ARIZONA DEPARTMENT OF ECONOMIC SECURITY
1717 W. Jefferson • P.O. Box 6123 • Phoenix, AZ 85005

Janet Napolitano
Governor

David A. Berns
Director

Ms. Debbie Davenport
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Dear Ms. Davenport:

Thank you for the opportunity to respond to the performance audit and sunset review of information security in the Department of Economic Security. We appreciate the professional approach the auditors took during the course of this review. The purpose of this letter is to forward the Department's written responses to the preliminary draft report.

As you are aware, in 2003, the current DES leadership had identified information security as a potentially vulnerable area and had implemented various improvements. We welcomed the Auditor General's review as a means to enhance and refine those efforts.

The Department agrees with the findings in the report and has identified and initiated work to implement most of the recommendations by January 2006. Five (5) recommendations that require organizational development and training will be implemented by July 2006. The remaining three (3) actions would require appropriated funding or specific authorization to implement. The Department will continue to review those three recommendations and determine the appropriateness of seeking additional funding.

Sincerely,

David A. Berns

Enclosure

DES Response - Information Security Performance Audit Draft Report

FINDING 1 - Controls over data security insufficient

Recommendation

1. In order to address user account weaknesses, DTS 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.
    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.
    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.

DES Response

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

    In November 2003, the Department recognized that its security controls required improvement and began to strengthen the role of this function with a realignment of the Information Security Administration (ISA) within the Division of Technology Services (DTS). This move included the hiring of a new Administrator in July 2004, who is responsible for ensuring that DES is in compliance with acceptable security industry practices. The first step in this process has been to strengthen DTS' central oversight and establish uniform standards and practices. ISA has already accomplished significant improvement toward this end through review and strengthening of existing, and establishment of new, security policies and procedures. Additional improvements, as recommended by the Auditor General, will also be implemented.

    a. Review of user access will be implemented as a part of ISA's Compliance Review Plan. By August 2005, ISA will complete the access control section of the Compliance Review Plan and will commence quarterly random reviews of user access at that time. These reviews will be done in coordination with the Division/Program Security Representatives. Any inappropriate access discovered will be addressed.
    b. In March 2005, DTS completed a review of accounts with security privileges. Unnecessary accounts were changed or deleted as a result of this review. A draft policy, based on industry standards and the concept of "least privilege", has been completed and is currently under review. This policy specifies the requirements for obtaining security privileges and what restrictions apply. Adoption of this policy will occur in August 2005. The account management

section of the Compliance Review Plan, which incorporates review of security privileges, will be completed, and ISA will commence quarterly random reviews of security privileges in August 2005.

c. In March 2005, new policies governing account management and access control were adopted. These policies established rules for reviewing user accounts, including old/unused accounts, accounts with password intervals, and duplicate accounts for an individual. In May 2005, ISA began enforcement of these new policies through monthly reviews and appropriate follow-up actions with the security administrators. By July 2005, ISA will begin publishing a periodic report that describes the results of compliance monitoring and follow-up regarding old and unused accounts.

Recommendation:

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.

DES Response:

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

   The ISA will continue to conduct periodic compliance reviews to ensure divisions are complying with security policies and procedures. In doing so, ISA will develop a schedule of these reviews and establish policies and procedures on the review process. The Compliance Review Plan, which will address the review schedule and documentation requirements, as well as all security risks not mentioned above, will be completed by October 2005.

Recommendation:

3. In order to increase compliance with security requirements, the Department should:

   a. Establish an internal IT audit function.
   b. Consider contracting for an independent security assessment.

DES Response:

3. The finding of the Auditor General is agreed to and the audit recommendation will be implemented.
   a. In the past, DES had an IT audit function; however, due to budget constraints, the function was eliminated in 1997. The Department is using savings achieved through internal efficiencies to re-establish an IT audit position that will report to the Office of Audit and Management Services. The position will be filled by early 2006.

b. As the Audit Report indicates, an external IT security assessment is estimated to cost several hundred thousand dollars, based on the experiences of the Department of Transportation and the Department of Administration. The Department recognizes the value of such an assessment, but would require additional funding appropriated for that purpose.

Recommendation:

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.
   b. Develop a manual regarding the duties of a security representative as a reference source.
   c. Ensure that security representatives understand their job duties and receive periodic training.
   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.

DES Response:

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

a. In June 2005, DTS completed a draft job description that includes minimum qualifications and job duty descriptions for security representatives. These job descriptions apply to all persons who perform these duties, regardless of what job title they are in. Only staff who meet these qualifications will be given the necessary clearance to perform the security analyst functions. The Department will work with the Office of Personnel Management to adopt this job description by December 2005 and to resolve any unexpected personnel issues that may arise as a result of the implementation of these minimum qualifications.
b. By December 2005, DTS, in conjunction with the Department's security representatives, will develop and implement a manual that defines the duties of a security representative .
c. Upon completion of the revised Data Security Analyst Manual, the Department's Office of Management Development (OMD) will work with DTS to develop and deliver periodic mandatory training to the security representatives to ensure they understand the security representative job duties and expectations. Training will begin in 2006.

d. Staff who perform non-mainframe security duties will be included as the Department implements the security representative roles and responsibilities. They will also be included in the aforementioned security representative trainings. These staff will also have clear job duty descriptions and expectations.

Recommendation:

5. The Department should ensure that new employees receive the mandatory computer security training.

DES Response:

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

   By October 2005, all current Department employees will have received the mandatory computer security training. DES is partnering with Arizona Government University to ensure that all training data is tracked. In addition, ISA and OMD are developing a plan to ensure that all new employees receive appropriate mandatory computer security training (DES Basic Security Awareness Training course). This new employee training plan also will be implemented by October 2005.

Recommendation:

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.

DES Response:

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

   The Department will seek an Executive Order or legislation to require background checks on all current and newly hired employees that are responsible for security duties or have access to sensitive agency-maintained information.

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

Recommendation:

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.
b. Periodically monitor to ensure that all computers have critical security updates installed.

DES Response:

1. The finding of the Auditor General is agreed to and the audit recommendation will be implemented.
   a. In April 2005, DTS identified an automated tool to centrally control and manage security updates. DTS procured the automated tool in June 2005 and will implement it by January 2006.
   b. ISA will include periodic monitoring of the automated tool in the development of its Compliance Review Plan, which will be completed by October 2005.

Recommendation:

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.
   b. Ensure that all computers have the virus protection installed.
   c. Monitor to ensure that all department computers regularly receive current updates.

DES Response:

2. The finding of the Auditor General is agreed to and the audit recommendation will be implemented.
   a. The Department established December 2005, as the date for all Divisions to have installed the entity-wide virus protection software.
   b. DTS will review Division actions in early 2006 to ensure that all Divisions have installed virus protection software.
   c. ISA will include periodic monitoring of the existence and regular updating of virus protection software on desktop equipment in the development of its Compliance Review Plan, which will be completed by October 2005.

Recommendation:

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.
   b. Monitor to ensure that its divisions and employees comply with the policy

DES Response:

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

implemented.

a. The department requires all new employees to pass the Basic Security Awareness Training course and also requires all employees (including LAN support staff) to take a Security Awareness Refresher Course annually. Both courses include information on the acceptable use policy, employees' responsibilities under this policy, and the potential consequences for violations of the policy, which include personnel actions up to and including termination. The LAN support staff will receive not only the above training but also additional training on the application of this policy as part of the minimum required training for LAN support staff that will be established by March 2006. See the Department's response to Finding 2, Recommendation 4.
b. ISA will include periodic monitoring of user compliance with this policy in the development of its Compliance Review Plan, which will be completed by October 2005.

Recommendation:

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.

DES Response:

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

   The Department will:

   - By early 2006, establish and fill an internal IT audit function within the DES Office of Audit and Management Services. (See the Department's response to Finding 1, recommendation 3.a.) This audit function will be charged with, among other things, reviewing the training practices of local LAN support units and recommending training requirements sufficient to ensure that LAN staff have and maintain adequate skill levels.
   - By March 2006, establish minimum initial and ongoing training requirements for all LAN support staff, based on input from the DES internal IT auditor, IT and Information Security personnel, and staff of OMD.
   - By March 2006, require the re-established IT audit function to monitor for adherence to the new Department IT Standard for LAN training requirements as part of its IT audit work plan.

FINDING 3 – The Department could improve its management of computer program changes

DES Response - Information Security Performance Audit Draft Report

Recommendation:

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.

DES Response:

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

   By December 2005, DTS will complete the development and implementation of the system development methodology and will apply the new practices to all project teams, to the extent appropriate.

Recommendation:

2. DTS should improve its testing of program changes by:
   a. Continuing its efforts to implement an automated testing tool.
   b. Ensuring that testers receive adequate training to use the new tool.
   c. Using the tool as frequently as possible, in accordance with the nature of the program change.

DES Response:

2. The finding of the Auditor General is agreed to and the audit recommendation will be implemented.
   a. In May 2005, DTS acquired a suite of automated testing tools. This software will be installed in July 2005 and will be used for testing new and modified programs on mainframe, internet, and server-based platforms.
   b. By July 2005, 25 Department staff will have attended a five-day, vendor-provided training. The training will cover all aspects of the five different tools that are part of the suite. The 25 trainees include many program staff as well as the entire DTS Quality Assurance staff.
   c. Beginning in July 2005, following completion of the vendor training, program staff will begin use of the suite of tools to develop and execute test scripts to evaluate program changes and to track results.

FINDING 4 - Department has made progress in disaster recovery planning

Recommendation:

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, network, 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.
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.
c. Add information to its mainframe, network, and server farm plans so that they include pertinent vendor information, such as vendor assets and supplies.
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.
e. Add information to its server farm plan to have a vendor provide backup resources for its server farm.

DES Response:

1. The finding of the Auditor General is agreed to and the audit recommendation will be implemented.
   a. As new disaster recovery initiatives are implemented by the Department, the disaster recovery plans will be adjusted to include the updated recovery information. For example, in June 2005 DTS initiated daily off-site back-up tape storage, use of the IBM hot site for testing purposes, and the first phase of the DES Disaster Recovery (DR) test plan. The DES DR Plan, including the mainframe, network, and server farm components, will be updated to reflect these changes by September 2005.
   b. In May 2005, the Department implemented a maintenance plan, which is designed to ensure that all recovery plan owners review and update the plans on a regular basis. The Disaster Recovery Manager is responsible for monitoring the compliance with the maintenance plan. By December 2005, all three DR plans will have been updated with detailed tasks and assignments for the recovery teams identified in those plans.
   c. The maintenance plan adopted in May 2005 also requires that all vendor data be reviewed by recovery plan owners per the maintenance plan review schedule. In plans that have no vendor dependence for supplies or information, an annotation of “Not Applicable” will be added by the appropriate plan owners at the next scheduled review. By December 2005, all three DR plans will have been updated with vendor information, such as vendor assets and supplies.
   d. The Disaster Recovery Manager will work with other key staff throughout the Department to identify the most critical applications and prioritize their recovery in the event of a disaster. By January 2006, the resulting information will be added to the mainframe recovery plan.
   e. The Department’s disaster recovery appropriation was reduced for fiscal year 2006, which was established to address mainframe recovery services and faster

tape drives for performing backups. There were no appropriated funds earmarked for server farm backup resources. As a result, the Department will be requesting additional funds this summer in the fiscal year 2007 budget to fully address the mainframe and server farm backup resources. In the meantime, the Department will update its server farm plan to note that vendor-provided backup resources will be needed.

Recommendation:

2. The Department should ensure it adds testing plan information to its recovery planning software as part of its ongoing plan maintenance.

DES Response:

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

   The Disaster Recovery Manager is responsible for ensuring that test plan information is added to its recovery planning software as part of the Department's ongoing plan maintenance. The Department created its initial test protocol in May 2005 and executed that protocol in June 2005. The next test under the current contract is scheduled for August 2005. The test plan will be updated within the recovery planning software at that time.

Recommendation:

3. The Department's Division of Technology Services should develop policies for critical system backups and add this information to its planning software.

DES Response:

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

   In June 2005, the Division of Technology Services implemented a process to create daily incremental backups of critical mainframe systems. Those tapes are created and sent off site on a nightly basis. By October 2005, the documentation of that process will be included in the Department's disaster recovery planning software.