STATE OF ARIZONA

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

OFFICE OF THE
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

December 21, 2006

The Honorable Laura Knaperek, Chair
Joint Legislative Audit Committee

The Honorable Robert Blendu, Vice Chair
Joint Legislative Audit Committee

Dear Representative Knaperek and Senator Blendu :

Our Office has recently completed a 24-month followup of the Arizona Department of Transportation—Motor Vehicle Division—Information Security and E-government Services regarding the implementation status of the 13 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in September 2004 (Auditor General Report No. 04-10). As the attached grid indicates:

- 12 have been implemented, and
- 1 is in the process of being implemented.

Unless otherwise directed by the Joint Legislative Audit Committee, this report concludes our follow-up work on the Department's efforts to implement the recommendations resulting from the September 2004 performance audit.

Sincerely,

Debbie Davenport
Auditor General

DD:lmn
Attachment

cc: Victor Mendez, Director
Arizona Department of Transportation

ARIZONA DEPARTMENT OF TRANSPORTATION
Motor Vehicle Division– Information Security and E-government Services
24-Month Follow-Up Report To
Auditor General Report No. 04-10

FINDING 1: ADOT should strengthen MVD's information system security controls

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
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.	**Implemented at 12 Months**	
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.	**Implemented at 6 Months**	
b. Periodically review the lists of third-party processors and other government employees to ensure that they are up-to-date and accurate.	**Implemented at 12 Months**	

ARIZONA DEPARTMENT OF TRANSPORTATION
Motor Vehicle Division– Information Security and E-government Services
24-Month Follow-Up Report To
Auditor General Report No. 04-10

FINDING 1: **ADOT should strengthen MVD's information system security controls (cont'd)**

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
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.	**Implemented at 12 Months**	
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.	**Implemented at 6 Months**	
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.	**Implemented at 6 Months**	

FINDING 1: ADOT should strengthen MVD's information system security controls (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
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.	**Implemented at 6 Months**	

ARIZONA DEPARTMENT OF TRANSPORTATION

Motor Vehicle Division– Information Security and E-government Services
24-Month Follow-Up Report To
Auditor General Report No. 04-10

FINDING 1: **ADOT should strengthen MVD's information system security controls (cont'd)**

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
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:	**Implemented at 6 Months**	
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.	**Implemented at 12 Months**	
b. Ensure that all of its employees as well as those of the third-party contractors undergo computer security awareness training at initial hire and on an ongoing basis.	**Implemented at 12 Months**	

ARIZONA DEPARTMENT OF TRANSPORTATION
Motor Vehicle Division– Information Security and E-government Services
24-Month Follow-Up Report To
Auditor General Report No. 04-10

FINDING 1: ADOT should strengthen MVD's information system security controls (concl'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
6. ADOT should implement the business continuity/disaster recovery plan on schedule and regularly test the plan for adequacy.	Implementation in Process	ADOT officials reported that ADOT has participated in biannual mainframe hot-site disaster recovery tests for over 2 years, with each test proving successful. During the audit, ADOT officials anticipated completing a business impact assessment by September 15, 2005, and implementing a recovery plan by February 2007. However, ADOT officials have since revised their estimated target date for implementing an approved and funded client server disaster recovery capability to April 2009.

ARIZONA DEPARTMENT OF TRANSPORTATION
Motor Vehicle Division– Information Security and E-government Services
24-Month Follow-Up Report To
Auditor General Report No. 04-10

FINDING 2: Growth in ServiceArizona makes better oversight more important

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
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.	**Implemented at 18 Months**	
2. MVD should amend its third-party agreement with IBM to ensure that the State receives Service Arizona's programmable source code if the third-party agreement terminates in the future.	**Implemented at 6 Months**	