STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

August 31, 2007

The Honorable Robert Blendu, Chair
Joint Legislative Audit Committee

The Honorable John Nelson, Vice Chair
Joint Legislative Audit Committee

Dear Senator Blendu and Representative Nelson:

Our Office has recently completed a 24-month followup of the Department of Economic Security—Information Security, regarding the implementation status of the 31 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in July 2005 (Auditor General Report No. 05-04). As the attached grid indicates:

- 29 have been implemented, and
- 2 are 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 July 2005 performance audit.

Sincerely,

Melanie M. Chesney, Director
Performance Audit Division

MMC:sjb
Attachment

cc: Tracy Wareing, Director
Department of Economic Security

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 1: Controls over data security need improvement

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
1. In order to address user account weaknesses, DES should:		
a. Create guidelines requiring periodic reviews of access rights to ensure that users have only the access that they need to perform their jobs.	**Implemented at 6 Months**	
b. Define who needs security administration privileges, and what kind of authority they need, so that these privileges can be restricted to the minimum levels required for employees to perform their duties.	**Implemented at 6 Months**	
c. DTS should monitor compliance with new and updated policies addressing account management and access control to ensure that old and unused accounts are properly deleted and account passwords are changed at least every 30 days.	**Implemented at 6 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 1: Controls over data security need improvement (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
2. The Information Security Administration should continue to conduct compliance reviews and assessments, develop a schedule of regular reviews, and establish policies and procedures to document its practices, including a follow-up process to ensure divisions comply with recommendations.	**Implemented at 6 Months**	
3. In order to increase compliance with security requirements, the Department should:		
a. Establish an internal IT audit function	**Implemented at 6 Months**	
b. Consider contracting for an independent security assessment.	**Implemented at 6 Months**[1]	

[1] DES included funding for this assessment in its budget requests for fiscal year 2007 and fiscal year 2008, but did not obtain the requested funds.

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 1: Controls over data security need improvement (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
4. In order to ensure that security representatives know their duties and are capable of doing them, DTS should work with security groups to:		
a. Adopt a job description with minimum qualifications for security representatives and ensure that only individuals who meet these qualifications are authorized to conduct these duties.	**Implemented at 6 Months**	
b. Develop a manual regarding the duties of a security representative as a reference source.	**Implemented at 6 Months**	
c. Ensure that security representatives understand their job duties and receive periodic training.	**Implemented at 6 Months**	
d. Identify other individuals who perform duties similar to security representatives; specifically, those who perform system application (non-mainframe) access right duties, and ensure that they understand their job duties and receive periodic training.	**Implemented at 6 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 1: Controls over data security need improvement (concl'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
5. The Department should ensure that new employees receive the mandatory computer security training.	**Implemented at 6 Months**	
6. The Department should determine which positions involve the security and access of sensitive information and therefore merit a background check. It should then request the authority, either through statute or an executive order, to conduct background checks and ensure background checks are conducted on those individuals. The Department should also conduct periodic background checks on long-term employees in accordance with the sensitivity of their position.	**Implemented at 18 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 2: Information in local area networks and computers not adequately protected

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
1. To ensure that all computers have up-to-date security patches installed, the Department should:		
a. Deploy as planned an automated tool that will allow it to centrally control and manage security updates.	Implementation in Process	The Department implemented an automated tool to centrally manage and control security updates for all of its desktop computers in April 2006. However, it has not implemented a tool that would allow it to patch servers automatically. The Department reported that it requested funding to acquire such a tool in its last two budget requests, but that it did not receive the funding in fiscal year 2007 because of statewide fiscal constraints, and that neither the Governor's nor the Legislature's fiscal year 2008 budget proposals included this item. The Department reported that it is reassessing the costs and will determine what other steps it can take to fully implement this recommendation.
b. Periodically monitor to ensure that all computers have critical security updates installed.	**Implemented at 12 Months**	
2. To better ensure computers are protected from viruses, the Department should:		
a. Develop a time frame by which all divisions must install the entity-wide virus protection software the Department has already purchased.	**Implemented at 6 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 2: Information in local area networks and computers not adequately protected (concl'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
b. Ensure that all computers have the virus protection installed.	**Implemented at 6 Months**	
c. Monitor to ensure that all department computers regularly receive current updates.	**Implemented at 12 Months**	
3. To better ensure computers are protected from spyware and other forms of malware, the Department should:		
a. Ensure that employees and local LAN support units understand the Department's acceptable use policy.	**Implemented at 12 Months**	
b. Monitor to ensure that its divisions and employees comply with the policy.	**Implemented at 12 Months**	
4. The Department should review the training practices of the local LAN support units and establish training requirements sufficient to ensure that LAN staff have and maintain adequate skill levels.	**Implemented at 12 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 3: Department could improve its management of computer program changes

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
1. DTS should standardize its program change process throughout programming teams by completing its current efforts to develop a documented system development methodology and program change policy and then applying the new practices to all project teams, to the extent possible.	**Implemented at 6 Months**	
2. DTS should improve its testing of program changes by:		
a. Continuing its efforts to implement an automated testing tool.	**Implemented at 6 Months**	
b. Ensuring that testers receive adequate training to use the new tool.	**Implemented at 6 Months**	
c. Using the tool as frequently as possible, in accordance with the nature of the program change.	**Implemented at 18 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 4: Department has made progress in disaster recovery

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
1. The Department needs to update and complete its disaster recovery planning software. Specifically, it needs to:		
a. Update all components of the plan—mainframe and server farm plans—as needed to include new disaster recovery initiatives including the emergency hot site, new network strategy, regular data backups, and testing procedures.	**Implemented at 6 Months**	
b. Add information to mainframe, network, and server farm plans so that they include detailed tasks and assignments for all recovery teams identified in those plans.	**Implemented at 6 Months**	
c. Add information to its mainframe, network, and server farm plans so that they include pertinent vendor information, such as vendor assets and supplies.	**Implemented at 6 Months**	
d. Add information to the mainframe plan to identify the most critical mainframe applications, and the priorities and sequence of events necessary to restore these applications.	**Implemented at 6 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 4: Department has made progress in disaster recovery (cont'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
e. Add information to its server farm plan to have a vendor provide backup resources for its server farm.	Implementation in Process	The Department developed a work plan to implement this recommendation, and anticipated completion by June 30, 2007. Full implementation required the issuance of a multi-agency Request for Proposal (RFP) for a disaster recovery server replacement. The Arizona Department of Administration published the multi-agency RFP that included the Department and four other state agencies on January 25, 2007. However, only one acceptable response was received when the RFP response period closed in March 2007. The Department and the other agencies determined the bid to be unacceptable because of both its high costs and the approach taken by the vendor, and the State Procurement Office subsequently canceled the RFP. The Department reported that it is working with the Government Information Technology Agency and the Governor's Office to discuss how to proceed, and that it plans to re-solicit these services later in 2007.
2. The Department should ensure it adds testing plan information to its recovery planning software as part of its ongoing plan maintenance.	**Implemented at 6 Months**	

DEPARTMENT OF ECONOMIC SECURITY—
INFORMATION SECURITY
24-Month Follow-Up Report To
Auditor General Report No. 05-04

FINDING 4: Department has made progress in disaster recovery (concl'd)

Recommendation	Status of Implementing Recommendation	Explanation for Recommendations That Have Not Been Implemented
3. The Department's Division of Technology Services should develop policies for critical system backups and add this information to its planning software.	**Implemented at 6 Months**	