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.

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