Janet Napolitano
Governor

Jerry A. Oliver, Sr.
Interim Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

100 North 15th Avenue • ROOM 401
PHOENIX, ARIZONA 85007

(602) 542-1500

September 21, 2005

Debbie Davenport
Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Dear Ms. Davenport:

The Department of Administration appreciates the efforts of the Auditor General's Office and professionalism in conducting the sunset audit for the Information Systems Division and newly created Telecommunications Program. These are dynamic areas where the department attempts to use technology for the betterment of state government. We as a department understand there is always room for improvement in any of our business activities. The Department appreciates the patience and discipline of the Auditor General's office during this audit, especially when the Department is in the midst of the major transformation taking place in the outsourcing of telecommunications for all state government.

The Department appreciates the importance of security in today's current technology environments, and to that end, has established a robust framework with the AzNet program to address network security through the outsourced contract that will effectively raise the security posture for all state government. We are keen to pursue the ideas suggested for legislative action to better serve state agencies. We also realize that AZNET security, in particular, needs to be a funded activity within ISD so there is a division of responsibilities between ISD and TPO/AZNET.

Sincerely,

Jerry A. Oliver
Interim Director

Enclosure

ADOA Agency Response, by Section and Finding

Auditor General Recommendations - ISD

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:*

    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;*

Agency Response:

The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented. While we agree with the recommendation to establish the policies, the Department is concerned there may not be sufficient funding for implementing those policies. As with b. and c. below, this is often beyond what our customers expect and can pay for, which by default, will cause conflicts with our customers.

b. *Ensuring that it obtains an independent security assessment at least every 3 years and developing policies regarding under what circumstances it would obtain an independent assessment more frequently;*

Agency Response:

The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented. While we agree with the recommendation to follow best practices, the Department is concerned there may not be sufficient funding for independent security assessments at that frequency.

c. *Conducting risk assessments at least every 3 years and as needed when systems, facilities, or other conditions change;*

Agency Response:

The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented. While we agree with the recommendation to follow best practices, the Department is concerned there may not be sufficient funding for risk assessments at that frequency.

d. *Developing a system to follow up on identified risks and weaknesses to ensure that they are addressed;*

Agency Response:

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

e. *Developing adequate security policies and procedures and ensuring that they include sufficient detail; and*

Agency Response:

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

f. *Providing annual security awareness training as provided for in both GITA and department policy.*

Agency Response:

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

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.*

Agency Response:

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

3. *The Department should request that the Legislature amend A.R.S. §41 -712 to give the Department statutory authority to enforce security requirements on state agencies using AZNE. If the Department receives such authority, it should ensure that it becomes part of its comprehensive security program in conjunction with the first recommendation.*

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. While we agree with the intent of the recommendation, the Department is concerned there will exist a conflict in statutory authority between 41-172 and the existing authority of GITA for statewide security, including the extent of the recommendation to GITA to create a Chief Security Officer role for state government. The Department will work with GITA to determine the best approach to address the gap in current statutes to enforce enterprise architecture security standards for AzNet, while ensuring conflicts are not created with the statutory authority being sought.

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*

Agency Response:

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

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 computers in one agency do not compromise other agencies' systems and data.*

Agency Response:

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

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 that is not available to the public.*

Agency Response:

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

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.*

Agency Response:

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

<u>Auditor General Recommendations - TPO</u>

1. *The Department should improve oversight over the inventory process by:*

    a. *Reviewing the TPO's current staffing assignments and reassigning staff to this function or, if necessary,*

Agency Response:

The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented. The FY06 budget request included technical staff that were not in the final appropriation. The TPO will look to other agency resources on an ad hoc basis.

    b. *Reallocating existing resources or taking other steps, as appropriate, to hire a private contractor to adequately oversee the inventory process.*

Agency Response:

The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented. The FY06 budget request included technical staff that were not in the final appropriation. The Department will implement a detailed process including resources of the AzNet team, the TPO and the other Agencies during the transition of an Agency onto the AzNet contract.

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*

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. This finding may require legislation (as identified in finding recommendation #3) to enforce security requirements on state agencies using AZNET.

    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.*

Agency Response:

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

3. *The Department should develop a process for monitoring the contractor and work with them to annually update the security plan to reflect any changes in state-wide network and security standards.*

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented