STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

April 1, 2008

The Honorable John Nelson, Chair
Joint Legislative Audit Committee

The Honorable Robert Blendu, Vice Chair
Joint Legislative Audit Committee

Dear Representative Nelson and Senator Blendu:

Our Office has recently completed a 30-month followup of the Department of Administration—Information Services Division and Telecommunications Program Office regarding the implementation status of the 17 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in September 2005 (Auditor General Report No. 05-11). As the attached grid indicates:

- 12 have been implemented;
- 2 have been partially implemented
- 2 are in the process of being implemented; and
- 1 recommendation is no longer applicable.

Unless otherwise directed by the Joint Legislative Audit Committee, this concludes our follow-up work on the Department's efforts to implement the recommendations from the September 2005 performance audit report.

Sincerely,

Melanie M. Chesney
Performance Audit Director

MC:Sjb
Attachment

cc: Bill Bell, Director
Arizona Department of Administration

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

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security

Recommendation	Status of Implementing Recommendation	Additional Explanation
1. The Department should designate a central authority, such as its state-wide security manager, with the responsibility for developing a comprehensive security program for the Department's internal information resources and network, as well as the data center. The Department should then ensure that the program addresses:	**Implemented at 30 Months**	
a. Developing a policy governing network scanning, monitoring, and testing, including how it should be done, the frequency, and follow-up procedures to correct identified vulnerabilities;	**Implemented at 30 Months**	
b. Ensuring that it obtains an independent security assessment at least every 3 years and developing policies regarding the circumstances under which it would obtain an independent assessment more frequently.	**Implemented at 30 Months**	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (cont'd)

Recommendation	Status of Implementing Recommendation	Additional Explanation
c. Conducting risk assessments at least every 3 years and as needed when systems, facilities, or other conditions change;	**Implemented at 30 Months**	
d. Developing a system to follow up on identified risks and weaknesses to ensure that they are addressed;	**Implemented at 30 Months**	
e. Developing adequate security policies and procedures and ensuring that they include sufficient detail; and	Implementation in Process	The Department has established some security policies and standards and is in the process of drafting additional policies and standards.
f. Providing annual security awareness training as provided for in both GITA and department policy.	**Implemented at 30 Months**	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (cont'd)

Recommendation	Status of Implementing Recommendation	Additional Explanation
2. The Department should determine if it needs additional staff, funding, and technical resources to perform additional security duties, and if so, assess whether it could reassign existing staff and resources or take other steps, as appropriate, to seek additional staff and resources.	**Implemented at 30 Months**	
3. The Department should request that the Legislature amend A.R.S. §41-712 to give the Department statutory authority to enforce security requirements for state agencies using AZNET. If the Department receives such authority, it should ensure that it becomes part of its comprehensive security program in conjunction with the first recommendation.	No Longer Applicable	Since this audit report was issued, the Legislature added A.R.S. §41-3507 which established the Government Information Technology Agency's Statewide Information Security and Privacy Office and directs this Office to develop, implement, maintain, and ensure that state agencies comply with a coordinated state-wide assurance plan for information security and privacy.

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (cont'd)

Recommendation	Status of Implementing Recommendation	Additional Explanation
4. The Department should enhance its interagency service agreements with state agencies that use the data center to define the Department's and the agencies' security responsibilities. The agreements should:		
a. Delineate the Department's responsibility to provide access to the state data center and the state agency's responsibility to meet specific, minimum security requirements; and	**Implemented at 30 Months**	
b. Define the circumstances under which a state agency may face actions for failure to comply with those security requirements, and the actions the Department can take to better ensure that corrupted systems in one agency do not compromise other agencies' systems and data.	Partially Implemented	Although the Department's interagency service agreements require state agencies to follow all network security guidelines as established by the Department and stipulate that the Department can terminate compromised agency servers, the service agreements do not detail what security criteria will be used, how compliance will be evaluated, and do not provide for the escalation and enforcement of security problems.

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 1: Several actions needed to improve information security (concl'd)

Recommendation	Status of Implementing Recommendation	Additional Explanation
5. The Information Services Division should better ensure that it does not publish sensitive information on its Web site by developing a policy requiring central review and approval of Web site content. The Division should also review current Web content to ensure that sensitive information has not remained on its Web site, and instead maintain any sensitive information in a more secure environment, such as the Department's internal network, which is not available to the public.	**Implemented at 30 Months**	
6. The Department should configure its information system resources, such as routers, switches, and servers, to comply with GITA standards to provide greater safety from external threats.	Implementation in Process	The Department has taken steps to comply with GITA standards and reported that it plans to fully implement this recommendation by December 31, 2008.

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 2: Improved oversight of telecommunications consolidation and privatized network needed

Recommendation	Status of Implementing Recommendation	Additional Explanation
1. The Department should improve oversight of the inventory process by:	**Implemented at 30 Months**	
a. Reviewing the TPO's current staffing assignments and reassigning staff to this function or, if necessary,		
b. Reallocating existing resources or taking other steps, as appropriate, to hire a private contractor to adequately oversee the inventory process.		
2. The Department should ensure that the contractor develops an adequate network security plan that includes the following:		
a. Requirements stipulated by the contract, including security service level agreements, compliance with GITA's state-wide security standards, and periodic security awareness and training for agency personnel; and	**Implemented at 30 Months**	

DEPARTMENT OF ADMINISTRATION
INFORMATION SERVICES DIVISION AND
TELECOMMUNICATIONS PROGRAM OFFICE
30-Month Follow-Up Report To
Auditor General Report No. 05-11

FINDING 2: Improved oversight of telecommunications consolidation and privatized network needed (concl'd)

Recommendation	Status of Implementing Recommendation	Additional Explanation
b. Other relevant aspects of an appropriate information technology security plan, such as defining clear security monitoring and enforcement processes, and how potential security breaches or other incidents will be identified, reported, and monitored.	**Implemented at 30 Months**	
3. The Department should develop a process for monitoring the contractors and work with them to annually update the security plan to reflect any changes in state-wide network and security standards.	Partially Implemented	Although the Department has implemented some processes for monitoring contractors, such as regularly holding meetings with contractors to discuss monitoring issues, it has not documented processes for monitoring contractors and annually updating the network security plan to reflect any changes in the network and security standards.