 30 CSRs hired in the past 3 years found that the Office performed background checks on only 24 (80 percent)of them. • Other personnel, including programmers responsible for maintaining MVD's computer systems, do not receive background checks at all.
Security awareness training: Helps ensure that users are aware of the data access rules, their responsibilities, and their expected behavior, thus limiting the possibility that users could misuse the data. ADOT policy calls for providing this training within 6 months of hire.	• The user account samples that auditors tested included accounts belonging to 78 ADOT and MVD employees. Auditors found that only 37 (47 percent) of these employees completed the required course. Further, just 8 of the 30 (27 percent) CSRs tested completed the security awareness course. • Although they are required to receive some computer security awareness training, MVD does not require third parties' employees to undergo the same level of computer security awareness training as ADOT and MVD employees.

Source: Auditor General staff analysis of ADOT's user summary report as of March 18, 2004; case file reviews performed by Auditor General staff; Deloitte & Touche's *ADOT Information Security Assessment* (June 2000); ADOT and MVD policy; and the U.S. Government Accountability Office's *Federal Information System Controls Audit Manual* (Jan. 1999).

computer security awareness training is given to employees when first hired and on an ongoing basis.

Business continuity/disaster recovery plan is not completed—A business continuity/disaster recovery plan specifies how an organization will protect and recover state assets while maintaining critical public services in the event of a major hardware or software failure or destruction of facilities. Arizona's Government Information Technology Agency (GITA) breaks the development of a plan into three phases: assessing the impact of a system failure on critical business processes, developing a strategy to recover from failure, and implementing the strategy. The Arizona Department of Administration (DOA), which houses MVD data on the ADOT mainframe, is responsible for bringing the mainframe back online in the event of a service disruption, but ADOT is responsible for bringing all of its computers and network equipment back up at all administrative and field office buildings in the event of service disruption. DOA has formulated a recovery plan for bringing the ADOT mainframe systems back online and tests the plan biannually.

However, although the ADOT Information Technology Group's 2004-2009 strategic plan shows it began working on a plan as early as October 2001, ADOT has not completed the first phase in developing its plan—performing a business impact assessment. According to an ADOT official, the agency plans to hire an individual by September 2004 whose primary responsibility will be to conduct a business impact assessment and develop a recovery strategy. In addition, ADOT has already purchased computer software to aid in documenting and designing the recovery program. According to ADOT officials, ADOT plans to complete the impact assessment by September 15, 2005, and implement a recovery plan by February 2007. ADOT should ensure that it develops and documents a recovery program, and that it is regularly tested once it is implemented.

Staffing issues contribute to lack of action

Staffing issues appear to have contributed to a lack of progress in addressing these security issues. The ADOT IT Group has experienced turnover and vacancies at key positions, which affects the level of effort and expertise available to address security concerns. Specifically:

- **Lack of leadership continuity**—Since June 2000, ADOT has had three different chief information officers. The current CIO has been in his position since February 2003.

- **Difficulty in filling vacancies**—The ADOT data security group has experienced vacancies recently, which has affected the amount of work it can perform. As of March 2004 the data security group consisted of three individuals and had two vacancies, and the group principally handled access management. Deloitte & Touche's 2000 security assessment noted that the data security group "lacked the time and expertise to function from an enterprise-wide view of information security."

While the ADOT CIO believes it is making progress in this area, he acknowledges that developing the necessary capability remains a work in process. ADOT began to address the lack of expertise by hiring a qualified data security manager in 2003. In addition, the IT Group recently restructured the data security group and hired a new security analyst with expertise in areas that the group previously had little experience in, such as network security. As of July 2004, the data security group consisted of seven individuals who now handle access management, network security, virus protection, and policy and procedure development.

Recommendations

1. To better manage access to systems and data, ADOT and MVD should collaborate to review the access of all user groups in order to ensure they are appropriately defined. In doing this, ADOT and MVD should document the rationale for access and authority level given to each user group. In addition, ADOT and MVD should ensure that users are placed in the appropriate user group. Access rights should also be reviewed on a periodic basis to ensure that they remain appropriate.
2. To better manage access to systems and data, MVD should:
   a. Work more closely with other government agencies to ensure that user accounts are removed when an employee leaves employment or when the employee no longer needs the access.
   b. Periodically review the lists of third-party processors and other government employees to ensure that they are up-to-date and accurate.
3. To better manage access to systems and data, ADOT should:
   a. Alter the access request form to better enable the IT Group to know the access and authority level it needs to give an individual within a given system, perhaps by including position title on the access request form.
   b. Ensure that it receives and maintains documentation required to set up new user accounts, and that controls are in place to help ensure that access is properly authorized.
   c. Produce reports that indicate accounts without password intervals and appropriately restricting this privilege, as well as document criteria for user accounts that are kept without password intervals or that are maintained in disuse.
4. MVD should better control the implementation of program changes by developing policies and procedures for ensuring that it maintains proper documentation for all program changes. In addition, MVD should implement controls to help ensure unauthorized changes are not made to the system.
5. ADOT should develop an entity-wide security program. This program should address all aspects of security such as establishing a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. In addition, the program should:
   a. Ensure that those accessing and securing its sensitive information meet generally accepted standards by requiring background checks of personnel on an initial and ongoing basis, consistent with the sensitivity of their positions.
   b. Ensure that all its employees as well as those of the third-party contractors undergo computer security awareness training at initial hire and on an ongoing basis.
6. ADOT should implement the business continuity/disaster recovery plan on schedule and regularly test the plan for adequacy.

FINDING 2

Growth in ServiceArizona makes better oversight more important

Since 1997, the MVD has worked with IBM Corporation (IBM) to operate ServiceArizona, an e-government system. ServiceArizona provides MVD's customers a convenient way to complete a wide array of services primarily through the Internet, and it is one of the most extensive programs of its type in the nation. ServiceArizona has become integral to MVD operations. Every year since its inception, ServiceArizona has grown in the types of services offered, the number of transactions handled, and in state revenues collected. As this piece of MVD's service network becomes more and more important to Arizonans, protecting its security and continuity therefore becomes more critical. To that end, MVD can strengthen its oversight of the program by requiring IBM to obtain an independent review of information security controls and by amending the current agreement to ensure that MVD receives the programmable source code if the relationship terminates.

E-government used to improve customer service and help field offices

In late 1997, MVD signed an agreement with IBM to work together to create ServiceArizona with the intent of improving customer satisfaction and shortening wait times at field offices by reducing the number of visits. Customers who use ServiceArizona and complete its survey report that they are very satisfied with the program. In addition, the number of field office transactions has remained fairly level instead of increasing with Arizona's growing population.

IBM developed program and receives third-party compensations—In October 1997, MVD added IBM to its third-party program specifically to develop and host ServiceArizona, an electronic service system that allows MVD customers to complete MVD services via the Internet and telephone. An MVD official said it selected IBM to host ServiceArizona because it was the only company willing to accept the project. MVD did not have resources to invest in the project and needed

to find a business partner that could assume the up-front costs associated with building ServiceArizona. IBM agreed to develop and host the program and receives compensation as shown in Table 3.[1]

Table 3: Services Available on ServiceArizona's Web Site
As of May 2004

Year Service Initiated	Services[1]	Service Fees Directed To IBM
1997	Vehicle Registration Renewal	$1 per registration plus a minimum of 2 percent of the vehicle license tax
1999	*Permanent Fleet Renewal*	$1 per registration plus a minimum of 2 percent of the vehicle license tax
1999	Specialty Plate	$2 per plate[2]
2000	Duplicate Driver's License	$4 per duplicate
2000	Address Change	-
2000	Dishonored Check/NSF Check Fee Payment	$1 per NSF check payment[2]
2000	Abandoned Vehicle Fee Payment	$1 per abandoned vehicle payment[2]
2001	Vehicle Sold Notice	-
2001	Personalized Plate	$2 per plate[2]
2002	Plate Credit	-
2002	Restricted 3-Day Permit	$1 per permit
2002	*Registration Plate Fee Credit*	-
2002	*Registration Fee Calculation*	-
2002	*90-Day Resident Registration Permit*	$1 per permit
2002	Driver's License Reinstatement	-
2002	Voter Registration	-
2003	*Motor Carrier Permit*	$1 per permit
2003	*Temporary Registration Permit*	$1 per permit
2003	*Dealer Licensing Renewal*	$5 per application[2]
2003	Duplicate Vehicle Registration	$1 per registration
2003	Vehicle De-insure Certificate	-
2003	Veterans Plate (AZ VA Dept)	$2 per plate[2]
2004	Customer 30-Day General Use Permit	$1 per permit
2004	*Vehicle Dealer 30-Day General Use Permit*	$1 per permit
2004	*Abandoned Vehicle Title*	$1 per title[2]
2004	Organ Donor Plate	$2 per plate[2]

[1] Services listed in italics are Business Services, while all other services listed are resident services.

[2] Fee became effective in late August 2004.

Source: Auditor General staff analysis of A.R.S. §28-5101 (E) and (F) and internal MVD reports.

[1] The fees charged by IBM have changed since ServiceArizona's inception. Initially, IBM and other third-party service providers could charge a reasonable and commensurate convenience fee for their services. Legislation effective in August 1998 allowed MVD to reimburse third parties such as IBM and set out specific amounts per service. Legislation passed in 2001 and new legislation that became effective August 25, 2004, specified amounts for additional services. Third parties are still allowed to charge fees in addition to the statutory reimbursements. MVD officials report that per A.R.S. §28-4549, IBM currently charges a fee for one business service—temporary registration permit—for which the State charges nothing.

Currently, ServiceArizona consists of three components: a Web site, an interactive voice recognition system (IVR), and kiosks that are located in several field offices. The Web site and IVR systems are available 7 days a week and nearly 24 hours every day. The Web site provides a wide array of MVD and other services, while the IVR system provides vehicle registration renewals. The kiosks, which are computer terminals that provide customers an additional way to access the Web site, are mostly located in several field offices in the Phoenix and Tucson areas.

Third-party fees include several different amounts, depending on the fees or taxes collected. A third party is allowed to collect and retain a reasonable charge for its services, according to A.R.S. §28-5101(E). In addition to such charges, A.R.S. §28-5101(F) prescribes the amounts that ADOT must reimburse a third party for various fees, taxes, and filings it collects for ADOT, while A.R.S. §28-374(B) requires a third party to deduct or be reimbursed for any fee charged or withheld for use of a credit card, debit card, or electronic transfer.

They Customers appreciate ServiceArizona—ServiceArizona's online survey results suggest that MVD has succeeded in developing an easy way for customers to conduct business with MVD, and customers are satisfied. At the conclusion of every resident service offered on ServiceArizona, the application offers customers a chance to complete a two-question survey and to provide comments. MVD officials report that overall customer satisfaction ratings for ServiceArizona have exceeded 90 percent since the program's start. In addition, MVD's annual updates to its strategic plan reports that average customer satisfaction ratings for fiscal years 2000 through 2004 exceeded 99 percent.

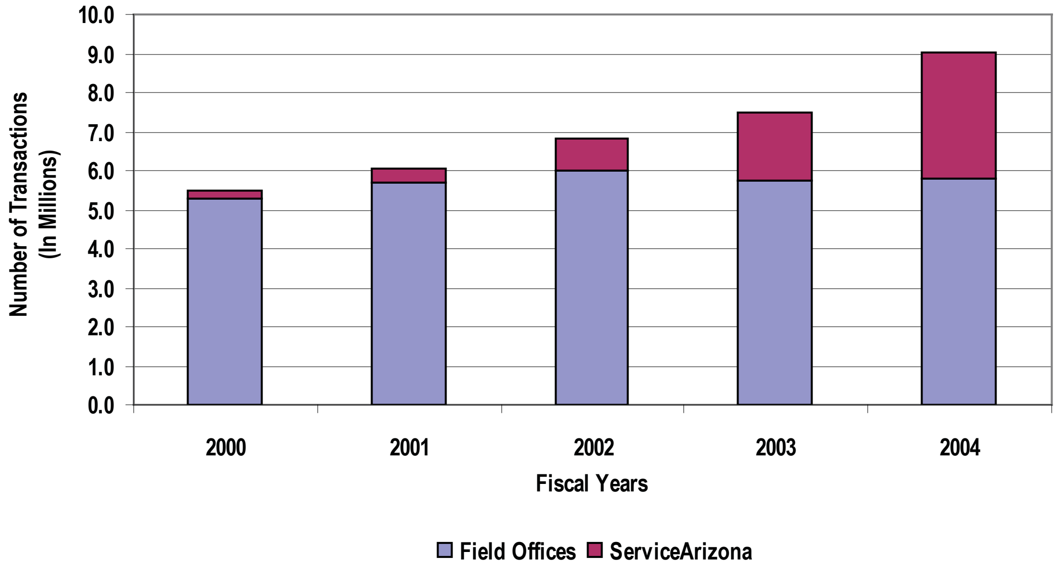
MVD reports high customer satisfaction with ServiceArizona.

- "Absolutely love that I can do this so quickly and so easily online & at my own convenience. So much better than trying to do it over the phone or in person. Thanks!"

- "I think that this is an excellent way to renew registration of vehicles. Took me less than 2 minutes."

ServiceArizona may have contributed to a leveling in field office transactions—MVD's third-party program was designed to reduce the need for field office visits, and thereby help achieve the goal of keeping field office service times to 30 minutes or less. MVD reports indicate that field office transactions have remained fairly level (see Figure 3, page 22). This does not mean, however, that ServiceArizona has had no effect on field office transactions. During this period, Arizona's population has continued to grow, and MVD indicated that field office transactions have remained relatively stable despite ServiceArizona. ServiceArizona use may have reduced field office transactions by helping to limit the number of people waiting for service, and thus keeping wait times from lengthening (see discussion in the Introduction and Background section of this report, page 7).

Figure 3: Comparison of MVD Field Offices and ServiceArizona Growth in Number of Transactions Fiscal Years 2000 through 2004 (Unaudited)



Source: Auditor General staff analysis of ADOT Motor Vehicle Division Director's Update to the Strategic Plan, Fiscal Years 2000 through 2004.

ServiceArizona has rapidly expanded

Growth in services offered and the number of transactions completed online has made ServiceArizona integral to MVD's operations. The program has grown significantly since inception in the number of services offered, transactions completed, and revenue collected.

ServiceArizona offers 26 different services.

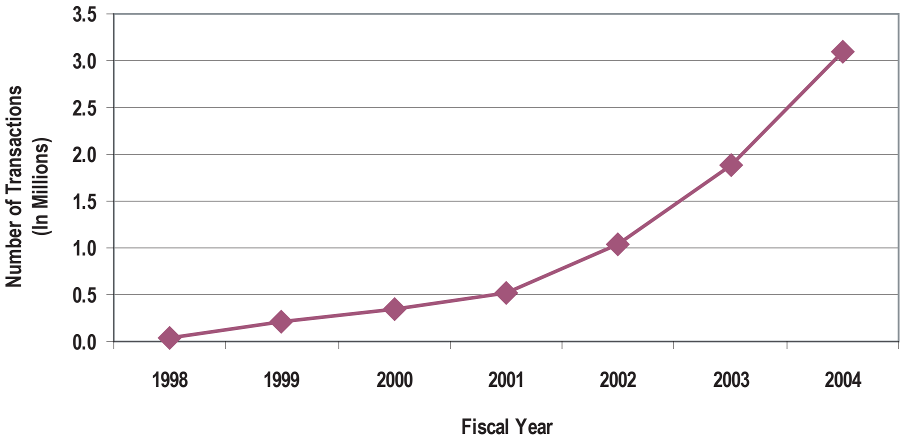
- More kinds of services—As of June 2004, the Web site allows citizens and businesses to complete 26 different services, including ordering specialty plates, driver's license address changes, and voter registration. As shown in Table 3 (see page 20), the program began by offering only vehicle registration renewals. An MVD official indicated that MVD initially selected renewals to reduce foot traffic into field offices and because MVD had already done business with these customers and they were already in MVD's database. MVD reports processing several million vehicle-registration renewals each year through its field offices, third-party programs including ServiceArizona, and renew-by-mail, and they comprise MVD's single largest service. As of July 2004, MVD is considering adding another 15 services to ServiceArizona's Web site over the coming years. For example, the Traffic Ticket Enforcement Assistance

Program is scheduled to go online in 2004 to help increase compliance with traffic ticket payments. This service will help the courts collect delinquent debts by preventing customers from renewing their vehicle's registration until they pay their tickets. According to an American Association of Motor Vehicle Administrators report completed in December 2003, 49 of 50 states' motor vehicle administrations offer some services via the Internet. However, few states offered as many services as ServiceArizona.

Few state motor vehicle administrations offer as many Internet services as ServiceArizona.

- **More transactions**—The growth and proportion of total MVD transactions that ServiceArizona completes has grown significantly since the program's inception. For example, MVD reports indicate that ServiceArizona handled close to 205,000 transactions in fiscal year 1999, its first full year of operation. This number consisted solely of vehicle registration renewals, and accounted for approximately 7.3 percent of renewals that fiscal year. In contrast, ServiceArizona accounted for 27.9 percent of vehicle registration renewals in fiscal year 2004. MVD reports that customers completed more than 3 million transactions through the Web portal in fiscal year 2004 (see Figure 4).

Figure 4: ServiceArizona Transactions[1]
Fiscal Years 1998 through 2004
(Unaudited)



[1] The table excludes Vehicles Sold Notices and Vehicle De-insure Certificates because MVD cannot identify which transactions were completed on ServiceArizona's Web site and which were completed on the Agency's Web site. All other transactions were included, whether or not a fee was associated with the transactions.

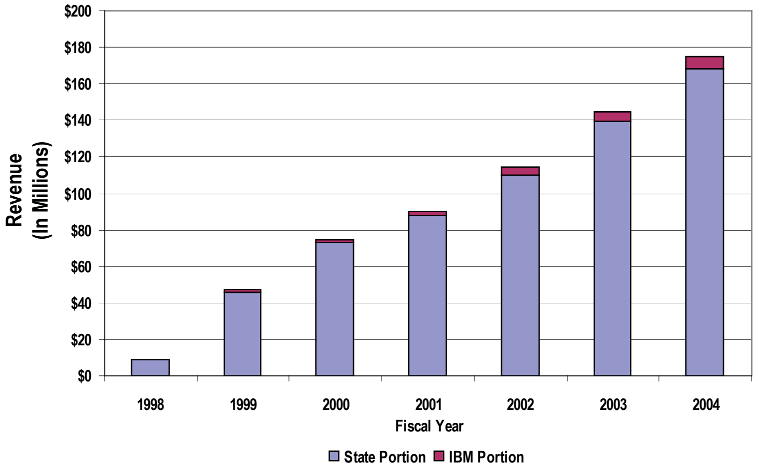
Source: Auditor General staff analysis of ServiceArizona's database transactions records.

- **More revenues collected**—The amount of MVD revenue that IBM collects has also grown each year. For example, as shown in Figure 5, MVD reports collecting nearly $168.4 million in state revenues through ServiceArizona in fiscal year 2004, compared to only $46 million in fiscal year 1999. MVD's third-party laws define how much any third party earns for a service. IBM collects revenue and receives reimbursement for 18 of the 26 services it offers (see Table 3, page 20). MVD also reports that in fiscal year 2004, IBM earned approximately $6.3 million for its services, or 3.6 percent of the fees collected. MVD also reports reimbursing IBM for more than $2.8 million in credit card transaction fees in fiscal year 2004.

IBM applies ServiceArizona earnings to state Web portal

In March 2001, the Government Information Technology Agency (GITA) contracted with IBM to develop and operate a second Web portal known as "Arizona at Your Service." This state Web portal provides a "one-stop shopping" Web site for Arizona's citizens, businesses, and other government entities who need to obtain information about state government. As of January 2003, if IBM's ServiceArizona revenues exceed its costs to provide services, IBM is required to make the excess ServiceArizona revenues available to the Arizona at Your Service Web portal. GITA reports that as of March 2004, IBM has contributed $191,000 to the state Web

Figure 5: ServiceArizona—Collected Revenues
Fiscal Years 1998 through 2004
(Unaudited)



Source: Auditor General staff analysis of MVD's financial data for annual revenue collected through ServiceArizona for fiscal years 1998 through 2004.

MVD should strengthen its monitoring of ServiceArizona

MVD should strengthen its oversight of ServiceArizona. MVD is responsible for monitoring the collection of millions of dollars in MVD revenues that pass through ServiceArizona each year and for protecting the personal data transmitted via the Internet. As the use of ServiceArizona continues to grow, effective monitoring becomes all the more important. MVD and IBM have reconciliation processes in place to monitor fee collection, and IBM reports having a number of controls in place for protecting the privacy and security of information. However, MVD should improve its monitoring of ServiceArizona's computer system by requiring IBM to hire an independent outside party to conduct an assurance review of IBM's controls, and by amending its third-party agreement with IBM to ensure that MVD receives ServiceArizona's source code if the agreement expires.

Reconciliation procedures exist to monitor revenue submission—Under its third-party agreement, IBM must comply with all of MVD's written security directives, statutes, rules, regulations, policies, and procedures that MVD provides, including those related to fee collection. Fee collection provisions include collecting and depositing all fees associated with the program's activities; maintaining logs that track the service and convenience fees collected; and reconciling the monies on an MVD form. IBM is required to maintain logs for audit purposes and to retain these records for a 5-year period. MVD reports that it has policies and procedures in place to monitor the revenues that ServiceArizona collects and remits. The policies and procedures include requirements set forth in MVD's third-party agreement, a written reconciliation process, and the actual reconciliation process. Although this Office did not audit MVD's system, auditors observed the reconciliation process once for deposits for 6 of the 18 ServiceArizona applications that generate revenues for IBM, and all appear to follow established policies and procedures.[1]

IBM reports various controls are in place for data security—IBM is responsible for securing and maintaining the ServiceArizona Web site, and IBM officials indicate that they have adequate controls in place to protect the privacy and security of customers' personal information. For example, IBM indicates that it uses secure socket layers, the computer industry's standard method for protecting Internet communication. Secure socket layers transmit data in an encrypted form, which decreases the chances that unauthorized parties can read the data because it requires the reader to have the appropriate decryption key. IBM officials report that they keep all confidential records encrypted while transmitting between its system and MVD's system. The ServiceArizona Web site also indicates keeping credit card information confidential by encrypting a customer's credit card number before it leaves the customer's computer.

Assurance review would improve oversight of MVD data—These procedures and controls notwithstanding, MVD can do more to ensure ServiceArizona data security. MVD's third-party agreement permits MVD employees, representatives, and agents to conduct unannounced inspections and audits, although MVD has chosen not to exercise this right to date. At this time, MVD would have to pay for someone to conduct a review because the current agreement does not contain any provisions that require IBM to hire outside auditors to contract and pay for an outside review. MVD should renegotiate the agreement to require IBM to hire an independent third party to complete an assurance review. This would provide MVD and the general public with a higher degree of confidence regarding IBM's efforts to protect the personal data that customers submit through the Internet. The current third-party agreement expires on December 31, 2005, and automatically renews for 2 years unless either party terminates within 30 days of that date. This termination date gives MVD an opportunity to negotiate a provision to include an

Third-party assurance reviews would provide a higher degree of confidence regarding data security.

[1] Auditors observed the reconciliation processes for the following applications: Dealer 30-Day General Use Permits, Duplicate Driver's Licenses, Fleet Renewals, Motor Carrier Permits, Temporary Registration Plates, and Vehicle Registration Renewals.

assurance review at IBM's expense before the agreement renews, or MVD could provide IBM with notice that it will not renew unless IBM agrees to complete an assurance review at its own expense. The extent of work that an outside auditor would be engaged to perform depends upon the level of assurance that MVD requires. For example, an assurance review can determine whether controls are in place, or whether they operate effectively. Although MVD and IBM can mutually decide what areas to review, the review's scope should include assurance on key information security areas, such as online privacy, confidentiality, security, and processing integrity.

Assurance reviews provide a way for organizations to help ensure that controls are in place to help protect their data. For example, in April 1992, the American Institute of Certified Public Accountants (AICPA) issued its Statement on Auditing Standards No. 70 (SAS 70). The SAS 70 provides guidelines for independent auditors to follow when reviewing the control activities of service providers. The SAS 70 is the authoritative guidance that allows organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. It signifies that an organization has had its control objectives and control activities examined by an independent auditing firm, and it provides guidance to enable an independent auditor to issue an opinion on an organization's description of controls. An example of an independent assurance review implemented by a business is Visa Corporation's Cardholder Information Security Program (CISP). The program defines a standard for securing Visa cardholder data by all entities storing, processing, or transmitting Visa cardholder data. Since IBM stores, processes, and transmits Visa cardholder data, it will likely be required to comply with CISP, and Visa's 12 security requirements could meet some of MVD's requirements. An IBM official said that IBM will probably be required to address CISP by March 31, 2005.

MVD should amend current agreement to ensure receipt of programmable source code—MVD should also work with IBM to amend their third-party agreement to ensure that if the agreement expires, the State receives ServiceArizona's programmable source code, which is the computer software in its original form as written by the programmer. According to an MVD official, both MVD and IBM agree that the current addendum means that MVD will receive the source code, and are willing to amend the addendum to clarify the issue. The current third-party agreement expires on December 31, 2005, although it will automatically renew for 2 years unless either party gives 30-day notice prior to the expiration date. If the parties elect to terminate the agreement, there is a provision that would transfer copies of those portions of the ServiceArizona applications software that IBM generally does not make available, but it does not specify the software's format. Further, the current agreement does not specifically state that IBM will transfer the software's programmable source code to MVD if the third-party agreement expires. If MVD received the ServiceArizona software as "object code" instead of "source code," its programmers would be unable to change the program, either to improve existing services or to add new services. Amending the current agreement to ensure that MVD receives programmable source code ensures that MVD's IT staff could modify the software to meet MVD's future needs.

Recommendations

1. Before renewing IBM's third-party agreement, MVD should renegotiate the agreement to require IBM to hire an independent third party to complete an assurance review of mutually agreed-upon audit issues. As part of this effort, MVD should ensure that the review includes assurance on key information security areas such as online privacy, confidentiality, security, and processing integrity.
2. MVD should amend its third-party agreement with IBM to ensure that the State receives ServiceArizona's programmable source code if the third-party agreement terminates in the future.

AGENCY RESPONSE

ADOT

Arizona Department of Transportation
Office of the Director
208 South Seventeenth Avenue Phoenix, Arizona 85007-3213

Janet Napolitano
Governor

Victor M. Mendez
Director

Debra Brisk
Deputy Director

September 24, 2004

Debbie Davenport
Auditor General
2910 North 44th Street
Phoenix, Arizona 85008

Dear Ms. Davenport:

The Arizona Department of Transportation extends its thanks to you and your staff for the professionalism displayed during the performance audit and Sunset review of the Arizona Department of Transportation, Motor Vehicle Division.

In response to the audit, the Department plans to implement the recommendations as follows:

Finding #1 ADOT should strengthen MVD's information system security controls

1. **Auditor General Recommendation**: To better manage access to systems and data, ADOT and MVD should collaborate to review the access of all user groups in order to ensure they are appropriately defined. In doing this, ADOT and MVD should document the rationale for access and authority level given to each user group. In addition, ADOT and MVD should ensure that users are placed in the appropriate user group. Access rights should also be reviewed on a periodic basis to ensure that they remain appropriate.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

   As part of an ongoing project to ensure the appropriateness of MVD user group transaction privileges, ADOT and MVD have already addressed the majority of user groups that have access to MVD's information systems. We plan to have the remaining accounts and user groups reviewed and any required adjustments made. We will also conduct periodic reviews to better ensure the appropriateness of MVD user group transaction privileges.

2. **Auditor General Recommendation**: To better manage access to systems and data, MVD should:

   a. Work more closely with other government agencies to ensure that user accounts are removed when an employee leaves employment or when the employee no longer needs the access.

Arizona Governor's Award for Quality

Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

MVD maintains contracts or agreements with these agencies to set the guidelines for securing MVD data. MVD will also add language to its agreements to require employee changes and terminations to be reported to MVD within an appropriate timeframe.

b. Periodically review the lists of third-party processors and other government employees to ensure they are up-to-date and accurate.

Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

3. **Auditor General Recommendation**: To better manage access to systems and data, ADOT should:

a. Alter the access request form to better enable the IT Group to know the access and authority level it needs to give an individual within a given system, perhaps by including position title on the access request form.

Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

Access request forms will be modified to include a position title or other information to ensure the assignment of appropriate access and authority levels.

b. Ensure that it receives and maintains documentation required to set up new user accounts, and that controls are in place to help ensure access is properly authorized.

Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

Rather than relying on paper forms, ADOT has developed a process by which access forms are accurately scanned, stored, and retrieved by a web application. This new process improves the confidentiality, integrity, and availability of user access documentation. The electronic forms are backed up on a scheduled basis. The agency plans to strengthen authorization controls through the introduction of business area security liaisons and is exploring options that employ automated authorization features.

c. Produce reports that indicate accounts without password intervals and appropriately restricting this privilege, as well as developing criteria for user accounts that are kept without password intervals or that are maintained in disuse.

Agency Response: The finding of the auditor general is agreed to, and the audit recommendation will be implemented.

These accounts are managed and maintained to satisfy valid business needs and do not increase the risk of unauthorized access because:

- Their access capabilities are limited to non-production resources.
- They cannot be used as a logon ID because no supporting RACF profile is defined.
- They cannot be used as a logon ID because no password is associated with the ID.

In addition to the current reports used to identify and eliminate user accounts, we will produce an individual report that lists accounts without password intervals. We plan to increase the frequency of our scheduled RACF USERID review activities and we will modify our existing RACF USERID management procedures to include the written criteria used to determine and maintain such accounts.

4. **Auditor General Recommendation**: MVD should better control the implementation of program changes by developing policies and procedures for ensuring that it maintains proper documentation for all program changes. In addition, MVD should implement controls to help ensure unauthorized changes are not made to the system.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

   The agency is in the process of developing policies and procedures to ensure that documentation is in place for all program changes.

5. **Auditor General Recommendation**: ADOT should develop an entity-wide security program. This program should address all aspects of security such as establishing a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

   ADOT's Information Technology Group (ITG) is developing an entity-wide security program to safeguard and protect IT resources and technology. As articulated in its strategic plan, ITG's Infrastructure Protection Unit is identifying and verifying critical physical and information assets, conducting a recurring vulnerability assessment against these assets, developing corrective plans to mitigate vulnerabilities, assuring that ADOT has response plans in place, educating agency personnel in the areas of physical and information security, reviewing and revising ADOT policies governing the management and protection of critical infrastructure assets, and supporting a long-term program to identify and close gaps resulting from the assessments referenced above.

   In addition, the program should:

a. Ensure that those accessing and securing its sensitive information meet generally accepted standards by requiring background checks of personnel on an initial and ongoing basis, consistent with the sensitivity of their positions.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

b. Ensure that all its employees as well as those of the third-party contractors undergo computer security awareness training at initial hire and on an ongoing basis.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

   All employees with computer access are mandated to attend computer security awareness training, and we will ensure that all employees are being sent to class as required. Existing training curriculum will be reviewed and evaluated to ensure it addresses the needs of the Division as well as its pertinence to third parties. If possible, changes will be incorporated in the computer security awareness-training curriculum so that third parties can be included.

6. **Auditor General Recommendation**: ADOT should implement the business continuity/ disaster recovery plan on schedule and regularly test the plan for adequacy.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

   ADOT participates in biannual mainframe hot-site disaster recovery tests. Additionally, the Department is currently recruiting for a Business Continuity Coordinator (BCC) and we anticipate this position will be filled by December 2004. The BCC, in conjunction with division representatives, will be responsible for conducting a business impact analysis and developing business continuity/disaster recovery strategies for senior leadership consideration. The current estimated target date for implementing an approved and funded client server disaster recovery capability, is February 2007. Once implemented, biannual disaster recovery tests will be conducted to ensure the functionality and reliability of ADOT's disaster recovery capabilities.

Finding #2 Growth in ServiceArizona makes better oversight more important

1. **Auditor General Recommendation:** Before renewing IBM's third-party agreement, MVD should renegotiate the agreement to require IBM to hire an independent third party to complete an assurance review of mutually agreed-upon audit issues. As part of this effort, MVD should ensure that the review includes assurance on key information security areas such as online privacy, confidentiality, security, and processing integrity.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

2. **Auditor General Recommendation:** MVD should amend its third-party agreement with IBM to ensure that the State receives ServiceArizona's programmable source code if the third-party agreement terminates in the future.

   Agency Response: The finding of the Auditor General is agreed to, and the audit recommendation will be implemented.

Sincerely,

Victor M. Mendez
Director

Performance Audit Division reports issued within the last 24 months

02-09	Arizona Health Care Cost Containment System—Sunset Factors
02-10	Department of Economic Security—Division of Children, Youth and Families, Child Protective Services
02-11	Department of Health Services—Health Start Program
02-12	HB2003 Children's Behavioral Health Services Monies
02-13	Department of Health Services—Office of Long Term Care
03-L1	Competitive Electric Metering, Meter Reading, and Billing and Collections
03-01	Government Information Technology Agency—State-wide Technology Contracting Issues
03-02	Registrar of Contractors
03-03	Water Infrastructure Finance Authority
03-04	State Board of Funeral Directors and Embalmers
03-05	Department of Economic Security—Child Protective Services—Foster Care Placement Stability and Foster Parent Communication
03-06	Arizona Board of Appraisal
03-07	Arizona Board for Charter Schools
03-08	Arizona Department of Commerce
03-09	Department of Economic Security—Division of Children, Youth and Families Child Protective Services—Caseloads and Training
04-L1	Letter Report—Arizona Board of Medical Examiners
04-L2	Letter Report—Gila County Transportation Excise Tax
04-01	Arizona Tourism and Sports Authority
04-02	Department of Economic Security—Welfare Programs
04-03	Behavioral Health Services' HB2003 Funding for Adults with Serious Mental Illness
04-04	Department of Emergency and Military Affairs and State Emergency Council
04-05	Department of Environmental Quality—Water Quality Division
04-06	Department of Environmental Quality—Waste Programs Division
04-07	Department of Environmental Quality—Air Quality Division
04-08	Department of Environmental Quality—Sunset Factors
04-09	Arizona Department of Transportation, Motor Vehicle Division—State Revenue Collection Functions

Future Performance Audit Division reports

Arizona Department of Transportation, Motor Vehicle Division—Sunset Factors