A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit

Department of Economic Security—

Information Security

JULY • 2005
REPORT NO. 05 – 04

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Robert Blendu,** Chair

Senator **Carolyn Allen**
Senator **Gabrielle Giffords**
Senator **John Huppenthal**
Senator **Harry Mitchell**
Senator **Ken Bennett** *(ex-officio)*

Representative **Laura Knaperek,** Vice Chair

Representative **Tom Boone**
Representative **Ted Downing**
Representative **Pete Rios**
Representative **Steve Yarbrough**
Representative **Jim Weiers** *(ex-officio)*

Audit Staff

Melanie Chesney, Director

Shan Hays, Manager and Contact Person
Monique Cordova, Team Leader
Aaron Cook
Pam Eck

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:
www.auditorgen.state.az.us

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

July 12, 2005

Members of the Arizona Legislature

The Honorable Janet Napolitano, Governor

Mr. David Berns, Director
Department of Economic Security

Transmitted herewith is a report of the Auditor General, A Performance Audit of the Department of Economic Security—Information Security. This report is in response to a November 20, 2002, resolution of the Joint Legislative Audit Committee. The performance audit was conducted as part of the sunset review process prescribed in Arizona Revised Statutes §41-2951 et seq. I am also transmitting with this report a copy of the Report Highlights for this audit to provide a quick summary for your convenience.

As outlined in its response, the Department of Economic Security agrees with all of the findings and plans to implement all of the recommendations.

My staff and I will be pleased to discuss or clarify items in the report.

This report will be released to the public on July 13, 2005.

Sincerely,

Debbie Davenport
Auditor General

Enclosure

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

PROGRAM FACT SHEET

Arizona Department of Economic Security
Division of Technology Services

Services:

The Division of Technology Services (DTS) provides technical and systems services for the development, maintenance, enhancement, and operation of the Department's automated business systems. The Division's responsibilities also include technical support for network and user information technology (IT) equipment and software; information security management; disaster recovery; customer support for IT and telecommunications equipment; IT help desk support for end users and field technical staff; and IT planning support for the Department.

DTS is part of the Department's central administration function, and does not carry out all IT-related activities within the Department. For example, the Department has 22 separate groups that support local area networks and computers with 72 network specialists, and 23 information security groups with 67 security representatives.

Facilities:

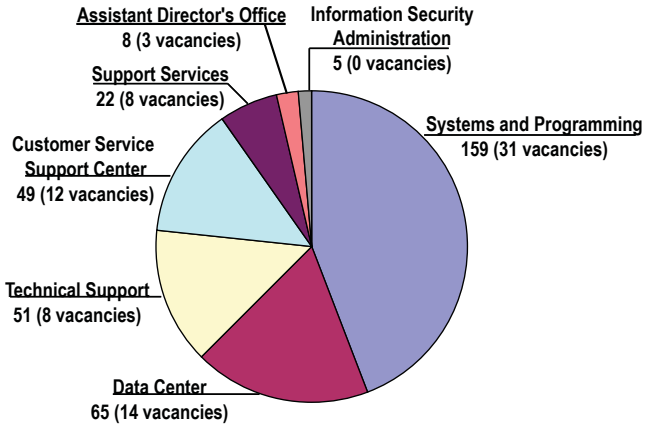
DTS' main administrative office and another facility are located in two state-owned buildings in Phoenix. In addition, DTS leases space in four other buildings in Phoenix, Tucson, and Flagstaff for an annual lease cost of $603,257.

Equipment:

In addition to office furniture, DTS has specialized equipment for which it has department-wide responsibility, such as the Department's mainframe computer. In addition, DTS reports that it has approximately 280 servers, which are computers that manage functions such as the Department's electronic mail system, its e-Government environment, and other critical agency functions.

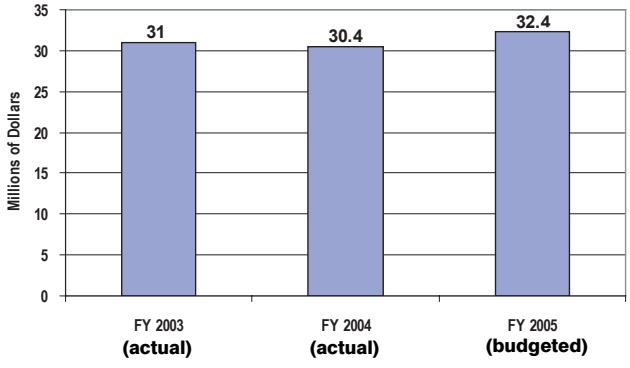
Program staffing:

359 FTE, including 76 vacancies (as of March 24, 2005)



Program revenue:

$32.4 million (fiscal year 2005 budgeted)



Mission:

The mission of DTS is to deliver efficient, effective business technology services for the Department's customers and employees, in partnership with the Department's programs.

Program goals:

1. To increase protection for the Department's information and individual privacy by enhancing information technology security measures.
2. To improve public service by enhancing IT systems and expanding electronic access.
3. To increase operational efficiencies by implementing innovative IT solutions.
4. To improve service quality by providing expanded communication, skill development, and career opportunities, and tools to optimize employee performance.

Adequacy of performance measures

DTS has developed 20 performance measures to support its 4 goals, including 9 output measures, 9 outcome measures, 1 quality measure, and 1 efficiency measure. While these measures generally were aligned with its 4 goals, auditors identified some areas where DTS could clarify how it uses measures to provide information. Specifically, DTS should consider reporting a combination of measures for all of its goals. For example, all 4 measures associated with DTS' second goal are identified as output measures. In addition, DTS has not identified any input measures.

Source: Auditor General staff compilation of unaudited information obtained from the State of Arizona Master List of Government Programs; the Division's strategic plan; staffing information from the Division's human resources manager; lease information from the Division of Business and Finance; equipment inventory, and other information provided by the Department and the Division of Technology Services.

SUMMARY

The Office of the Auditor General has conducted a performance audit of the Arizona Department of Economic Security's information security pursuant to a November 20, 2002, resolution of the Joint Legislative Audit Committee. The audit was conducted as part of the sunset review process prescribed in Arizona Revised Statutes (A.R.S.) §41-2951 et seq and is the third in a series of six reports on the Department of Economic Security (Department). This audit addresses four major aspects of the Department's controls over computer-based information:

- Controls over access by employees and others who use the data
- Protection of computers and local area networks (LANs) against virus attacks and other intrusions or data losses
- Procedures for making changes to computer programs
- Contingency planning for restoring service in the event of a major system failure

The first report reviewed the Department's welfare programs (Auditor General Report No. 04-02) and the second its unemployment insurance program (Auditor General Report No. 05-01). Subsequent reports will examine the Department's service integration initiative, the Division of Developmental Disabilities, and the Department's performance in light of the sunset factors contained in Arizona statutes.

The security of the Department's information systems is important because of the sensitive nature of its data. Department systems assist employees in important tasks such as tracking child welfare cases, monitoring information on developmentally disabled clients in state care, determining clients' eligibility to receive welfare benefits, and processing claimants' applications for unemployment insurance. Nearly 14,100 user accounts access various parts of department systems. About 11,730 accounts are for internal department use. In addition, more than 2,350 users, including local, state, tribal, federal, and private agencies, access the Department's systems. The Department reports that it has more than 80 different information systems, and manages a substantial amount of money through its systems. For instance, in fiscal year 2004, the Department used its systems to process $175 million in Temporary Assistance for Needy Families (TANF) cash benefits, and approximately $395 million in unemployment claims.

Controls over data security need improvement (see pages 9 through 15)

The Department needs to establish better access controls over its information systems and strengthen central oversight of data security. Access controls and other aspects of the security environment need to be strengthened throughout the Department. For example, auditors found that access rights were not periodically reviewed, old/unused accounts were not deleted in a timely fashion, and the use of special privileges that allowed individuals to create and delete user accounts was not adequately restricted.

The Department has not provided sufficient central oversight of the security environment. Unlike some state agencies, the Department has not established minimum qualifications and duties for personnel involved in security administration and it has provided neither a manual nor adequate training to ensure that security personnel understand their functions. In addition, new department employees do not always take a mandatory computer security training course, and the Department lacks the legal authority, from either an executive order or statute, to request background checks for personnel in sensitive information technology positions. The Department has begun to address some entity-wide security concerns through its Information Security Administration, located in the Division of Technology Services (DTS). For example, in March 2005, it adopted new policies governing account management. This administration also recently began conducting security compliance reviews within the Department, but needs to develop a regular schedule for such reviews and better document its processes.

Information in local area networks and computers not adequately protected (see pages 17 through 22)

The Department needs to improve management of its local area networks (LANs) and computers to better ensure system security and operability. Good management of LANs and computers provides protection against virus attacks, hacker intrusion, and possible loss of data. However, the Department does not provide sufficient protection in three areas:

- Security patches—Every operating system has vulnerabilites that hackers can potentially exploit to attack a system. Security patches are designed to correct for identified security weaknesses, and need to be installed on computers in order to protect them from attacks. However, in general, the Department does not install these patches in a timely manner and exposes its information systems to an increased risk of inoperability or compromise.

- Virus protection software—Since 2002, the Department has annually purchased a product that, when installed, allows it to centrally ensure that all computers have updated virus protection. However, not all divisions have installed this software on all their machines.

- Software downloaded from the Internet—The Department's acceptable use policy regarding downloading software from the Internet prohibits employees from downloading any software not specifically authorized by their local IT unit. However, auditors found instances of computers with inappropriate software downloaded from the Internet. Such software potentially installs malicious programs onto department computers that could slow or lock up a computer or make it easier for hackers to attack its systems.

In order to resolve these problems, the Department needs to deploy as planned a software package that will allow it to centrally manage security updates, set a time frame by which all divisions should install its entity-wide virus protection software, ensure its employees and local LAN support units understand its acceptable use policy, and monitor to ensure its divisions and employees comply with its policy.

Department could improve its management of computer program changes (see pages 23 through 25)

The Department could better manage its process for making changes to computer programs. Effective controls over the change process help ensure that computer program modifications are implemented only if they are properly requested, designed, tested, and approved. Failure to adequately control the program change process could lead to programs with errors or program changes that are inadequate and require additional resources to implement. For instance, in an audit released in January 2005, auditors identified computer errors in the Department's Unemployment Insurance Program that potentially have subjected Arizona employers to fines and assessments by reporting inaccurate information to the U.S. Internal Revenue Service. Due to an apparent lapse in adequate testing, programmers were unable to fix this problem during the course of the previous audit.

The Department should standardize the program change process throughout its programming teams. Auditors found that the program change process varied considerably among the 20 programming teams. The lack of a uniform, standardized process increases the risk of inappropriate or inadequate changes being introduced into a system. In addition, programming teams were unable to provide testing documentation. DTS is making efforts to address both of these weaknesses. DTS is developing a documented program change management policy and plans to apply this policy to all programming teams. In addition, DTS acquired an automated testing tool that will allow it conduct well-documented and extensive testing of program changes, which it plans to implement in July 2005.

Department has made progress in disaster recovery (see pages 27 through 31)

Although the Department has not completed a disaster recovery plan for its computer systems, it has begun to take steps to implement this goal and to join in a state-wide agency planning effort. Disaster recovery planning allows critical services to continue in the event of damage to an entity's computer systems. In 2002, the Department purchased a computer software planning system for disaster recovery, but due to staff vacancies made little progress in completing the required information.

Beginning in calendar year 2004, the agency has increased its disaster recovery efforts. For example, it began regular off-site remote backups of data and hired a disaster recovery manager. Further, along with other state agencies, it obtained one-year funding in fiscal year 2005 for emergency computer facility ("hot site") services and purchased hardware to allow for faster backups of its data. The Legislature approved additional funding for fiscal year 2006, although it reduced the Department's appropriation from the previous fiscal year.[1] The Department also has begun plans to redirect its computer network to the hot site in the event of an emergency, and has started daily backups of critical system data. Finally, in addition to its own efforts, the Department is meeting with other state agencies to discuss planning for state-wide disaster recovery solutions. However, the Department needs to finish documenting its disaster recovery plan.

1 JLBC's recommendation stated that the reduced appropriation for fiscal year 2006, which was made from the Risk Management Fund, could generate federal matching fund monies. However, because the Fund includes federal monies, the Department is working with the State Comptroller's Office to determine whether and how this can be done while complying with restrictions on federal monies.

TABLE OF CONTENTS

• continued

TABLE OF CONTENTS

concluded •

INTRODUCTION & BACKGROUND

The Office of the Auditor General has conducted a performance audit of the Arizona Department of Economic Security's information security pursuant to a November 20, 2002, resolution of the Joint Legislative Audit Committee. This audit addresses four major aspects of the Department's controls over computer-based information:

- Controls over access by employees and others who use the data
- Protection of computers and local area networks (LANs) against virus attacks and other intrusions or data losses
- Procedures for making changes to computer programs
- Contingency planning for restoring service in the event of a major system failure

The audit was conducted as part of the sunset review process prescribed in Arizona Revised Statutes (A.R.S.) §41-2951 et seq and is the third in a series of six reports on the Department of Economic Security (Department). The first report reviewed the Department's welfare programs (Auditor General Report No. 04-02) and the second its unemployment insurance program (Auditor General Report No. 05-01). Subsequent reports will examine the Department's service integration initiative, the Division of Developmental Disabilities, and the Department's performance in light of the sunset factors contained in Arizona statutes.

Sensitive client and benefits data increases importance of security

Because the Department uses its information systems to maintain sensitive client data and process benefits, the security of these systems is critical. The Department reports that it has more than 80 different information systems, and estimates that it serves more than one million children, adults, and families each month, and it uses its computers to perform a range of functions involving client data. For example, computer systems assist the Department in tracking child welfare cases, monitoring

provider information and bill payments information for people with developmental disabilities, and determining eligibility for potential Temporary Assistance for Needy Families (TANF) clients. The Department's systems also assist in processing client benefits, such as TANF cash benefits and unemployment insurance. In fiscal year 2004, the Department used its systems to process $175 million for TANF cash benefits and approximately $395 million in unemployment claims.

Thousands of employees of various agencies use the Department's systems. In all, there are nearly 14,100 user accounts giving access to the system. Approximately 11,730 accounts are for internal department use. In addition, more than 2,350 users, including local, state, tribal, federal, and private agencies, access the Department's systems. For example, other government agencies and private providers access the Department's systems to determine eligibility for programs such as employment assistance or housing and to coordinate service delivery for people with developmental disabilities.

Information technology management

The Department manages its information technology (IT) systems through a combination of centralized and decentralized management approaches. DTS manages some aspects of the Department's systems centrally, while other divisions manage other aspects for their own systems.

- IT Functions—Division of Technology Services (DTS): DTS staff manage several department-wide information technology functions. For example, DTS operates and maintains the Department's mainframe computer and network, and its staff perform programming changes required for the Department's systems. DTS also has responsibility for disaster recovery planning for the Department's mainframe and central server farm in the event of damage or destruction to its Data Center. Additionally, DTS is responsible for developing policies and procedures for the entire agency and for ensuring that the Department complies with state-wide policies established by the State of Arizona's Government Information Technology Agency (GITA), as well as any federal requirements.

- IT Functions—Other Divisions: Other divisions also employ their own IT staff to manage several important information technology functions. For example, the divisions are responsible for user account management, including approving or terminating a user's access to the division's computer system and assigning access rights within a system. The divisions also perform their own local area network (LAN) and desktop support duties. Specifically, they are responsible for installing, configuring, upgrading, and maintaining their servers, workstations, and computer peripherals.

Budget and staffing

The Department's budget and staffing for information technology functions are also divided between DTS and other divisions:

- **Division of Technology Services**—As of March 24, 2005, DTS had 359 authorized FTE positions with 76 vacancies. DTS is organized into the following units:

  - **Assistant Director's Office** (8 authorized positions, 3 vacancies)—The Assistant Director is the chief information officer of the Department and conducts agency-wide information technology planning activities, such as disaster recovery planning.

  - **Data Center Services** (65 authorized positions, 14 vacancies)—Manages all Data Center operations, functions, and procedures. The Department reports that the Data Center processes, on average, more than 2.5 million online business transactions each day.

  - **Technical Support** (51 authorized positions, 8 vacancies)—Manages the Department's mainframe operating and database systems, its centrally located server hardware and software, and other information technology networks.

  - **Systems and Programming** (159 authorized positions, 31 vacancies)—Designs, develops, and maintains the Department's primary IT systems. DTS assigns programming personnel to specific programming teams that assist specific divisions.

  - **Support Services** (22 authorized positions, 8 vacancies)—Provides services such as budget and fiscal management and agency-wide information technology planning activities.

  - **Information Security Administration** (5 authorized positions, 0 vacancies)—Initiates and maintains measures to protect the Department's computer hardware, software, and associated data against improper use, modification, or loss.

  - **Customer Service Support Center** (49 authorized positions, 12 vacancies)—Responds to help desk calls, repairs PCs, and is responsible for the installation and maintenance of mainframe and other system hardware and software.

As shown in Table 1, estimated fiscal year 2005 revenues for DTS are approximately $32.4 million, including special line items for lease purchasing of nearly $7 million and for disaster recovery of approximately $750,000. Estimated fiscal year 2005 General Fund monies for DTS total approximately $6.4 million. The majority of DTS' operating expenditures are for personnel-related expenses.

Table 1: Schedule of Revenues and Expenditures[1]
Years Ended June 30, 2003, 2004, and 2005
(Unaudited)

	2003 (Actual)	2004 (Actual)	2005 (Budgeted)
Revenues:			
State General Fund appropriations	$8,107,903	$7,273,112	$8,116,569
Government grants and contracts:			
Federal Centers for Medicare and Medical Services Research, Demonstrations, and Evaluations	6,037,169	6,025,094	6,368,799
Federal Child Support Enforcement	3,730,251	2,949,418	3,522,562
Federal Unemployment Insurance	2,981,122	2,826,739	3,065,696
Federal Temporary Assistance for Needy Families	1,712,780	1,481,211	1,685,150
Federal Food Stamps Cluster	1,329,074	1,720,849	1,612,514
Federal Social Services Block Grant	1,045,811	1,221,375	1,198,039
Other	4,382,019	4,450,802	4,664,101
Child support incentives [2]	1,631,989	2,263,371	2,060,222
Miscellaneous	76,640	182,357	137,332
Total revenues	$31,034,758	$30,394,328	$32,430,984
Expenditures:			
Personal services and employee-related	$16,932,868	$16,914,266	$17,805,643
Professional and outside services	555,981	443,928	1,285,204
Travel	34,372	36,415	93,041
Other	4,067,953	3,904,281	4,777,876
Equipment	9,443,584	9,095,438	8,469,220
Total expenditures	$31,034,758	$30,394,328	$32,430,984

[1] Although amounts for 2003 and 2004 are actual revenues and expenditures as of April 20, 2005, the Department anticipates further administrative adjustments for those years.

[2] Amount that is recovered by the Division of Child Support Enforcement from families who received Temporary Assistance for Needy Families. These monies are considered incentives and, therefore, are not considered federal monies.

Source: Auditor General staff analysis of Arizona Department of Economic Security-provided financial information for the years ended June 30, 2003 and 2004, from its Financial Management Control System as of April 20, 2005, and budgeted information for the year ended June 30, 2005.

- **Other Divisions**—Although staff outside of DTS also perform IT-related functions, auditors were unable to obtain a reliable estimate for the number of staff assigned to IT duties across the other divisions because the Department does not use standardized position requirements for staff who perform duties such as

user account management. However, according to DTS, as of March 2005, there were 23 separate security groups across the divisions, with 67 security representatives. In addition, as of February 2005, according to DTS, there were 22 separate groups that support local area networks and computers across the divisions that employ a total of at least 72 network specialists.

Standards for information security

This audit reviewed information security controls in four areas: access controls, local area network (LAN) and desktop computer management, program change controls, and disaster recovery management. GITA develops standards for information security controls for state agencies. At the national level, the National Institute of Standards and Technology develops standards, and the U.S. Government Accountability Office provides auditing guidelines for information security. Table 2 (see page 6) lists some of the more important controls necessary for effective information security.

Audit scope and methodology

This audit focused on the security of the Department's information systems and the adequacy of its information security controls. It includes four findings and associated recommendations.

- The Department should improve its oversight of access controls, including (1) gaining authority to and then performing background checks on personnel according to the sensitivity of their position, (2) ensuring that employees receive the mandatory new hire computer security training course, (3) developing a job description of security representatives with minimum qualifications and description of duties, and (4) continuing to perform compliance reviews to ensure that security policies are followed.

- The Department should improve its oversight of LAN/desktop computer support duties, including (1) completing efforts to deploy software for controlling the implementation of security updates, (2) ensuring employees understand its acceptable use policy regarding software downloaded from the Internet, and monitoring compliance with its policy, (3) establishing a time frame by which all divisions and administrations must install centrally controlled virus protection software, and (4) establishing minimum training requirements for LAN staff that ensure staff have and maintain adequate skill levels.

Table 2: Examples of Common Information Security Controls

Area	Examples
Access controls and security-related personnel policies	• Policies and procedures for managing user accounts • User access limited to the minimum set of resources required for user's role • Background checks of users • Security awareness training for users
LAN and desktop computer management	• Policies and procedures restricting the use of software downloaded from the Internet to protect against spyware, adware, and other forms of malicious software • Access to Internet and shared platforms restricted to authorized employees and contractors • Regular installation of security patch updates • Regular installation of virus protection updates • Barriers or firewalls to prevent unauthorized access and protect sensitive internal information
Program change controls	• Adequate controls for computer program changes so that all changes are appropriately requested, designed, tested, approved, and implemented • Testing of changes • Documentation of program changes showing supervisory approval, when and how changes are made, and testing information
Disaster recovery	• Regular data backup and remote storage • Plan for restoring services and recovering systems and data • Periodic testing of restoration and recovery procedures

Source: Auditor General staff compilation of information from GITA security standards and the *U.S. Government Accountability Office Federal Information System Controls Audit Manual (1999)*.

- The Department should ensure that computer program changes are better controlled by continuing with its efforts to develop and implement policies to help standardize the process, and to implement an automated testing tool to improve documentation of program changes that it has acquired.

- The Department should complete its disaster recovery plan for information technology systems and add new initiatives it has recently undertaken for disaster recovery.

Auditors used several methods to review the issues addressed in this audit. Audit methods included interviews with department management and staff and review of relevant statutes, rules, policies, and procedures. Auditors also reviewed information

technology security standards as defined by GITA and by federal sources such as the U.S. Government Accountability Office.

In addition, to obtain background information for this audit, auditors reviewed unaudited department reports and records, such as the State Fiscal Year 2004 DES annual report, a list of the Department's mainframe security system's user account information, FTE data for DTS, and descriptive information about DTS organization and functions.

Additionally, auditors used the following specific methods in reviewing each area:

- To evaluate the Department's access control practices, auditors analyzed mainframe user accounts to identify old and unused accounts or accounts whose passwords were not set to expire at regular intervals. To evaluate the Department's compliance with standards regarding computer security training for new employees, auditors reviewed the training transcripts of 50 randomly selected department employees. To gain a better understanding of what security representatives should do, auditors obtained information from two other state agencies regarding the job descriptions and salary classifications of comparable staff.[1]

- To evaluate whether local area networks and computers are adequately protected, auditors met with LAN managers from 4 LAN support groups and analyzed reports on 39 computers provided by those 4 groups.[2] In addition, auditors conducted visits to offices supported by 3 different LAN support groups and reviewed a total of 20 computers in those visits.[3] During these field office visits auditors evaluated whether security patches had been installed, inspected desktop computers for the presence of software downloaded from the Internet that could introduce viruses or spyware into the network, and also reviewed for the presence and status of virus protection software.

- To review the program change process auditors randomly selected ten program changes for the month of October 2004 from four of the larger department systems.[4] Auditors subsequently met with the team leaders for each of the

1 Auditors received information from the Departments of Transportation and Administration, two other large state agencies that handle user account management duties.

2 Auditors met with and received reports from LAN managers in the Division of Developmental Disabilities; the Division of Children, Youth and Families; the Division of Employee Services and Support; and the Division of Employment and Rehabilitation Services—Employment Administration.

3 Auditors conducted visits to field offices supported by LAN staff from the Division of Developmental Disabilities; the Division of Children, Youth and Families; and the Division of Employment and Rehabilitation Services—Employment Administration.

4 Major systems corresponded to the Division of Benefits and Medical Eligibility—Family Assistance Administration; the Division of Child Support Enforcement; the Division of Children, Youth and Families; and the Division of Employment and Rehabilitation Services—Employment Administration.

teams responsible for those systems to review program change documentation, how the process is performed in their team, and to review testing practices.

- To assess the status of the Department's disaster recovery plan, auditors reviewed the computer software disaster recovery planning program the Department purchased and a staff outline showing steps completed in the planning process. Auditors also reviewed logs of backup tapes for agency data and results of tests to reduce backup time. Additionally, auditors reviewed a tri-agency Project Investment Justification (PIJ) that the Arizona Information Technology Committee approved for disaster recovery planning as well as vendor contracts for the provision of temporary emergency computer services and storage of the Department's backup tapes.

The audit was conducted in accordance with government auditing standards.

The Auditor General and staff express appreciation to the director of the Department of Economic Security, the director of the Division of Technology Services, and their staff for their cooperation and assistance throughout the audit.

FINDING 1

Controls over data security need improvement

The Department needs to establish better access controls over its information systems and strengthen central oversight of data security. Access controls and other aspects of the security environment should be strengthened throughout the Department to prevent subjecting confidential information to potential loss or disclosure. Although the Department has recently begun to strengthen central oversight, its monitoring and supervision of data security functions still needs improvement. Account management practices within individual divisions are generally poor. For instance, department units vary greatly in the qualifications they have established for employees responsible for data security, and newly hired employees are not necessarily receiving the mandatory computer security training the Department has established.

Access controls should protect data

Access controls should be designed to protect computer systems and data from unauthorized modification, loss, or disclosure. For example, access controls should ensure that security privileges, such as the ability to create, update, or delete user accounts and reset passwords, are limited only to those people who need this function to perform their job duties. Weak access controls increase the risk of fraud or identity theft, or the loss of data integrity. As noted in the text box, the Department has experienced internal security incidents in the past.

Data Security Incidents

Identity theft—In 2001, an employee of a contractor that administered public assistance programs admitted to Phoenix Police and the Department's Office of Special Investigations that she printed out the personal information of welfare recipients from a department system, and then sold that information.

Social engineering—During 2001-2002, a department employee used a social engineering technique to access the account of a coworker who was on leave and used that account to fraudulently issue herself more than $50,000 in welfare benefits. Social engineering is any technique that manipulates individuals to disclose or alter passwords, allowing others to gain unauthorized access.

Fraud—Because the Department cannot legally perform background checks on people with access to its systems, it unknowingly hired an individual with a criminal record for fraud who lied on her application. This woman subsequently committed fraud against the Department in excess of $100,000. This incident occurred between 1992 and 1994, but the Department still does not have authority to perform background checks on eligibility interviewers like this former employee.

Each division within the Department manages its own access controls. They hire their own security representative(s) to create user accounts, assign individuals' access to data and resources, and manage user accounts. While every division has at least one security group, some divisions have multiple security groups designated to assist specific business units. According to DTS, as of March 2005 there were 23 separate security groups, with 67 security representatives. DTS has recently begun to address department-wide security issues through its Information Security Administration. Within the past year the Information Security Administration has begun to perform compliance reviews and general assessments of information security throughout the Department.

Weaknesses exist in protecting data

The Department's current security environment and access controls should be strengthened. Auditors found that the Department does not effectively manage its user accounts. While it is beginning to address some of the deficiencies, the Department needs to take additional steps to improve.

Controls to restrict access and protect data need improvement—As shown in Table 3 (see page 11), the Department lacks several controls to help ensure that data is adequately restricted and protected. Auditors found that these weaknesses are common throughout the Department and indicate that the Department is not in compliance with GITA state-wide standards. These weaknesses increase the risk that employees have too much access or authority to sensitive data and that unauthorized access could occur through old and unused accounts. Because auditors were primarily assessing system controls, they did not attempt to identify actual cases in which a breach of security occurred. However, auditors did observe situations that illustrate the potential for such occurrences. Table 3 (see page 11) explains the controls required in state and national standards and describes the situations that auditors found regarding them.

Department is taking action, but needs to do more—During the course of the audit the Department began to address some of the issues identified in Table 3 (see page 11). For example, DTS has begun to address the high number of user accounts with security administration privileges by removing these privileges from some accounts.

Table 3: Deficient Access Controls in the Department as of November 2004

Necessary Controls	Conditions Found	Potential Threat
Reviewing access rights: Access rights should be reviewed periodically to ensure that access to resources is granted only to those who need them to perform their jobs.	• In general, security representatives do not review access rights on a regular basis to ensure users' access to data and authority to create, modify, or delete records is appropriate.	Failure to ensure appropriate access rights could permit employees to improperly access confidential or other sensitive data without a need to do so.
Assigning special privileges: Security and account privileges, which provide the authority to perform special functions, such as creating, updating, and deleting user accounts, should be defined and properly restricted.	• The Department has not defined who should have security administration privileges, nor documented why they need such privileges. Individuals range from a grade 8 clerical pool staff to division management. • More than 80 individuals had security administration privileges, more than the number of individuals managing user accounts at two large state agencies: the Departments of Transportation and Administration. Many of these people do not use or need this privilege and many are not members of their unit's security group. • Some security accounts belong to individuals who either left their division or transferred to a job that does not need such special privileges.	Failure to appropriately restrict security administration privileges increases the risk that unauthorized accounts may be created and data improperly accessed. In addition, individuals may not be properly trained or qualified for special privileged access.
Updating passwords: Users should have to change their passwords regularly. According to department policy, passwords should be changed at least once every 30 days.	• More than 200 accounts assigned to individuals do not require users to change their passwords at regular intervals. For instance, one employee has not changed his password in nearly 2 years.	Not changing passwords on a regular basis increases the risk of passwords being discovered and used by unauthorized users.
Removing unused user accounts: Unused accounts should be removed from the system as appropriate regularly. According to department policy, unused accounts should be deleted after 90 days of disuse.	• More than 2,000 user accounts have not been accessed for 90 days or more (nearly 900 belong to specific individuals, while the rest are training or system accounts), and more than 1,300 of those accounts have not been accessed in over a year. • More than 1,100 user accounts have never been used (more than 950 belong to specific individuals).	The presence of old and unused accounts increases the risk that people who should no longer have access may continue to access systems, or that other people, such as hackers, may discover and use the accounts to access systems. This is an especially serious risk in the Department because its mainframe security software does not automatically lock out a user after 90 days of disuse.

Source: Auditor General staff analysis of the Department's 14,082 mainframe user accounts as of November 29, 2004; follow-up interviews with security group personnel located in divisions and programs throughout the Department; review of department policies; and guidelines from the *U.S. Government Accountability Office's Federal Information System Controls Audit Manual (1999)*.

In order to comply with standards regarding data security, DTS should continue to develop new guidelines and improve practices in the following control areas:

Access rights—privileges that define the extent to which an individual can access computer systems and use or modify the programs and data.

- **Reviewing access rights**—Security group personnel should conduct periodic reviews of access rights to ensure these rights are appropriately defined, and DTS should monitor security groups for compliance.

- **Special account privileges**—DTS should define who needs security administration privileges and what kind of authority is needed. The Department should then use its mainframe security software to restrict the authority of accounts with appropriate security administration privileges. For example, if the user needs to reset passwords only, he or she should not be allowed security privileges. DTS needs to collaborate with the divisions to define and restrict security administration privileges to the minimum level required for employees to perform their duties. In March 2005, DTS completed a review of accounts with security privileges. As a result, it deleted some accounts and reduced privileges for some others.

- **Passwords and user account management**—In March 2005, the Department adopted a new policy governing account management. This policy requires the production of a monthly report that shows all users who have not accessed the Department's mainframe in 30 days, and another report showing users who have not accessed it in 90 days. In addition, in April 2005, DTS updated its access control policy to set forth clear guidelines related to deleting old and unused accounts. DTS should monitor compliance with these new and updated policies to ensure that old and unused accounts are properly deleted and account passwords are changed at least every 30 days.

Department has not provided sufficient central oversight

The existence of general security concerns, such as poor user account management, appears to be related to a lack of central oversight of the separate security groups, security representatives, and the activities they perform, as well as a historically weak internal security structure. The Department can improve central oversight by adding an IT audit function, better defining its internal security structure and security representative job requirements, ensuring new employees receive mandatory computer security training, and obtaining legal authority to conduct background checks of employees in sensitive positions.

Lack of central review for security compliance—Historically, the Department has not provided central oversight of security functions. However, DTS established an Information Security Administration in September 2003, and has

recently begun to perform some compliance reviews and general assessments of information security throughout the Department. The Information Security Administration should continue to conduct compliance reviews and assessments, develop a schedule of regular reviews, and establish policies and procedures or a manual to document its practices. In addition, the Information Security Administration should develop a follow-up process to ensure divisions appropriately comply with recommendations.

While DTS' activities will help improve central oversight, the Department needs to augment this review. The Department does have an internal auditing group, but it currently does not audit IT issues. In addition, the Department has never undergone an external independent third-party review of its information security. An internal IT audit function is important because it helps the Department obtain effective and efficient security controls. In addition, other state agencies, such as the Departments of Transportation and Administration, have contracted with external experts to perform security assessments to review the adequacy of their IT structures. Although such security assessments may cost several hundred thousands of dollars, they provide independent assurance that certain state and federally mandated standards are met. According to DTS management, if and when the Department decides to acquire an external review, it will then identify an appropriate funding source. The Department should establish an internal IT audit function. In addition, the Department should consider contracting for an independent security assessment.

Department has not defined security representative position—The Department has not created a job position, description, or minimum qualifications for security representatives. Instead, each security group decides who to hire and to some extent their job responsibilities. As a result, auditors found that one division has security representatives with backgrounds in information technology. These security representatives are paid substantially better than those in other security groups, which use support and clerical staff to perform the same functions. By comparison, the Departments of Transportation and Administration have job descriptions, minimum qualifications, and pay grades for their employees who manage user accounts. These employees are paid salaries greater than the Department's security representatives noted above. Some essential tasks of such positions include user account management, monitoring user access, and investigating security violations. The Department developed a draft job description in June 2005, which contains the minimum qualifications for a security representative. The Department should adopt this job description to ensure that only individuals who meet these qualifications are authorized to conduct security representative duties.

Security representative job resources and training inadequate—In addition to lacking a job description and minimum qualifications for security representatives, the Department does not have a manual explaining what security representatives should do, and does not provide them regular training. The

Department should develop a manual regarding the duties of a security representative that can be used as a reference resource and ensure that adequate training is provided so that they understand their jobs and duties. Currently, the Department considers only employees who handle mainframe access rights to be security representatives. However, in some divisions other personnel handle system application access rights and therefore could also be considered security representatives. The Department needs to identify these people who perform similar duties, include them as security representatives, and ensure they meet certain minimum qualifications and receive appropriate training.

Not all newly hired employees receive computer security training—GITA standards require that all state employees receive computer security training prior to being allowed computer access, and the Department has a similar policy. The Department's training informs employees of its security practices. For instance, the training manual tells employees that they should never divulge their passwords to anyone. However, in a random sample of 50 employee training records maintained in a central training database, only 21 (42 percent) department employees had taken this mandatory course. According to the Department's training management, the Department has failed to create tracking and follow-up mechanisms to ensure that all new hires receive this mandatory training. The Department should ensure that all employees receive this mandatory training and monitor for compliance.

Department lacks legal authority to conduct background checks on key personnel—Background checks are an important tool in making sure that untrustworthy individuals who might commit identity theft or fraud, or otherwise compromise data integrity, are not hired or placed in positions of trust. According to Arizona Revised Statutes, noncriminal justice agencies must receive either statutory authority or an executive order granting them the ability to conduct background checks for the purpose of hiring particular employees. However, the Department does not have this authority, other than for some employees who work with juveniles or children. Another state agency, the Department of Administration, has statutory authority to request criminal background information on IT personnel.

Criminal background checks are not conducted on IT personnel.

The Department should determine which positions involve the security and access of sensitive information and therefore merit a background check. The Department should then request the authority, through statute or an executive order, and ensure background checks are conducted on those individuals. In addition, periodic background checks should be conducted on long-term employees in accordance with the sensitivity of their position.

Recommendations

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.

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.

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.

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.

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

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.

FINDING 2

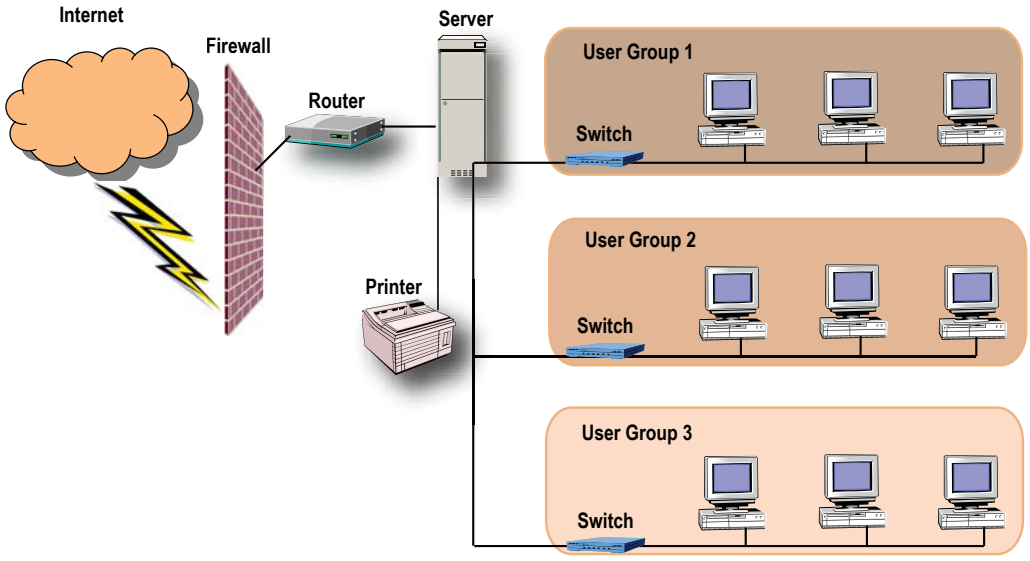
Information in local area networks and computers not adequately protected

The Department needs to improve management of its local area networks (LANs) and computers to better ensure system security and operability. Good management of LANs and computers provides protection against virus attacks, unauthorized intrusion, and possible loss of data. However, the Department does not adequately ensure that virus protection updates and security patches, which fix known security vulnerabilites from outside threats, are up-to-date, and that employees do not download unsafe software from the Internet. While the Department is taking some steps to improve security, it could do more.

LAN/computer support important to system security and operability

Local area networks connect computers within a limited geographic area so that they can share information, share computer peripherals such as printers, and access systems and data that support their job functions. (See Figure 1, page 18, for an illustration of a LAN.) Separate LANs can be connected to form larger networks, as is the case within the Department. The Department uses larger networks to connect computers throughout the State to each other and to central data repositories. For example, the Division of Children, Youth and Families' employees use their network connection to use shared devices in field offices, such as printers, and to access the Internet, e-mail, the Division's computer systems, and any other department computer systems that a given employee is authorized to use.

Figure 1: Example of a Simple Local Area Network Connected To the Internet



Source: Auditor General staff.

The Department manages LAN/computer security in a decentralized manner. Each division operates one or more local LAN support units by hiring its own network support specialists who install, configure, upgrade, and maintain the local area networks, servers, and computers. According to DTS, there are 22 separate local LAN support units, with 72 network specialists in those groups. DTS, through its own LAN manager, conducts monthly meetings for LAN support staff during which entity-wide issues may be discussed.

Securing local area networks and computers is important so that viruses or security weaknesses in one computer cannot negatively impact other computers in the network, and to prevent unauthorized access into systems and data. For example, in August 2003 the Department, along with other entities that failed to implement a specific security patch update, was infected by the Nachi virus (see text box). This virus quickly spread throughout the

Example of Nachi Virus Infection at the Department

Discovery date—August 18, 2003

Method of infection—Spreads by exploiting a vulnerability in Microsoft Windows. Irrespective of virus protection, if the machine is not patched, it is susceptible to attack.

Resolution—Apply Microsoft security update MS03-026 and then disinfect the system with a virus removal program.

Intentions of the virus—Spreads by exploiting a hole in Microsoft Windows. It instructs a computer to download and execute the virus from the infected host.

Source: McAfee, Inc. Web site, reviewed March 29, 2005.

Department and increased network traffic by about eight times its normal rate, bringing down or limiting system operability for about 2 days throughout the Department. The Department's virus protection software detected about 134,000 infections by the Nachi virus during one week. This attack was propagated due to inadequate computer security patches.

Poor protection of computers resulted in limited network operability for 2 days.

Computers and networks not adequately protected

The Department needs to improve management of its LANs and computers to better protect them against possible virus attacks, hackers, and possible loss of data. Auditors found that local LAN support units do not consistently perform key security functions such as installing security patches to protect computers from outside threats, installing virus protection software, and prohibiting the download and installation of Internet software that can contain harmful programs.

Security patches not installed—Timely installation of security patch updates is vital in order to maintain the operational availability, confidentiality, and integrity of information technology systems, but the Department is not ensuring that these patches are deployed in a timely manner. Every operating system has vulnerabilites that hackers can potentially exploit to attack a system. For example, hackers have discovered vulnerabilites in the Microsoft Windows operating system. As a result, Microsoft regularly issues critical security updates that are designed to patch the security hole that had been identified. For instance, one February 2005 security update is necessary in order to help ensure that a computer environment is not vulnerable to an outside attack (see text box). If this update is not installed on the machine, the computer environment may be exposed to an unnecessary amount of risk.

Example of a Windows Security Update

Release Date—February 8, 2005.

Recommendation—Customers should apply the update immediately.

Vulnerability details—An attacker could exploit a vulnerability that could potentially allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Source: Microsoft Security Bulletin MS05-012.

Automated computer tools exist that allow organizations to centrally control and install security updates on all computers connected to a given network. However, auditors reviewed the practices in four different local LAN support units and found that only one of the four uses an automated tool to ensure that updates are installed on all computers. Staff in the other three local LAN support units stated that they perform security updates only when they either physically go to the computer or remotely access it, installing updates one computer at a time. Auditors reviewed 57 department computers and found 55 computers missing one or more critical updates. Seven were missing more

Seven computers were missing more than 20 critical security updates.

than 20 updates, and some of the missing updates have been available since 2003. For example, one update issued in October 2003 patches a vulnerability that could allow an attacker to remotely control a computer if that computer user accesses a Web site or views e-mail from someone with malicious intent. Microsoft recommends that this patch be installed immediately.

In April 2005, the Department identified an automated tool that will allow it to centrally control security updates for all Department computers. DTS reports it procured the tool in June 2005, and plans to implement it in January 2006. According to department officials, this will help ensure that the Department can respond to risks in the computer environment in a more timely and effective manner. The Department should implement the tool as planned. In addition, it should periodically monitor to ensure that updates are installed on all computers.

Virus protection coverage recently improved—Antivirus software helps protect a computer from virus attacks by detecting and removing computer viruses, which in turn helps protect the network from attacks because the computer would then not infect other computers in the network. The Department has recently increased participation in a centrally controlled virus protection software, but this software is still not used uniformly. Since 2002, the Department has purchased an annual license for an entity-wide version of virus protection that can be installed on every machine in the Department and allows the Department to centrally control and monitor to ensure that the most recent virus protection updates are received by every computer. However, not every division is using this software to protect all of their computers.[1] The Department is in the process of moving all of its computers to this centrally controlled process, and internal reports indicate the number of computers receiving daily virus updates has increased from nearly 4,600 in November 2004 to nearly 5,700 in February 2005. According to internal reports, about 2,000 computers still remain outside the Department's centrally controlled virus protection software. The Department should create a time frame by which all divisions and administrations must use this centrally administered virus protection software, ensure that all computers have the virus protection software installed, and then monitor to ensure that all computers regularly receive current updates.

Downloaded software poses risk—Downloading and installing software from the Internet can potentially expose a computer environment to malicious code, and currently not enough is being done to minimize this risk. When an employee installs a free program from the Internet, he or she may also unknowingly be installing adware, spyware, or other forms of malware (see text box on page 21). This software can potentially allow outside users to discover passwords, slow or lock up a system, and install other forms of malware. The Department has an acceptable use policy which states that employees are prohibited from downloading and installing any

1 Staff in four local LAN support units said all their computers have at least a local version of virus protection installed. One of these units provided a report indicating that all of its more than 600 personal computers have virus protection software installed and are receiving weekly updates; however, ensuring that the entire network is protected would require checking thousands of additional computers.

software program not specifically authorized by local IT management. However, when auditors conducted field office visits of three divisions, they found the presence of nonbusiness-related software downloaded from the Internet on 6 of 20 computers reviewed. For example, auditors found a Web search tool that is known to also install adware that logs the computer's Internet activity, changes the Internet browser, and displays advertisements. The Department should ensure that its employees and local LAN support units understand its current acceptable use policy, and monitor its divisions and employees for compliance. For example, local LAN support units could conduct random reviews of computers to determine if nonbusiness-related software had been installed.

Spyware—any software that covertly gathers user information, such as passwords, through the user's Internet connection; typically bundled as a hidden component in freeware or shareware programs that are downloaded from the Internet.

Adware—a form of spyware that collects information about the user in order to display advertisements in the Web browser.

Malware—software designed to disrupt or harm a system, such as a virus.

Department has not provided sufficient central oversight

Similar to its lack of central oversight of groups of security representatives, the Department historically has not provided sufficient central oversight over the security of its LANs and computers, and therefore some of the weaknesses and recommendations identified in Finding 1—Access Controls (see pages 9 through 15) apply to LAN oversight and compliance as well. Specifically, the Department has not provided oversight to ensure that local IT staff comply with relevant standards. The Information Security Administration is now beginning to review certain LAN security issues throughout the Department, and, as recommended in Finding 1, should continue to conduct compliance reviews and assessments, develop a schedule of regular reviews, and document its practices. If, as recommended in Finding 1, the Department establishes an internal IT audit function and possibly contracts for an independent security assessment, it should include the security of LANs and computers as part of those reviews.

While DTS is currently attempting to address the lack of central oversight by establishing centralized control of key LAN security tasks, more needs to be done to ensure employees have the necessary skills for their jobs. Current projects in the Department will bring all networks into a single administrative structure, centralize security patch management, and centralize virus protection. However, the Department has not established standards for minimum training requirements for network support personnel. Training for these employees is important because they work in a constantly changing environment. The Department should review the training practices of the local LAN support units and establish regular training requirements that will help ensure that LAN support staff have and maintain adequate skill levels.

Recommendations

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.

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.

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.

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.

FINDING 3

Department could improve its management of computer program changes

The Department could better manage its process for making changes to computer programs. Effective controls over this process help ensure that only authorized modifications are made to computer programs. DTS has more than 20 project teams working on department systems. Their processes are inconsistent across programming teams and their testing of programming changes is not always adequate to ensure that program modifications are fully functional and correct. However, the Department is making efforts to address these issues.

Effective change process important to system functionality

Department systems frequently require changes to their computer programs. State or federal mandates, such as the federal Health Insurance Portability and Accountability Act (HIPAA), require changes in department systems. In addition, divisions that use the systems may identify errors or recommend changes for improvement. During the first half of fiscal year 2005, the Department implemented 991 change requests to its mainframe systems, according to a department report.

Effective management of the program change process is important to ensure that programmers do not introduce malicious or inappropriate changes to a system, and to safeguard systems against ineffective or faulty program changes. Inadequate program change management can lead to programming errors and inefficiencies. For example, in a previous audit, auditors found significant computer errors that potentially subjected Arizona employers to penalties and assessments by providing inaccurate information to the U.S. Internal Revenue Service. During that audit the Department

Program Change Example

Requesting Unit—Division of Benefits and Medical Eligibility

Reason for Request—The Department's electronic benefits transfer (EBT) program changed vendors.

Request—Allows for changes that are necessary to convert EBT to the new vendor.

attempted to correct the errors, but auditors found that the program continued to produce inaccurate information, indicating that testing of this program change was inadequate. For greater detail on this programming error, see the Department of Economic Security, Division of Employment and Rehabilitation Services—Unemployment Insurance Program, Auditor General Report No. 05-01, pages 21-24.

Current change process lacks consistency

The current process for making changes varies greatly among programming teams. The program change process should be adequately controlled so that all changes are appropriately requested, designed, tested, approved, and implemented. The Department's Quality Assurance group, which moves program changes to production, does not move any change to production without documentation showing that the change is appropriately approved by the end user and the programmer's supervisor. However, the lack of consistency between teams increases the risk of having inadequate controls over some program changes. DTS is making efforts to improve its program change process.

Program change process can be improved—DTS can improve two aspects of program change management:

- Program change process not standardized across programming teams—The DTS programming group employs more than 120 programmers assigned to over 20 programming teams that each work on separate systems or parts of systems. Different teams use different procedures to manage the program change process. Specifically, teams use different procedures and forms to receive user requests for program changes, track progress, and note approval for program changes. Some teams had no written documentation illustrating their procedures or overall methodology. The lack of a uniform, standardized process increases the risk of having inappropriate or inadequate changes introduced into a system and having inadequate documentation necessary for performing program maintenance.

- Testing of program changes is not always adequate—An essential step in developing a program change is adequate testing so that the change will be fully functional and work correctly once it is moved to production. However, according to division officials, programmers typically conduct only limited testing of program changes before allowing the end user to conduct testing. Further, DTS has not established standards for what is acceptable testing of program changes. Often, DTS could not provide auditors with documentation of test plans and test results.

DTS making efforts to address weaknesses—DTS is making efforts to address both of these weaknesses. Specifically:

- Standardizing the program change process—DTS is developing a written system development methodology and program change management policy. The new methodology and policy are being created to govern a new programming area within the Department, but DTS anticipates using these policies and procedures to standardize, to the extent possible, this same methodology across all teams. According to DTS management, these policies will not be finalized until some time after June 30, 2005. DTS should ensure that this methodology is applied to all project teams.

- Improving the adequacy of testing—In April 2005, the Department acquired an automated testing tool that will allow it to conduct well-documented, thorough testing of program changes. According to DTS management, this tool should be implemented by July 2005. DTS should ensure that the testers receive adequate training to use the new tool and ensure that it is used as frequently as possible, in accordance with the nature of the program change.

Recommendations

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.

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.

FINDING 4

Department has made progress in disaster recovery

The Department has made progress in improving its disaster recovery planning—its procedures for what to do in the event of a major hardware or software failure—although it needs to complete its efforts to put effective procedures in place. Disaster recovery planning allows critical services to continue even when major computer systems are damaged or destroyed. Since 2004, the Department has taken a number of actions to put a disaster recovery plan in place, although it still needs to complete and test the plan and move forward with plans to back up critical systems daily. However, its current plans address only those actions needed if disruptions last for a short period. A comprehensive solution will require state-wide disaster recovery planning and identification of future funding sources.

Disaster recovery planning minimizes service disruption

Disaster recovery planning allows critical services to continue in the event of damage to an agency's computer systems. Without such planning, an agency can lose the ability to provide services to the public for an extended period of time. In the Department's case, loss of its computer systems would disrupt services to an estimated over 1 million people and affect claims and benefits payments such as unemployment insurance or TANF cash assistance (see text box). Therefore, it is very important for the Department to have an up-to-date contingency plan so it can resume services as quickly as possible should a major computer hardware or software failure occur.

The Department reports that it serves over 1 million children, adults, and families per month. Damage to the Department's computer systems can lead to the disruption of critical services, such as:

- Unemployment insurance payments: an average of over $32.9 million per month in fiscal year 2004
- Federal TANF cash benefits: an average of over $14.6 million per month in fiscal year 2004
- Ability to track client information for programs such as Child Protective Services and foster care
- Timely payments to agencies providing services to Arizona children, families, the disabled, and the elderly

Source: Auditor General staff analysis of the *Department of Economic Security Annual Report for SFY 2004*; and list of mainframe application systems provided by the Department.

Comprehensive government and industry standards exist for disaster recovery plans. For example, GITA's standards include developing procedures and tasks for staff to assist in system recovery and arranging with vendors to provide computer services. In general, a comprehensive disaster recovery plan should include the following components:

- A risk analysis identifying critical transactions for department programs;
- A designated alternative computer facility or "hot site";
- Development of test plans to determine the effectiveness of disaster recovery procedures with periodic testing of these plans;
- Employees organized into disaster recovery teams along with tasks assigned to those teams;
- A list of procedures for processing critical transactions, including forms and other documents to use; and
- Scheduling frequent regular backups of agency information and storing that information at remote sites throughout the year.

Department has improved disaster recovery planning

The Department has made progress in disaster recovery planning after experiencing some delays due primarily to lack of staff. Although the Department has made progress since hiring disaster recovery staff, it still needs to complete and update some plan components, conduct testing, and move forward with plans to conduct critical backups on a daily basis.

The Department reports that lack of a disaster recovery manager slowed down initial progress that started in 2002.

Disaster planning started slowly but has made progress—The Department did not effectively address disaster recovery planning for several years. In 2002, the Department purchased a computer software planning system for disaster recovery that has also been used by other state agencies, such as the Department of Administration and the Department of Public Safety, and in 2003 the Department developed a nearly 40-page outline that shows steps for completing the plan. However, according to department officials, turnover in the disaster recovery planning position resulted in only partial progress in entering information into the planning software.

More progress came in calendar year 2004 when the Department hired a disaster recovery manager, obtained funding for disaster recovery initiatives, began regular off-site storage of the data it backs up, and obtained access to emergency hot site

services. Additionally, according to department officials, it has established a timetable for completing the information in its software planning system. Table 4 (see page 30) shows the status of the Department's disaster recovery planning activities as of February 2005. As the table shows, the Department has taken action in each of the four major planning areas—mainframe recovery, network recovery, server farm recovery, and facility recovery.

Department should complete and test its plan—The Department needs to update its planning software to include information on the more recent planning activities undertaken, including the emergency hot site services, new network strategy, and regular data backups. It should also follow through with its timetable to complete the plan so that it includes all of the items shown in Table 4 (see page 30). For example, it should add information to its mainframe and network plans on recovery teams' tasks and assignments and vendor assets and supplies. The Department adopted a maintenance plan in May 2005, which sets forth a schedule for updating individual plan components. In addition, the Department needs to determine which mainframe applications are most critical, develop a prioritized list for the sequence of recovering these applications, and add this information to its recovery planning software. The Department should also update its recovery planning software to include information about its plan to have a vendor provide backup resources for its server farm. The Department developed a final test plan prior to its scheduled testing dates at the emergency hot site in June 2005. The Department should ensure that it adds testing plan information to its recovery planning software as part of its ongoing plan maintenance.

Department should conduct daily backups of critical systems—In addition to determining which mainframe systems are most critical and adding this information to the plan, the Department should also begin daily backups of its most critical applications. The Department has begun to take action in this area. For example, the Department used some of its disaster recovery funding to purchase new tape drives, allowing faster backups. The Department reports that it can now back up its systems faster. The Department began daily backups of its most critical mainframe systems starting in June 2005. In addition to adding this information to its plan, the Department should continue to conduct these daily backups, and develop policies related to these backups, and add this information to its planning software.

The Department reports that its new tape drives allow faster backups of mainframe systems.

Comprehensive solutions require state-wide planning

According to department officials, current planning activities do not provide comprehensive disaster recovery solutions. For example, the Department estimates that it could take a minimum of 2 weeks to restore mainframe and network services at the current temporary hot site. In the event of an emergency, hot site services are contractually guaranteed by the vendor to be available to the Department for only 6 weeks. The funding and contract for the hot site was initially approved for fiscal year

Table 4: Status of Disaster Recovery Planning Activities as of February 2005

Plan Components	Purpose of Plan Component	Actions Taken
Mainframe recovery	Restore and recover hardware and software functions to operate the Department's mainframe computer.	• Spring 2004—The Department began to back up mainframe data on a regular basis and store it at a remote site. • Spring 2004—GITA approved a tri-agency Project Information Justification (PIJ) to allow the Department, the Department of Administration, and the Department of Public Safety to seek funding for disaster recovery initiatives. The Department reports that it subsequently: ◆ Obtained 1-year funding for a hot site and scheduled test dates for recovery of mainframe functions at the hot site; ◆ Used part of this funding to purchase tape drives for faster backups of mainframe computer data through the year. • The Department has partially completed its plan. Missing items include: ◆ Identification of the Department's most critical mainframe applications. ◆ Tasks and assignments for 6 of its 15 restoration or recovery teams. ◆ Documentation of some vendors to supply equipment and for vendor assets and supplies.
Network recovery	Restore the network's capacity to provide division and program connections to the Department's mainframe computer.	• Fiscal year 2005—the Department plans to implement a process with a contractor to enable its computer network to be redirected to the emergency hot site. • The Department has partially completed its plan. Missing items include: ◆ Tasks and assignments for 8 of its 15 recovery or restoration teams. ◆ Documentation of some vendors to supply equipment and for vendor assets and supplies.
Server farm recovery	Restore operations for programs run from a group of department servers at a department data center.	• The Department reports that it is working with state procurement staff to efficiently obtain vendors to supply backup servers in the event of an emergency. • The Department has partially completed the plan. Missing items include: ◆ Tasks and assignments for 6 of its 58 recovery or restoration teams. ◆ Assets, equipment, and supplies lists by vendor. ◆ Telecommunication lines and equipment information.
Facility[1]	Provide for safe evacuation and relocation of staff, assessment of damage, and the cost to restore the facility.	• DTS' main facility has an evacuation plan, which has been tested.

[1] Three areas of the Department coordinate facility recovery plans: facilities management in the Division of Budget and Finance, risk management in the Division of Employee Services and Support, and building coordinators for each facility. Local office coordinators, local office managers, or building coordinators are responsible for oversight of staff evacuation.

Source: Auditor General staff compilation of information from the Department's Living Disaster Recovery Planning System software program, budget reports, interviews with DTS staff, and vendor contracts.

2005 only. That year, the Legislature approved $742,300 from the State's Risk Management Fund for the Department's disaster recovery plan. The Legislature approved additional funding from the same funding source in its fiscal year 2006 budget, although it reduced the amount to $271,500.[1]

Current planning activities do not provide a comprehensive solution.

State-wide planning may be required to support comprehensive disaster recovery solutions for the Department and other state agencies that maintain critical data. Department officials are currently participating in a state-wide planning group with other agencies, such as the Department of Administration and the Department of Public Safety, to work on long-term disaster recovery solutions. This state-wide planning group, which includes the Governor's Office, is discussing strategies such as an information systems recovery services site to serve all state agencies. In addition to state-wide planning, these long-term solutions also require the identification of additional funding beyond that which supports temporary hot site services.

Recommendations

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.

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

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

[1] JLBC's recommendation stated that the reduced appropriation from the Risk Management Fund for fiscal year 2006 could generate federal matching fund monies and permit total funding of $742,300. However, because the Fund includes federal monies, the Department is working with the State Comptroller's Office to determine whether and how this can be done while complying with restrictions on federal monies.

AGENCY RESPONSE

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.

Performance Audit Division reports issued within the last 24 months

03-05 Department of Economic Security—Child Protective Services—Foster Care Placement Stability and Foster Parent Communication
03-06 Arizona Board of Appraisal
03-07 Arizona Board for Charter Schools
03-08 Arizona Department of Commerce
03-09 Department of Economic Security—Division of Children, Youth and Families Child Protective Services—Caseloads and Training

04-L1 Letter Report—Arizona Board of Medical Examiners
04-L2 Letter Report—Gila County Transportation Excise Tax
04-01 Arizona Tourism and Sports Authority
04-02 Department of Economic Security—Welfare Programs
04-03 Behavioral Health Services' HB2003 Funding for Adults with Serious Mental Illness
04-04 Department of Emergency and Military Affairs and State Emergency Council
04-05 Department of Environmental Quality—Water Quality Division
04-06 Department of Environmental Quality—Waste Programs Division
04-07 Department of Environmental Quality—Air Quality Division
04-08 Department of Environmental Quality—Sunset Factors
04-09 Arizona Department of Transportation, Motor Vehicle Division— State Revenue Collection Functions
04-10 Arizona Department of Transportation, Motor Vehicle Division—Information Security and E-government Services
04-11 Arizona Department of Transportation, Motor Vehicle Division—Sunset Factors
04-12 Board of Examiners of Nursing Care Institution Administrators and Assisted Living Facility Managers

05-L1 Letter Report—Department of Health Services—Ultrasound Reviews
05-01 Department of Economic Security—Unemployment Insurance
05-02 Department of Administration—Financial Services Division
05-03 Government Information Technology Agency (GITA) & Information Technology Authorization Committee (ITAC)

Future Performance Audit Division reports

Department of Economic Security—Service Integration

Department of Revenue—Business Reengineering/Integrated Tax System (BRITS)