A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit

Department of Administration—

Information Services Division and Telecommunications Program Office

SEPTEMBER • 2005
REPORT NO. 05 – 11

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

Dale Chapman, Manager and Contact Person
Channin DeHaan, Team Leader
Aaron Cook
Jay Dunkleberger

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

September 26, 2005

Members of the Arizona Legislature

The Honorable Janet Napolitano, Governor

Mr. Jerry Oliver, Interim Director
Arizona Department of Administration

Transmitted herewith is a report of the Auditor General, A Performance Audit of the Department of Administration—Information Services Division and Telecommunications Program Office. 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 Administration agrees with all of the findings and plans to implement or implement in a different manner 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 September 27, 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

Department of Administration
Information Services Division

Services:

The Information Services Division (Division) delivers state-wide information technology services to executive branch agencies and provides technology services to support internal functions within the Department of Administration (Department). In addition to eight positions that report to the assistant director and provide administrative support and planning, the Division provides services in five main areas:

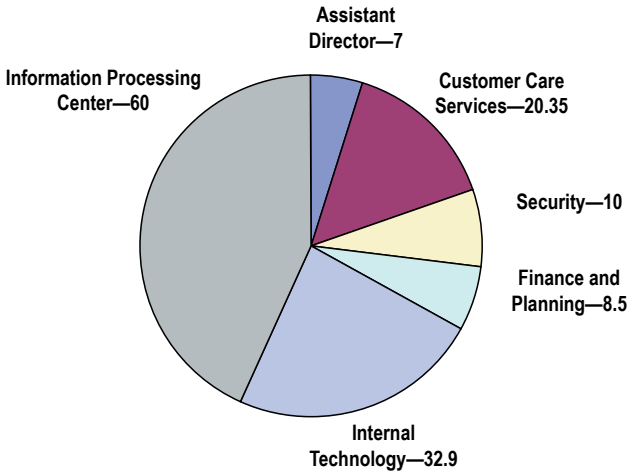
- Information Processing Center—Operates and maintains the Department's data center, which provides data processing and storage services for state agencies such as the Arizona Health Care Cost Containment System, the Arizona Department of Transportation, and the Department of Revenue.
- Security—Conducts a variety of security services for the Department and other state agencies, such as providing state employees with computer system and network security access, and security training for department employees.
- Internal Technology—Provides support for the Department's desktop computers, operates the Department's internal agency network, and supports the Department's Arizona Financial Information System and the Human Resources Information Solution.
- Finance and Planning—Provides budget, planning, and financial analysis to the Division and determines the rates agencies are charged for services. This section also administers the Department's 9-1-1 telecommunications services.
- Customer Care Services—Provides liaison services and customer support to the Division's internal and external customers and houses the state switchboard, which answers calls to a central state number and routes them to the appropriate person or agency.

Facilities:

The Department's headquarters are located at 100 North 15th Avenue in Phoenix and are leased under the private lease-to-own (PLTO) program. In fiscal year 2005, the

Division staffing:

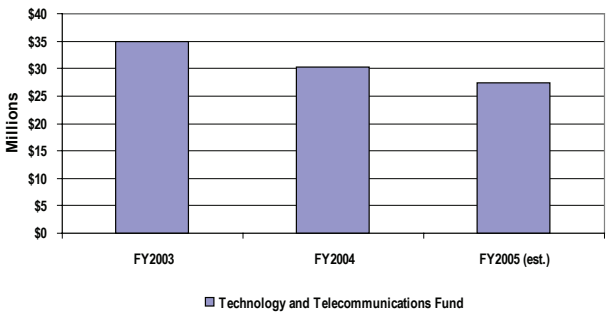
138.75 filled postions and 26.9 vacancies (as of July 2005)[1]



[1] **Includes 11 FTE funded by the Telecommunications Program Office appropriation but housed in the Division.**

Division revenue:

$27.4 million (fiscal year 2005, estimated)



Division used approximately 21,000 square feet at this facility and paid an annual lease fee of approximately $419,000. In addition, the Division leases office or storage space in three other buildings in Phoenix and two buildings in Tucson, and paid annual lease fees of approximately $390,000 for those facilities.

Equipment:

In addition to common office equipment, the Division has specialized equipment for which it has state- or department-wide responsibility, such as the mainframe system, backup power generators, servers, and other network equipment.

Mission:

The Division has adopted the Department's mission:

To provide effective and efficient support services to enable government agencies, state employees, and the public to achieve their goals.

Goals:

The Division has adopted the Department's three goals:

1. To deliver customer service second to none.
2. To attract and retain a high-performance team of employees.
3. To aggressively pursue innovative solutions and/or opportunities.

Adequacy of performance measures:

The Division's 66 performance measures are generally adequate and include measures for outcome, output, efficiency, and quality. Almost all of the Division's service units have their own set of performance measures, and each of the measures directly corresponds to one of the Division's three goals. However, Customer Care Services does not have any performance measures. The Division should develop performance measures that help ensure Customer Care Services meets division goals, such as the time it takes to respond to customer requests for service and customer satisfaction with the help desk.

Source: Auditor General staff compilation of unaudited information obtained from the Arizona Financial Information System (AFIS) for the years ended June 30, 2003 and 2004; the Department's fiscal years 2005-2009 strategic plan; and other information provided by the Department, including financial estimates for the year ended June 30, 2005.

PROGRAM FACT SHEET

Department of Administration
Telecommunications Program Office

Services:

The Telecommunications Program Office (TPO) was created by the Legislature in 2005 to enter into a contract with a contractor to provide for the telecommunications needs for each state office, department, or agency. The contractor will manage telecommunications services for all executive branch state agencies, including obtaining local and long-distance telephone calling service and building a state-wide telecommunications network.

Funding:

Although the Department of Administration (Department) organized the TPO in fiscal year 2005 and funded it with part of the Information Services Division appropriation, the TPO did not receive its initial appropriation of nearly $2.2 million until fiscal year 2006. This includes $350,000 in a one-time appropriation for professional and outside services, and a $9,000 one-time appropriation for equipment.

Facilities:

The TPO uses approximately 3,000 square feet of the Department of Administration facilities at 100 N. 15th Avenue in Phoenix, Arizona. In addition, the telecommunications contractor uses approximately 12,000 square feet at two department buildings in Phoenix, and a third in Tucson. To reimburse the Department for the approximately $200,000 in costs associated with the use of these facilities, the Department plans to add a surcharge to agency telecommunications bills in fiscal year 2006.

Program staffing:

11 FTE (fiscal year 2006)[1]

[1] **Eleven FTEs who assist with network security, switchboard, and helpdesk are housed in the Information Services Division.**

Equipment:

The TPO owns common office equipment, but is also charged with administering a contract that develops a unified state voice and data network for executive branch agencies.

Mission:

The TPO has adopted the Department's mission:

To provide effective and efficient support services to enable government agencies, state employees, and the public to achieve their goals.

Goals:

The TPO has adopted the Department's three goals:

1. To deliver customer service second to none.
2. To attract and retain a high-performance team of employees.
3. To aggressively pursue innovative solutions and/or opportunities.

Adequacy of performance measures:

The TPO was formally created in statute as of June 30, 2005, and at the time of this audit had not developed performance measures to meet its goals. According to a department official, the TPO plans to create these performance measures by the end of October 2005 and is currently in the process of developing customer service questions evaluating agency satisfaction with various aspects of state-wide telecommunications services.

Therefore, the TPO should ensure it develops appropriate measures such as those evaluating agency satisfaction with the contractor's telecommunications service and the contractor-managed state-wide privatized network, and the effective use of a state-wide investment pool to purchase telecommunications equipment.

Source: Auditor General staff compilation of unaudited information obtained from the *State of Arizona, FY 2006 Appropriations Report*; Arizona Revised Statutes; contracting documents; and other information provided by the Department.

SUMMARY

The Office of the Auditor General has conducted a performance audit of two areas within the Arizona Department of Administration—the Information Services Division and the Telecommunications Program Office—pursuant to a November 20, 2002, resolution of the Joint Legislative Audit Committee. This 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 second in a series of four reports on the Department of Administration (Department). The first audit reviewed the Department's Financial Services Division (Auditor General Report No. 05-02), and the third audit will review the Department's Human Resources Division, including the State's self-funded health benefits program. The final report will be an analysis of the 12 statutory sunset factors.

The Information Services Division (Division) provides a variety of information technology and telecommunications services to the Department and other state agencies, including maintaining and operating the department mainframe, providing information security services to the Department and other state agencies, supporting the Department's computer network, and operating the State's main telephone switchboard. The Telecommunications Program Office (TPO) provides oversight for a 5-year, approximately $40-million-per-year telecommunications outsourcing contract required under Laws 2003, Chapter 263, Section 101. Under a contract signed in January 2005, the State will consolidate management of all executive branch telecommunications services under a single contractor. Further, the contractor is required to create a single state-wide voice and data network used by executive branch agencies called AZNET.

Several actions needed to improve information security (see pages 11 through 21)

The Department should take a variety of actions to further ensure the security of the State's information systems and the data stored on them. The Department maintains and secures some of the State's most sensitive information technology (IT) resources and data, including driver's license and vehicle registration information and state employees' payroll information. While the Department performs some security functions well, such as properly securing its desktop computers, it does not perform

What Are the Department's Networks?

Internal Network—The Department maintains a network of computers linking its divisions to serve its internal needs.

State Network—A network linking state agencies, allowing them access to data and computer applications housed in the Division. This network will be expanded to form Arizona Network (AZNET), a consolidated, privatized telecommunications network that will provide both voice and data capabilities. The AZNET is scheduled to be completed in May 2006.

many functions that national guidelines dictate. Specifically, the Department does not perform regular monitoring and testing of its internal network in order to identify and resolve potential system vulnerabilities. This lack of monitoring and testing increases the risk of network intrusion, which could allow a hacker to gain access to sensitive systems and data. Additionally, the Department has not performed risk assessments to identify and evaluate the risks to the security of its information resources, developed comprehensive security policies and procedures, ensured corrective actions are implemented to address identified security weaknesses, and provided annual security awareness training to department employees.

To ensure that the Department has a coordinated security program that addresses the deficiencies described above, it should establish a centralized and comprehensive security program. Specifically, the Department should assign one of its positions, such as the state-wide security manager, the responsibility for administering a comprehensive security program. The Department should determine if it needs additional resources, including staff to enhance security. If additional staff and resources are needed, the Department should assess whether it could reassign existing staff and resources or take other steps, as appropriate, to seek additional staff and resources.

Additionally, the Department should request statutory authority to enforce security requirements that state agencies must follow to use AZNET. Currently, no agency has statutory authority to enforce security standards for information systems shared by state agencies. GITA has statutory authority to issue state-wide security standards, but not operational authority to enforce its standards. Further, GITA's functions do not include the daily oversight of AZNET that would be necessary to enforce its standards.

Finally, the Department needs to restrict public access to its information system resources. Specifically, the Division does not centrally control Web site content, and as a result, some inappropriate and sensitive details appear on its Web site. Further, some department IT resources are configured in such a way as to potentially be identified and manipulated by unauthorized external users.

Improved oversight of telecommunications consolidation and privatized network needed (see pages 23 through 30)

The Department should improve its oversight of activities related to consolidating telecommunications support services and developing a single, privatized telecommunications network. To consolidate these services, the Department and its contractor will perform several activities during a transition period that will last until March 2006, including an inventory of agency telecommunications equipment. An accurate inventory of this equipment is needed to determine an agency's telecommunications equipment needs and costs under the contract, and to also identify costs for equipment upgrades. For example, the inventory will determine which of seven categories each of the State's approximately 40,000 phones falls into. Service costs for these phones can vary as much as $40 per month, per phone.

The Department plans to rely on state agencies' staff and the contractor to develop the inventory and thus determine additional costs under the contract for equipment upgrades. To ensure an accurate inventory is conducted, the Department should either reassign personnel to work on the inventory or contract for a technology expert to oversee this process. The Department should review its current staffing assignments to determine if it can reassign personnel within the Department; if not, it should seek to reallocate funding to hire a contractor.

Additionally, the Department should work with its Information Services Division and the contractor to develop an adequate security plan for the privatized telecommunications network. The contract requires that the contractor prepare a network security plan, but the contractor's planning efforts thus far do not address all needed security features. Instead, the contractor indicated that a more complete security plan that will address all contractual requirements, such as compliance with state security standards, will be developed by late 2005. The Department should ensure that the contractor develops this plan as required.

Other pertinent information (see pages 31 through 34)

During this audit and in response to a legislative inquiry, auditors collected other pertinent information related to the billing process and costs under the telecommunications contract. Specifically:

- Billing—The contractor for the privatized telecommunications network will adopt a single billing system used by all agencies to pay for carrier services. In the past, agencies contracting these services from the Department had as much as 2 months to pay their bills. Under the contract, agencies will have 20 days to pay

their bills. The bills will reflect charges for each telephone that an agency maintains, service calls, adding or replacing equipment, local and long-distance service, and the Department's costs to oversee the contractor and operate a help desk.

- Contract costs—The contractor has agreed to provide telecommunications services for approximately $40 million per year when agencies are fully transitioned to contractor-provided services. However, to assist state agencies with the transition to privatized telecommunications services, individual agency costs for telecommunications services in fiscal years 2006 and 2007 will be held at or near their fiscal year 2004 estimated amounts as determined by a 2004 department study of state agency telecommunications spending. Because of differences in the rates that agencies have been paying for these services, the TPO indicates that if the contractor's prices were charged to each agency immediately, some agencies would significantly exceed their telecommunications budgets, while others would be well under their budgets. As a result, for fiscal years 2006 and 2007, the contractor will adjust agency bills to make them consistent with their estimated 2004 expenditures.

  After the contract was awarded, the Department updated its 2004 study and as of August 2005, estimated that agencies spent only approximately $35 million for telecommunications services in fiscal year 2005. In addition, the Department plans to charge agencies approximately $3 million annually in administrative costs to oversee the contractor, operate a help desk, and pay for other costs, such as rent for office space. As a result, the Department estimates that there will be a more than $8 million deficit in fiscal years 2006 and 2007 between agency expenditures and contract and administrative costs. The Department is exploring several options to address this deficit, including deferring $3.1 million in contractor charges for fiscal year 2006 until later fiscal years, using carrier cost savings, and proposing that agencies approach the Legislature for a supplemental budget request.

  Beginning in fiscal year 2008, the contractor's normal prices will go into effect. All agencies will be affected by this change in pricing, and some agencies may need to adjust their budgets to reflect the changes in telecommunications costs.

TABLE OF CONTENTS

• continued

TABLE OF CONTENTS

concluded ◆

INTRODUCTION & BACKGROUND

The Office of the Auditor General has conducted a performance audit of two areas within the Arizona Department of Administration—the Information Services Division and the Telecommunications Program Office—pursuant to a November 20, 2002, resolution of the Joint Legislative Audit Committee. This 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 second in a series of four reports on the Department of Administration (Department). The first audit reviewed the Department's Financial Services Division (Auditor General Report No. 05-02), and the third audit will review the Department's Human Resources Division, including the State's self-funded health insurance program. The final report will be an analysis of the 12 statutory sunset factors.

Information Services Division history, programs, and staffing

The Department of Administration's Information Services Division (Division) provides a variety of information technology services to the Department and other state agencies. In 1972, the Legislature created the Department of Administration, including a Data Processing Division, to provide for the collection, storage, and processing of data and to develop and maintain a coordinated state-wide plan for data processing and data communication systems. Laws 1996, Chapter 342, removed the state-wide planning function from the Department by transferring that responsibility to the Government Information Technology Agency (GITA). The Division currently provides information technology services and support both within the Department and to other state agencies. Services and support include activities such as mainframe and other types of data processing, creating and maintaining Web sites, and maintaining and providing technical support for both the Department's internal network and the state-wide network.

As of July 2005, the Division had 165.65 positions with 26.9 vacancies. Six filled positions report directly to the assistant director and provide administrative support,

business continuity and disaster planning, and technology planning for the Division. In addition, the Division has five sections carrying out its numerous responsibilities:

- Information Processing Center (60 filled positions)—Also known as the data center, this section operates and maintains the Department's mainframe that runs high-volume applications for the Department and approximately 50 other state agencies, such as the Arizona Health Care Cost Containment System, the Arizona Department of Transportation (ADOT), and the Department of Revenue. For example, the mainframe houses ADOT's title and registration database, which includes information such as names, addresses, social security numbers, driving records, and vehicle records. Over the course of a week, the mainframe processes more than 8 million transactions or queries on ADOT's data. The data center also maintains servers that provide computer processing for applications that process smaller numbers of transactions. For example, the Department's Human Resources Information Solution is housed on several servers in the Data Center, and the Naturopathic Physicians Board of Medical Examiners leases server space from the Department. The Data Center operates 24 hours per day, 7 days per week and charges fees to agencies for the services it provides.

- Security (10 filled positions)—This section conducts a variety of security services for the Department and other state agencies, such as providing some state employees with mainframe access, and security training for department employees. In addition to its services for the Department, according to the section's manager, if an agency requests it, the section will use software to scan the agency's networks to identify security vulnerabilities, and monitor intrusions and illegal attempts to access state agency data networks.

- Internal Technology (32.9 filled positions)—This section provides support for the Department's desktop computers and operates the Department's internal agency network. This section also tests and ensures that security patches are installed on agency desktop computers and supports the Department's Arizona Financial Information System and the Human Resources Information Solution.

- Finance and Planning (8.5 filled positions)—This section provides budget, planning, and financial analysis to the Division. The section is responsible for determining the rates that agencies are charged for services and refunding any overcharges. This section also houses the Department's 9-1-1 telecommunications services. The Department is required to administer and disburse the 9-1-1 excise tax that is deposited into the emergency telecommunication services' revolving fund, and it reviews and approves political subdivisions' payment requests for operating emergency telecommunication service systems.

- **Customer Care Services (20.35 filled positions)**—This section provides support to the Division's internal and external customers and houses the state switchboard, which answers calls to the State's central number and routes them to the appropriate person or agency.

Telecommunications services

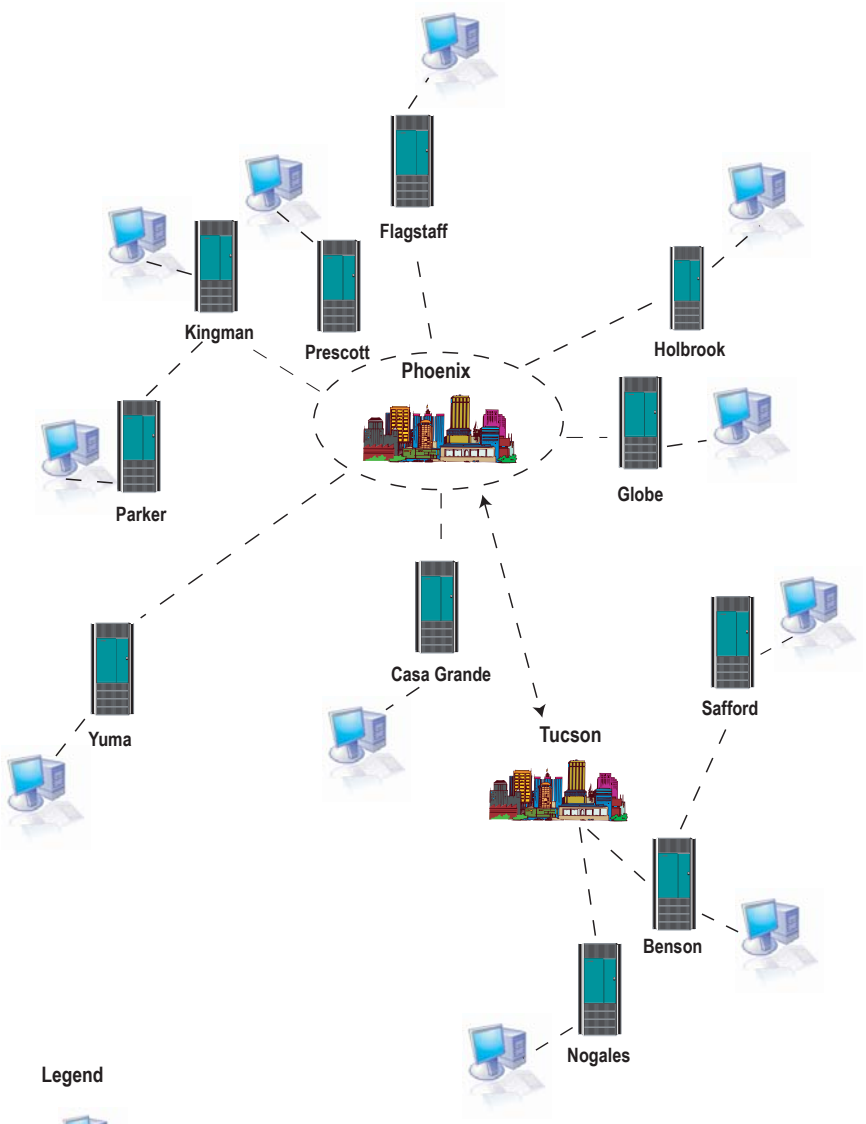
The Department also provides oversight for the State's privatized telecommunications services contractor and AZNET, the State's privatized telecommunications network. Under Laws 2003, Chapter 263, the Legislature required GITA, in consultation with the Department, to privatize telecommunications services for all executive branch agencies. In January 2005, the Department awarded a 5-year, approximately $40 million annual contract, with options for up to two 2-year extensions to a single contractor to carry out this legislative mandate. The contract provides for the following:

The Legislature has required privatization of telecommunications services for all executive branch agencies.

- **Consolidates management of telecommunications services under a single contractor**—The contractor will provide telecommunications services for all executive branch agencies. Prior to the contract, the Department's Arizona Telecommunications System (ATS) provided approximately 30 percent of voice and data telecommunications services to state agencies. Agencies separately obtained the remaining 70 percent of telecommunication services from private providers who supplied telephone maintenance, long distance, Internet, and other services. Each state agency that worked with a private contractor managed and maintained its own telecommunications network and its own equipment inventory, including when to upgrade or purchase new equipment. Under the new contract, a single contractor will provide or coordinate these services for all executive branch agencies and eventually eliminate the separate contracts that agencies have with different providers.

- **Creates a single state-wide voice and data network (AZNET)**—The same contractor is required to develop a unified state voice and data network for executive branch agencies. Many agencies used private contractors and their own staff to develop their own networks linking together agency offices throughout the State. The new contract will consolidate agencies' individual telecommunications networks into a single, privatized network called AZNET (see Figure 1, page 4). For example, Yuma has more than ten individual circuits, or transmission lines, from different agencies running to Phoenix. Those ten individual circuits could be linked together in Yuma, and one connection to Phoenix could handle all voice and data traffic from Yuma. The contractor estimates that AZNET will reduce telecommunications costs by coordinating these networks. Further, it will enable state agencies to take advantage of new

Figure 1: Planned Agency Network (AZNET)



Source: Auditor General staff analysis of the contractor's draft Network Convergence Architecture plan.

technologies that will allow them to contact each other directly over the network, reducing local and long-distance service charges.

As a result of this change to a single provider for all telecommunications services, the ATS was eliminated and the Telecommunications Program Office (TPO) was created. Specifically, by consolidating telecommunications services under a single contractor and developing a single, privatized telecommunications network, the ATS was no longer needed to provide telecommunications services. This reduced the Department's budget by approximately $13 million and eliminated 55.6 FTEs who previously worked for the ATS. Most of the FTE reduction was handled by employees transferring to the contractor or other state employment, or through attrition.

In order to oversee the contract, for fiscal year 2006, the Department received legislative approval to establish the TPO with 22 positions and a budget of nearly $2.2 million. The TPO is not part of the Information Services Division, but instead reports directly to the Department's director. TPO responsibilities include ensuring that the contractor meets the terms of the contract, ensuring contractor invoices are accurate, reviewing documents provided by the contractor, working with the Telecommunications Executive Governance Committee (TEGC) and other committees formed to facilitate the transition to the contractor, and managing the transition of agency telecommunications services to the new contractor.

The Department has housed 11 of the TPO's 22 positions in the Information Services Division to assist agencies with the privatized network. Specifically, the Department has 2 positions to staff a help desk that receives initial support calls from agencies, documents the calls, and passes the information to the contractor for resolution; 7 positions to operate the state switchboard to route calls from state agency employees and the public to other state agency employees, as well as facilitate conference calls; and 2 security investigator positions to investigate telecommunications fraud, inappropriate Internet use, and other telecommunications crimes related to the privatized network.

What Is the TEGC?

The Telecommunications Executive Governance Committee is made up of the directors or deputy directors of 13 state agencies:

Departments of:
- Administration
- Agriculture
- Commerce
- Corrections
- Economic Security
- Environmental Quality
- Game and Fish
- Public Safety
- Revenue
- Transportation
- Water Resources
- Arizona Health Care Cost Containment System
- Arizona State Retirement System

The TEGC manages and governs the TPO, oversees the contractor's performance, and reviews and approves plans for new telecommunications projects.

Operating budgets

Through fiscal year 2005, the Division's operating budget consisted primarily of monies appropriated from the Technology and Telecommunications Fund. The revenues consisted of charges assessed to state agencies for the various services the Division provides, which were deposited into the fund; legislative appropriations; grant monies; and monies from the sale of telecommunications and automation assets. The Division's revenues are intended to offset its operational costs, and the Division raises or lowers its fees to match expenditures. If revenues exceed expenditures, the Division refunds the monies to agencies. Table 1 (see page 7) illustrates the Division's actual revenues and expenditures for fiscal years 2003 through 2005. The Division received approximately $30.3 million in revenues in fiscal year 2004, and an estimated $27.4 million in revenues in fiscal year 2005. According to the Division, revenues fluctuate yearly because agencies' use of division services varies from year to year.

Effective July 1, 2005, the Legislature eliminated the Technology and Telecommunications Fund and created the Automation Fund to support the Information Services Division and the Telecommunications Fund to support the Telecommunications Program Office. For fiscal year 2006, the Automation Fund was appropriated $23.7 million, and the Telecommunications Fund was appropriated nearly $2.2 million.

Audit scope and methodology

This audit focused on the security of the various information systems for which the Department is responsible, including its internal network, state network, data center, and the single, privatized state network that is under development; and the Department's oversight of the transition to a single, private provider for telecommunications services and the privatized network. The report presents findings and recommendations in the following areas:

- The Department should take several steps to improve security on various information systems, including its internal network and the state network, which contain critical applications and data, by centralizing responsibility for security.

- The TPO needs to adequately oversee the process for conducting an inventory of state agency telecommunications equipment, and ensure that the contractor develops an appropriate security plan for the privatized telecommunications network.

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

	2003 (Actual)	2004 (Actual)	2005 (Estimated)
Revenues:			
Charges for services	$34,917	$30,265	$27,385
Expenditures and transfers:			
Personal services and employee-related	9,598	10,050	9,968
Professional and outside services	1,233	1,698	1,513
Travel	74	65	52
Other operating	7,590	7,404	5,152
Equipment	11,186	10,642	8,492
Allocated costs	267	276	268
Total expenditures	29,948	30,135	25,445
Net operating transfers out	24	22	14
Total expenditures and operating transfers	29,972	30,157	25,459
Excess of revenues over expenditures and operating transfers	$ 4,945	$ 108	$ 1,926

1 Represents the financial activity of the Technology and Telecommunications Fund. Beginning in fiscal year 2006, the fund was divided into two new funds, the Automation Operations Fund and the Telecommunications Fund, in accordance with Laws 2005, First Regular Session, Chapter 301. The Automation Operations Fund will be used to pay the costs of any automation applications the Department implements, and the Telecommunications Fund will be used to pay for costs incurred in operating the Telecommunications Program Office. The Department reports that approximately $11.1, $10.2, and $7.8 million of the expenditures presented above for 2003, 2004, and 2005, respectively, were for activities that the Telecommunications Program Office will be performing.

Source: Auditor General staff analysis of financial information provided by the Department of Administration from its Arizona Financial Information System for the years ended June 30, 2003 and 2004, and department-prepared estimates for the year ended June 30, 2005. (Actual information was not available at the time of this report.)

The report also presents other pertinent information regarding how the contractor will bill agencies for telecommunication services and the potential impact of contractor charges for these services on state agencies' telecommunications budgets beginning in fiscal year 2008.

Auditors used various methods to study the issues addressed in this report, including interviewing department, division, TPO, and other state agency officials and staff, and reviewing the Division's and the TPO's financial information and statutes. Auditors also used the following specific methods:

- To evaluate the effectiveness and sufficiency of the Division's information system security, auditors reviewed the Division's policies and procedures, including those related to security awareness training and risk analysis, and also toured the data center. To test department security procedures, auditors reviewed

division security patch management logs and inspected a sample of 12 department computers for the presence of security updates, virus protection, and nonbusiness-related software. In addition, auditors inspected 20 desktops, laptops, and servers at State Surplus Property to ensure that the hard drives had been properly erased. To measure the effectiveness of the Division's security practices, auditors compared the Department's security practices to two resources on IT controls and security and to GITA's Statewide Standards for IT security.[1,2,3] To determine IT resource configuration practices in other state agencies, auditors interviewed security managers from the Departments of Economic Security and Public Safety. To identify past evaluations of the Division's IT security practices and determine the Division's response to these evaluations, auditors reviewed scans of the Department's network from 2004 and a consultant's IT security assessment of the Division from 2001. Finally, to review access controls, auditors analyzed reports and data from the mainframe security system, the Human Resources Information Solution system, and the Department's local area network.

- To evaluate the Department's oversight of the transition to a single, private provider for telecommunications services, auditors identified the contract's intent and requirements by reviewing the state agency telecommunications privatization services' contract statement of work, the offerer's proposal, other contract documents, and GITA's 2003 Telecommunications Roadmap. To identify and evaluate the Department's process for carrying out this intent, auditors reviewed draft documents related to the transition process, such as the draft security architecture plan; and convergence and transition plans from the Department's telecommunications contractor; and inventory records sheets and draft proposals for using state monies for agency projects; attended a meeting of the Telecommunications Executive Governance Committee and other telecommunications-related committees; and compared the contractor's draft security plan to standards and best practices from the National Institute for Standards and Technology and to guidelines published in the IT Governance Institute's Control Objectives for Information and Related Technology.[4,5]

1 U.S. Department of Commerce. Technology Administration. *An Introduction to Computer Security: The NIST handbook*. NIST Special Publication 800-12. Gaithersburg, MD: National Institute of Standards and Technology, Oct. 1995.

2 U.S. Government Accountability Office. *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6). Washington, D.C.: U.S. Government Accountability Office, Jan. 1999.

3 U.S. Department of Commerce. Technology Administration. *Guideline on Network Security Testing*. NIST Special Publication 800-42. Gaithersburg, MD: National Institute of Standards and Technology, Oct. 2003.

4 COBIT Steering Committee. *COBIT: Governance, Control, and Audit for Information and Related Technology.* 3rd ed. Rolling Meadows, IL: IT Governance Institute, 2000.

5 U.S. Department of Commerce Technology Administration. *Guide for Developing Security Plans for Information Technology Systems.* NIST Special Publication 800-18. Gaithersburg, MD: National Institute of Standards and Technology, 1998.

- To gather information related to the contractor's billing practices and service charges, auditors reviewed the Department's planning documents; the Department's 2004 Total Cost of Ownership study and department draft documents updating the study for 2005; relevant portions of the contractor's proposals, such as its pricing workbook; and documents related to the transition to the new, single provider for telecommunications services, including a contractor's telecommunications bill for April 2005.

- To gather information for the Introduction and Background section, auditors reviewed unaudited information from the Department's and GITA's November 2002 report to the Joint Legislative Budget Committee on the Arizona Telecommunications Service, the Joint Legislative Budget Committee fiscal year 2006 appropriations report, the statement of work from the telecommunications contract, the July 2005 Arizona Department of Administration personnel listing, and other information provided by the Division.

The audit was conducted in accordance with government auditing standards.

The Auditor General and staff express appreciation to the director of the Department of Administration and the staff of the Information Services Division and the Telecommunications Program Office for their cooperation and assistance throughout the audit.

FINDING 1

Several actions needed to improve information security

The Department should take a variety of actions to further ensure the security of the State's information systems and the data stored on them. The Department maintains and secures some of the State's most sensitive IT resources and data, including driver's license, vehicle registration, and medical information. While the Department performs some security functions well, it does not perform other important security functions, which increases these systems' vulnerability to unauthorized entry and potential manipulation. To improve security, the Department should emphasize security planning by designating someone to be responsible for the overall security effort of its internal network and the data center, and by including more security requirements in the intergovernmental service agreements with state agencies that use the data center. In addition, the Department should request authority from the Legislature to enforce security requirements for the state-wide network, or AZNET. Finally, the Department needs to improve its own network security by taking steps to keep sensitive information off the Information Services Division Web site and changing how it sets up IT devices.

Security of information systems important

As computer technology has advanced, agencies have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Adequate security of information and the systems that process it is a fundamental management responsibility. Information security includes issues such as restricting and allowing access to systems and applications, setting up hardware and software to ensure appropriate access, securing buildings and rooms that house critical hardware and software, and conducting background checks of the personnel who work directly with critical information systems. Nationally, government officials are increasingly concerned about attacks from individuals and groups with malicious intent, which appear to be

increasing. For example, the number of reported incidents handled by Carnegie-Mellon University's CERT Coordination Center increased from 21,756 in 2000 to 137,529 in 2003.[1]

Network—A group of two or more computers linked together by cables, telecommunications lines, or radio waves.

The Department is responsible for the security of information resources and the data that resides on them. The Department maintains an internal network and also operates and maintains the data center, which runs computer applications and serves as a data repository for its own systems and those of many state agencies. For example, the data center handles both the Department's own Human Resources Information Solution, which contains data associated with payroll, personnel, employee benefits, and other associated functions for state employees, and the Arizona Department of Transportation's Motor Vehicle Division data that includes names, addresses, social security numbers, driving records, and vehicle records.

Department performs some security functions well, but lacks coordinated security program

While the Department performs some security functions well, it lacks a comprehensive and coordinated security program with several essential features. The Department has adequately performed some security functions, such as ensuring that its desktop computers have up-to-date virus protection and security updates. However, the Department has not performed several important security functions, such as conducting network scans and tests, and it has failed to develop comprehensive policies and provide ongoing security training.

Department performs some security functions well—As shown in Table 2 (see page 13), the Department conducts some important activities that help to ensure IT resources' security. For example, auditors examined 12 desktop computers, along with the Department's security update logs and alerts, and found that these computers had current security updates and virus protection. In addition, auditors found that data on all 20 department computers and servers that were at the State's Surplus Property in May 2005 were erased or destroyed according to Surplus Property requirements. The Department also adequately restricts personnel access to the data center and requires sufficient password protection for both its desktop computers and the mainframe.

The Department appropriately disposes of surplus hardware equipment.

Other security functions not performed well—While the Department takes some steps to provide a basic level of protection, it does not perform many security functions that national standards dictate. The Department needs to take additional steps to more fully guard against the kinds of intrusions attempted by hackers or

1 Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.

Table 2: Security Functions the Department Performs Well

Function	Audit Results
Desktop computer security	• Security and virus protection software was current on all 12 department computers that auditors tested.
Data Center physical security	• Access was controlled by electronic keycards. • Electronic keycards were issued and collected from terminated employees promptly.
User access (mainframe system)	• Password length was sufficient. • Employees changed passwords every 30 days. • All user IDs were unique.
User access (desktop computers)	• Employees changed passwords at appropriate intervals.
Disposed-of computers and servers	• Data on all 20 computers and servers present at Surplus Property in May 2005 was erased according to policy.

Source: Auditor General staff analysis of mainframe system and network user account parameters and Auditor General staff inspection of data center, desktop computers, and disposed-of computers and servers.

others seeking to gain inappropriate access to sensitive data and systems. Specifically:

- **Network scanning inconsistent**—The Department has performed some network scanning in the past, but it does not perform regular monitoring and testing of its internal network in order to identify and address potential vulnerabilities. By scanning the network, the Department could identify potential vulnerabilities, such as any unauthorized computers connected to the network and any unauthorized services on the network. As illustrated in Table 3 (see page 14), the National Institute of Standards and Technology (NIST) recommends several network scans and tests that should be conducted on a regular basis to help identify potential weaknesses and vulnerabilities that expose networks to increased risk of unauthorized access.[1] For example, NIST recommends that organizations perform a network scan continuously to quarterly for systems that provide security such as firewalls, and semi-annually for low-risk systems such as those that a firewall protects. However, according to the Department, the last complete scan of the Department's network was done in 2001, while in 2004, the Department contracted for a scan of only the Human Resources Information Solution application. This lack of

Firewall—A system designed to prevent unauthorized access to or from a private network. It is considered the first line of defense in protecting private information.

[1] The National Institute of Standards and Technology issues information security standards for all federal agency operations except national security systems.

Table 3: Network Testing and Recommended Frequency

Test Type and Benefits	Recommended Frequency[1]
Network scanning • Lists the network structure, computers, and associated software • Identifies unauthorized computers connected to a network • Identifies public connections to computers • Identifies unauthorized services	Continuously to semiannually
Vulnerability scanning • Lists the network structure, computers, and associated software • Identifies a target set of computers to focus vulnerability analysis • Identifies potential vulnerabilities on the target set • Validates that operating systems and major applications have up-to-date security and software	Bimonthly to semiannually
Penetration testing • Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred • Tests IT staff's response to perceived security incidents and its knowledge and implementation of the organization's security policy and system's security requirements	Annually

[1] Frequency depends on the system's sensitivity.

Source: U.S. Department of Commerce. Technology Administration. *Guideline on Network Security Testing*. NIST Special Publication 800-42. Gaithersburg, MD: National Institute of Standards and Technology, Oct. 2003.

monitoring and testing increases the risk of network intrusion, which could allow a hacker to gain access to sensitive systems and data.

- Independent security assessments not obtained—The Department has not obtained an independent security assessment since 2001 and does not have a policy defining the frequency and under what circumstances such assessments should be obtained. According to NIST, an organization should obtain an independent review of its security controls at least once every 3 years and more frequently for critical systems. The Department last obtained such an assessment in 2001, when it paid more than $310,000 to a private contractor to conduct a security assessment that looked at areas such as the Department's security policies and procedures, mainframe security, and network vulnerabilities. However, the Department has not since contracted for an independent security assessment of its operations, even though that

The Department has not performed a complete network scan since 2001.

assessment identified many concerns with the Department's internal and statewide networks. For example, in the 2001 assessment, reviewers found that the Department was running an unsecure version of an operating system and that many computers had inappropriate open public connections.

- **Risk assessments not performed**—While the Department has a policy detailing how to conduct a risk assessment, it has not performed a comprehensive risk assessment. A risk assessment identifies and evaluates a particular potential vulnerability's risk and its potential impact on information systems to determine the extent of a potential threat and appropriate actions to mitigate the threat. Risk assessments should be performed and documented on a regular basis, at least every 3 years or whenever systems, facilities, or other conditions change. Risk assessments consider data sensitivity, the need for integrity, and the range of risks that might affect an entity's systems and data. These assessments would help the Department determine how best to complete other oversight functions, such as network scanning. According to a department official, it has not conducted risk assessments because it was not considered a high priority.

The Department has not performed a comprehensive risk assessment.

- **Corrective actions not tracked, monitored, and implemented effectively**—When significant weaknesses are identified, the related risks should be reassessed, appropriate corrective actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. However, the Department has not created a formal follow-up process to ensure that identified weaknesses are tracked and effective corrective actions taken. Failure to take effective corrective actions results in the Department's continuing to leave both its own and state information resources vulnerable. For example, the Department has not taken actions to address many of the weaknesses identified in the 2001 security assessment, such as sensitive information being made available on its Web site.

Security policies and training inadequate—The Department does not ensure that staff have the tools to understand security requirements. Specifically:

- **Security policies and procedures not adequate**—The Department lacks comprehensive security policies and procedures, and the few it does have do not provide sufficient detail or have not been updated since 2000. For example, the Department does not have a policy regarding the use of wireless connections to prevent unauthorized access to internal networks even though wireless communications are being used within the Department. Failure to define such standards increases the risk of providing a pathway for unauthorized users to access a network. According to GITA, state agencies are responsible for creating any necessary policies and procedures in order to establish a security program. Additionally, the Department's 2001 comprehensive security assessment, for which the Department contracted, found its security policies and procedures lacking. Therefore, the assessment

recommended that the Department create more detailed policies and procedures, and that the department director sign all security policies and procedures in order to ensure central management approval and buy-off.

- Ongoing security awareness training not conducted—The Department does not provide its employees with ongoing security awareness training. Training that informs department employees of necessary security policies, such as not revealing one's password, should be conducted at initial hire and on an ongoing basis. Although GITA and department policy requires both initial and annual training, department employees currently receive training only at the time of initial hire. Failure to provide ongoing security awareness and training to employees increases the risk that users could misuse data or resources, or that unauthorized personnel could gain access to data or resources.

Department should implement coordinated information security program

In order to ensure that a coordinated information security program is in place, the Department should take two steps. First, the Department should establish a position responsible for all security functions so that security is better emphasized within the Department. Second, it should enhance its interagency service agreements with agencies that use the data center to better define each party's responsibilities for information security. In addition, the Department should request the statutory authority to enforce minimum standards for AZNET users.

Security functions should be centralized—To ensure that the Department has a coordinated security program that includes the features described above and that it meets its responsibility for securing its internal network and the data center, the Department should establish a centralized and comprehensive security program. Although the Department has a state-wide security manager, this position does not have the responsibility to ensure compliance with accepted security standards or that the Department performs the necessary activities to help ensure the security of the networks, systems, and data for which it is responsible. Instead, this position responds to and attempts to address individual security questions and problems as they arise, such as stopping corrupted computers from sending out e-mails contaminated with a virus. However, the U.S. Government Accountability Office noted in its study of organizations with leading information security practices that these organizations had established centralized security responsibilities.[1] By doing so, the organizations ensure that they had adequate security policies and that these policies address security risks on an ongoing basis.

[1] U.S. Government Accountability Office. *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6). Washington, D.C.: GAO, Jan. 1999.

Therefore, the Department should assign one of its positions, such as the state-wide security manager, the responsibility for security of the Department's internal information resources and network, as well as the data center. This position should be responsible for administering a comprehensive security program that would address:

The Department should assign a person to oversee a comprehensive security program.

- Developing a policy governing network scanning, monitoring, and testing, including how it should be done, the frequency, and follow-up procedures;

- Obtaining an independent security assessment at least every 3 years and developing policies regarding under what circumstances it would obtain an independent assessment more frequently;

- Conducting risk assessments on a regular basis, at least every 3 years and as needed when systems, facilities, or other conditions change;

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

- Developing adequate security policies and procedures and ensuring that they include sufficient detail; and

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

The Department has begun to address some of these specific items. For example, it plans to develop recommended policies and procedures for network scanning and monitoring and obtaining independent security assessments, to begin performing scans of its internal network by September 2005 and conducting risk assessments by November 2005, and establishing ongoing training by September 2005. However, the Department should ensure that it has assigned the responsibility for ensuring that these activities are completed to one of its positions. The Department should also determine if it needs additional staff, funding, and technical resources to perform these additional security duties, and if so, assess whether it could reassign existing staff and resources or take other steps, as appropriate, to seek additional staff and resources.

Security responsibilities should be defined in interagency service agreements—In order to adequately protect the information systems maintained in the data center, the Department should enhance its interagency service agreements with state agencies that use the data center. While the Department has agreements with these agencies, these agreements lack specific details regarding responsibilities for system and application security. For example, one agreement stated that the Department would provide system security support and the agency would provide security for applications, but it did not provide additional detail.

According to GITA policy, agencies may develop agreements to help ensure sufficient and acceptable security protection for all participating agencies. Therefore, the Department should develop agreements that define minimum security standards, how the Department will monitor compliance with the policies and procedures, and how standards will be enforced. The agreements should also delineate the Department's responsibility to provide access to the state data center and the state agency's responsibility to meet specific, minimum security requirements. Further, the agreements should define the circumstances under which a state agency may face actions and the actions the Department may take. For example, the Department could restrict a state agency's access to the data center for failure to comply with those security requirements. This would allow the Department to better ensure that vulnerabilities or corrupted computers in one agency do not compromise the systems of other agencies that use the data center. According to the Department, beginning in August 2005, more detailed security requirements will be included in these agreements as the current agreements expire.

Statutory authority needed to ensure sufficient security over AZNET—The Department should request statutory authority from the Legislature to enforce the specific minimum security requirements state agencies must follow related to AZNET. The Department's enabling statutes charged it to "provide for an efficient and coordinated utilization of automation equipment, techniques and personnel to achieve optimum effectiveness … and productivity in the … security of information." However, when GITA was created in 1996, this wording was removed from the Department's statutes, and GITA was given statutory authority to issue state-wide security standards. However, GITA was not given operational authority to enforce its standards. This resulted in a lack of statutory authority to enforce security standards for information systems shared by state agencies. Specifically, although GITA has the responsibility for setting state-wide security standards and is considering designating a staff member to serve as the State's chief security officer, its functions do not include the daily oversight of AZNET that would be necessary to enforce its standards.

If one state agency does not sufficiently secure its resources, it potentially exposes the other state agencies using a shared resource, such as AZNET, to an increased risk of data loss or hacker intrusion. Therefore, the Department should ask the Legislature to amend A.R.S. §41-712 to give the Department statutory authority to enforce security requirements on state agencies using AZNET. This authority should permit the Department to ensure that agencies using AZNET meet security standards, as defined by GITA. The Department's responsibilities would extend to implementing GITA policies and standards and working with GITA to develop operational minimum security standards with regard to AZNET. For example, GITA requires that state agencies review, test, and audit firewall policies, but is not specific about how frequently this should occur. The Department would need to work with GITA to develop a policy for AZNET users to follow regarding the minimum frequency of such reviews and how to deal with agencies that fail to effectively implement

firewalls. In addition, the Department would need to ensure that any authority to enforce security standards is included in its comprehensive security program.

Department needs to better limit access to its information system resources

The Department has not implemented sufficient measures to restrict public access to its information system resources. This could potentially allow unauthorized personnel to access sensitive information. Specifically:

- Sensitive information on Web site—The Information Services Division does not centrally control the content on its Web site, and as a result, sensitive information is available on the Internet. The Division has been aware of this problem since the 2001 comprehensive security assessment recommended that it remove such material from its Web site. However, the Division has continued to maintain sensitive information on its Web site. During the audit, the Division began to review the content available over the Internet and to draft a policy that would govern Web content. The Division should ensure that the policy requires central review and approval of Web site content to ensure that sensitive information is not available to the public. Additionally, the Division should ensure that sensitive information is removed from its Web site, and instead maintain any sensitive information in a more secure environment, such as the Department's internal network, which is not available to the public.

The Division has kept information that could compromise the security of sensitive data and systems on its Web site.

- Poor configuration of devices—GITA standards require that internetworking devices such as routers and switches, and shared platforms such as servers, be set up in a way that limits potential access by unauthorized external users. However, department devices are configured in a manner that potentially allows them to be identified and manipulated by unauthorized external users. GITA standards define how these devices should be set up to guard against such external risks, and the Department should configure its resources to comply with those standards.

Recommendations:

1. The Department should designate a central authority, such as its state-wide security manager, with the responsibility for developing a comprehensive security program for the Department's internal information resources and network, as well as the data center. The Department should then ensure that the program addresses:

    a. Developing a policy governing network scanning, monitoring, and testing, including how it should be done, the frequency, and follow-up procedures to correct identified vulnerabilities;

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

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

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

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

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

2. The Department should determine if it needs additional staff, funding, and technical resources to perform additional security duties, and if so, assess whether it could reassign existing staff and resources or take other steps, as appropriate, to seek additional staff and resources.

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

4. The Department should enhance its interagency service agreements with state agencies that use the data center to define the Department's and the agencies' security responsibilities. The agreements should:

    a. Delineate the Department's responsibility to provide access to the state data center and the state agency's responsibility to meet specific, minimum security requirements; and

    b. Define the circumstances under which a state agency may face actions for failure to comply with those security requirements, and the actions the Department can take to better ensure that corrupted systems in one agency do not compromise other agencies' systems and data.

5. The Information Services Division should better ensure that it does not publish sensitive information on its Web site by developing a policy requiring central review and approval of Web site content. The Division should also review current Web content to ensure that sensitive information has not remained on its Web site, and instead maintain any sensitive information in a more secure environment, such as the Department's internal network, which is not available to the public.

6. The Department should configure its information system resources, such as routers, switches, and servers, to comply with GITA standards to provide greater safety from external threats.

FINDING 2

Improved oversight of telecommunications consolidation and privatized network needed

The Department should improve its oversight of two activities related to consolidating telecommunications support services and developing a single, privatized telecommunications network. To consolidate these services, the Department and its contractor will perform several activities, including addressing existing telecommunications contracts and conducting an inventory of agency telecommunications equipment. However, the inventory process is being conducted by state agency staff and the contractor without sufficient department oversight. Given the potential impact of this process on additional costs to the State, the Department should reassign staff to oversee the inventory process, or, if necessary, reallocate existing funding or take other steps, as appropriate, to hire a private contractor to oversee the process. Additionally, to protect the network, the Department should work with its Information Services Division to ensure that the contractor develops an adequate security plan that meets the contract requirements and contains all the features of an appropriate security plan.

Agencies will phase in consolidated telecommunications management

In order to consolidate the management of state agency telecommunication services under one contractor, the Department and its contractor need to perform several activities. These include a phased approach to consolidating the management of all executive branch agency telecommunications services under a single contractor who will provide telecommunications, equipment maintenance, long distance, and other telecommunications services. Prior to the contract, state agencies independently obtained these services from the Department or other contractors.

When will agencies be transitioned?

Phase 1: According to the Department, Phase 1 was substantially completed by the beginning of July 2005. During that time, the contractor began offering services and billing agencies that previously had telecommunications services provided by the Department's Arizona Telecommunications System. These agencies include the Department of Education, the Arizona State Parks Board, and the Department of Commerce.

Phase 2: The following agencies that used other contractors for telecommunications services are scheduled for transition beginning in August 2005. The Department expects all agencies to be transitioned by March 2006:

- August 2005—Arizona Health Care Cost Containment System, the Departments of Revenue, Game and Fish, and Environmental Quality, and the Arizona School for the Deaf and Blind.
- September 2005—The Department of Transportation and the Department of Corrections.
- October 2005—The Department of Economic Security.
- November 2005—The Department of Education, the Arizona State Retirement System, and Boards and Commissions.
- December 2005—The Department of Public Safety.
- January 2006—Remaining state agencies.

The Arizona Telecommunications System provided about 30 percent of the voice and data services provided to the State.

The contractor will transition agencies to a single provider for telecommunications services in two phases. With the completion of Phase 1, the contractor began offering services and billing those agencies that previously had telecommunications services supplied by the Department's Arizona Telecommunications System (ATS). According to department records, this accounted for approximately 30 percent of voice and data telecommunications services provided to state agencies. Agencies separately obtained the remaining 70 percent of telecommunication services. During the summer of 2005, the contractor and the Department evaluated the results of the Phase 1 transition, updated transition plans for Phase 2, and began transitioning the remaining state agencies to the contractor providing telecommunications services.

This transition to a consolidated telecommunications management under the contractor consists of several additional changes to each agency's operations. As each agency is transitioned, several processes will be carried out, including:

- Implementing contractor management systems—The contractor will implement management processes and software systems necessary to provide telecommunications services to each agency. The contractor plans to implement an electronic billing system within each agency, install a system linking the agency to a help desk used for requesting telecommunications support or services, and implement an asset inventory management system that records and tracks the telecommunications equipment the agency owns.

- Resolving current agency telecommunications services contracts—The contractor will work with the Department's Telecommunications Program Office (TPO) and each agency to review existing telecommunications services contracts. This will involve a review of each contract to determine whether the contractor will manage the contract itself on behalf of the agency, terminate it and provide the services itself, or allow the State to retain and continue to pay the contract. The TPO has assigned staff to assist in this process and work with the agency and the contractor to identify and review the agency's existing contracts. The contractor intends to terminate most existing agency contracts for telecommunications maintenance and support, and transfer the work to itself or its subcontractors. The Department and the contractor believe there will be little difficulty in replacing contracts, according to the TPO staff member assigned to help in this process, because the TPO has encouraged agencies to adopt short-term contracts with their current vendors. The contractor indicates that it will retain contracts where it is appropriate to do so; for example, where there is a substantial termination penalty.

- Performing an inventory—The contractor, with the help of agency staff, will conduct a physical inventory of each agency's telecommunication assets. As of July 2005, a department official indicated that the physical inventory process was complete for the agencies transitioned to the single provider as part of Phase 1. As each agency transitions during Phase 2, its telecommunications equipment will be inventoried. An accurate, state-wide inventory of this equipment does not currently exist, and one is needed to determine precisely what equipment exists at state agencies and whether it is obsolete. While the Department estimated that there were approximately 40,000 telephone sets state-wide prior to entering into the contract, the contract requires a precise counting of state telecommunications assets covered under the contract. Therefore, the Department plans to request that agencies document their telecommunications equipment, identifying the manufacturer's version of the equipment; location of telephones, voice, and wide-area network telephone circuits; and telecommunications software applications. The contractor will attempt to confirm these records using a combination of site visits and diagnostic tools, and record the assets in a centralized database.

An accurate, state-wide inventory of telecommunications equipment is needed to assess agencies' equipment needs.

Department should oversee inventory process

The Department should assign a technology expert to oversee the process of identifying and categorizing state telecommunications equipment. An accurate inventory of this equipment is needed to determine an agency's telecommunications equipment needs and costs under the contract, and to identify costs for equipment upgrades. However, although the performance and outcome of the inventory will have a significant effect on the revenues that the contractor can earn under the contract, the Department has not dedicated sufficient resources to oversee this process. Instead, it plans to rely on agency staff and the contractor to develop the inventory and thus determine additional costs under the contract for equipment upgrades. Therefore, the Department should review the TPO's current staffing assignments and reassign staff to this function, or alternatively seek additional resources from the Legislature or a private contractor to adequately oversee the inventory process.

Inventory process can impact contract costs—The performance and outcome of the inventory of state telecommunications equipment will have a significant effect on the revenues that the contractor can earn under the contract. Specifically, the inventory process will help determine each agency's flat fee for telephone service. Under the contract, telephones are divided into seven categories and associated service costs depending on the features of the phone. For example, the contractor's fees to provide telecommunications service for a single-line telephone are approximately $40 less than fees for a multi-button phone with a display that might be used by a call center supervisor. Based on the Department's initial estimate of 40,000 telephones state-wide, determining the actual number and types of telephones that the network will serve will significantly affect the contractor's revenues.

Additionally, an accurate inventory of current telecommunications equipment is necessary to determine whether this equipment can be successfully integrated into the network. The inventory process will determine if agency telecommunications equipment that connects to the network, such as routers or other equipment, such as PBX or key systems, will need to be upgraded. The contract specifies that if this equipment is within two versions of the manufacturer's most recent version of the equipment, the contractor will upgrade this equipment at no additional charge. However, if the equipment is no longer supported by the manufacturer, the state agency will need to purchase the upgrade separately since it would not be covered under the contract. Therefore, not only will the contractor assist in developing an accurate inventory, it will determine which assets that must be upgraded are already covered under the contract and which assets that must be upgraded are not covered, thus identifying potential additional costs.

What are routers, PBX, and key systems?

A **router** is a device that forwards data along networks.

PBX and **key systems** are private telephone networks used within an enterprise that route telephone calls between users and allow for the sharing of a certain number of outside lines for making calls external to the system.

Finally, a correct inventory of assets is important because the process can allow the contractor to adjust its contract prices. Specifically, because there was insufficient information available before the contract was signed, the contract allows the State or the contractor to revise the scope or prices in the contract once each year. At the end of the contract's first year, if the inventory is significantly different from the original estimates, the contractor can negotiate with the State to adjust its prices.

Department has not dedicated staff to oversee the inventory process—Despite the potentially significant impact of the inventory process, the Department has not dedicated personnel to oversee this process. Specifically, the Department does not have on its staff an expert in the technologies being inventoried and evaluated to assist agencies with identifying their current equipment, ensuring equipment is properly identified and categorized, and overseeing the contractor in this process. Even though the Department has dedicated staff to oversee other transition activities, such as transferring current agency telecommunications contracts to the new vendor or overseeing billing, it has not done so for the inventory process. While the Department originally planned to hire an expert in telecommunications technology to assist in the inventory process, according to an agency official, the Department has not obtained this expertise due to budget and staffing constraints. Instead, the Department continues to rely on agencies and the contractor to develop accurate inventories of their telecommunications equipment. A department official also indicated that two staff will be available to assist agencies and answer their questions. However, these staff have other responsibilities and may not have the necessary expertise or time to actually oversee the inventory process.

The Department needs to oversee the inventory process.

While the Department believes this process mitigates the concern regarding the inventory process, because of the importance of this inventory process and its effect on contract costs, the Department should assign a technology expert to oversee this process. Specifically, the Department should review the TPO's current staffing assignments to determine if it can reassign personnel within the TPO to review Phase 1 inventories and oversee Phase 2 inventories. The TPO employs 22 full-time staff, including contract managers and financial analysts. The Department should review these staff members' skills to determine if they have sufficient expertise in telecommunications technology to appropriately oversee the inventory process. If the Department determines it is more appropriate to obtain additional staff or expertise, it should reallocate existing funding or take other steps, as appropriate, to hire a private contractor to assist in overseeing the inventory process.

Department should improve oversight of network security

To adequately protect the telecommunications network, the Department should ensure that the contractor develops an adequate security plan that fulfills all contract

requirements and contains all appropriate security plan features. The current plan being developed by the contractor and the Department does not include every contractually required feature. Additionally, the Department should ensure that the security plan adequately addresses other important features, including processes for regularly monitoring the network and enforcing compliance with security standards.

Network security is critical since agencies will process and transmit vital and confidential information on the network.

Network security plan does not address all contract requirements—The contractor has not developed an adequate security plan as required by the contract. The contract requires the contractor to develop a security plan that addresses security responsibilities for the state-wide network. These include managing firewalls that protect the State's systems that connect to the Internet and operating equipment that detects and reports intrusions on the network. Ensuring adequate security for this network is important since agencies will use it to process and transmit vital and sometimes confidential information. Developing a security plan also helps to ensure that the contractor will take the necessary steps to assure the security of the network and that these steps are consistent with the Information Services Division's security framework and policies and procedures.

The contractor's planning efforts thus far do not include all of the contractually required features. As a preliminary step to creating the plan, the contractor submitted a "centralized security plan" in April 2005. This plan covers high-level security issues such as the contractor's philosophy of how security will be carried out and high-level design features, such as the security services the contractor offers. According to department staff, once the Department accepts this plan, the contractor plans to meet with representatives of state agencies to complete a more detailed network security plan, which is estimated to be completed by late 2005. While the centralized security plan covers some detailed information on the equipment used, the plan does not include features called for in the original contract as part of an overall network security plan. Specifically:

- Plan does not include Security Service Level Agreements (SLAs)—According to the contract, the network security plan should include SLAs addressing security concerns and issues. An SLA details the contractor's responsibilities and the penalties assessed to contractors if they violate any element of the SLA. For example, an SLA might specify penalties to the contractor if the network is unavailable to state users for more than a specified amount of time each month. While the contract calls for the plan to include security SLAs, the architecture plan does not include any SLAs detailing contractor responsibilities, or penalties in the event the contractor fails to prevent data concerning the public or agency operations from being stolen, deleted, or altered.

- Plan does not address state-wide security standards—The contract requires that the network security plan comply with the Government Information Technology Agency's (GITA's) standards for information technology security. However, auditors compared the centralized security plan to GITA's standards

and determined that the plan does not address some of these standards. For example, this plan does not address developing a process, including necessary controls, to protect the network through ongoing computer program updates, and does not call for proactively conducting periodic tests to identify and correct network vulnerabilities.

- **Plan does not include periodic security awareness and training**—The contract requires the network security plan to include periodic network security awareness and training for agency personnel. However, the centralized security plan does not address this issue. This training, which the contractor is required to provide, is supposed to educate agency personnel on issues that affect security vulnerability.

Department should ensure an adequate security plan is developed—The Department, working with the contractor, has taken steps to begin incorporating some of the missing elements. Specifically, after reviewing the plan and meeting with auditors, the Department began working with the contractor to incorporate security SLAs and to address state-wide security standards and training in a complete security plan that will be developed by late 2005, before the first agency begins operations on the network. Moreover, the Department should work with its Information Services Division to ensure that the revised plan appropriately addresses the contractual requirements and includes any monitoring, testing, or compliance policies or procedures that the Division develops.

The network security plan should incorporate national guidelines and benchmarks for effective network security.

In ensuring this plan's adequacy, the Department should also determine if it meets appropriate national standards and benchmarks for what constitutes effective network security management. For example, an internationally recognized set of information technology guidelines notes that a successful security plan should define clear security monitoring and enforcement processes, such as how potential security breaches or other incidents will be identified, reported, and monitored.[1] Moreover, according to NIST, federal security plans should include analyses of the sensitivity of the information that the system handles, management controls in place to protect the system, the systems' threats and vulnerabilities, and a plan for independent review of the system's security. NIST also recommends that organizations get independent advice and comment on the security plan from individuals within or outside of the organization, such as the organization's IT security manager.[2] Therefore, the Department should work with its Information Services Division to ensure that the contractor's security plan appropriately includes these relevant aspects of a good IT security plan. Finally, the Department should develop a process for monitoring the contractors and work with them to annually update the security plan to reflect any changes in state-wide network and security standards.

1 COBIT Steering Committee. COBIT: Governance, Control and Audit for Information and Related Technology, *Management Guidelines, Critical Success Factors: DS5—Ensure Systems Security.* 3rd ed. Rolling Meadows, IL: IT Governance Institute, 2000.

2 U.S. Dept. of Commerce, Technology Administration. *Guide for Developing Security Plans for Information Technology Systems.* NIST Special Publication 800-18. Gaithersburg, MD: National Institute of Standards and Technology, 1998.

Recommendations:

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

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

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

2. The Department should ensure that the contractor develops an adequate network security plan that includes the following:

    a. Requirements stipulated by the contract, including security service level agreements, compliance with GITA's state-wide security standards, and periodic security awareness and training for agency personnel; and

    b. Other relevant aspects of an appropriate information technology security plan, such as defining clear security monitoring and enforcement processes, and how potential security breaches or other incidents will be identified, reported, and monitored.

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

OTHER PERTINENT INFORMATION

During this audit and in response to a legislative inquiry, auditors collected other pertinent information related to the billing process and costs under the telecommunications contract.

Contractor billing system will bring changes

The contractor for the privatized telecommunications network will employ a different billing system from the one used by Arizona Telecommunications Services (ATS) to pay for carrier services. In the past, carriers invoiced ATS, and ATS immediately paid them. Thirty days later, ATS added carrier charges to its monthly agency bills, giving agencies an additional 30 days to pay their bills. As a result, agencies were paying for carrier services up to 2 months after ATS received the invoice. In contrast, the contractor will take 10 days to process the bill then pass the carrier charges directly to the agency, giving the agencies 20 days to pay. Because changing from ATS to the contractor involves removing 30 days from the billing process, during the first year, the contractor will create an extra 13th-month bill. The monthly bill will contain charges for the five following basic services:

- **Per-Seat Charges**—The contractor will introduce "per-seat charges," or monthly fees, to agencies for each telephone set (seat) the contractor services. The per-seat charge varies by the telephone type and features added to the telephone. The per-seat charge covers a variety of costs, including the costs for monitoring and managing network equipment; upgrading equipment and software that was current at the time the contract was signed; and providing network security (see Finding 2, pages 27 through 29).[1]

What Comprises a Per-Seat Charge?

For a single-line telephone with no long-distance capability located on the Capitol Mall in Phoenix or Tucson, the contractor will charge $42.20 per month during fiscal year 2008. If the telephone has the capacity to place calls over the state network, the fee is $46.11. The contractor adds additional charges for features such as $3 per month for each added phone or fax line, and $4 per month for a 22-button, add-on module.

Source: Telecommunications outsourcing contract pricing worksheets.

1 Under the contract, equipment and software is current if it is within two versions of the manufacturer's most recent release.

In contrast, ATS did not charge agencies a per-seat fee. Instead, it charged agencies separately for many of the costs covered under the per-seat pricing schedule.

- Moves, Adds, or Changes (MACs)—The contractor will also charge for service calls beyond a maximum number allowed under the per-seat charges. The per-seat charge includes labor and material costs for some alterations or changes to an agency's telephone system. Each year, an agency can have a maximum of one MAC that does not require a service call from the contractor for each telephone the contractor services and a maximum of one MAC that involves a service call for every five telephones the contractor services. For example, if an agency wanted to reset a password or add voice mail, the contractor would not have to come to the agency, but could perform the changes using remote software. However, changing from one type of phone to another could be considered a MAC that requires a site visit. The contractor will charge additional fees for MACs above the maximum amounts. As of June 2005 the contractor and the TPO had not determined these fees.

- Project Charges—The contractor will also charge agencies for major projects that are not included in the per-seat charges and are too extensive to qualify as MAC charges. Examples of such projects include adding equipment, replacing equipment that is no longer supported by the manufacturer, or removing older telephone equipment and replacing it with new technologies.

- Carrier Charges—The contractor will bill agencies for local and long-distance service and data services supplied by telephone companies, or carriers, such as Qwest. However, the contractor is adding new technology through the privatized network that will allow agencies to reduce these types of telephone costs by routing calls between state agencies through the network rather than using traditional phone lines.

- Administration Costs—The contractor's bill will also include charges to reflect the Department's costs for administering this contract. These costs are estimated to be $2.5 million annually for fiscal years 2006 through 2010. These include personnel costs for staff in the TPO to oversee the contract and operate a help desk. Additionally, bills will include a charge to recover nearly $500,000 in costs for department office space and associated costs at buildings that the contractor and TPO use.

Telecommunications contract costs

To assist state agencies with the transition to privatized telecommunications services, agency costs for telecommunications services in fiscal years 2006 and 2007 will be held at their fiscal year 2004 estimated amounts. Specifically, while the contractor has

developed a cost estimate of approximately $40 million annually to provide telecommunications services to the State, it has also agreed to maintain individual agencies' telecommunications costs for fiscal years 2006 and 2007 at their fiscal year 2004 estimated amounts. However, more current estimates of state agency telecommunications spending indicate that agencies' spending will be more than $8 million less than contract and administrative costs per contract year, and the Department is exploring several options to address this deficit.

The contractor's transitional pricing will allow agencies to prepare for 2008 telecommunications contract costs.

Pricing plan sets agency telecommunications costs at fiscal year 2004 amounts—The contractor has agreed to provide telecommunications services for approximately $40 million per year when agencies are fully transitioned to contractor-provided services. The contractor's pricing proposal is consistent with a 2004 department study of total state agency telecommunications spending. Specifically, since agencies have not historically created separate telecommunications budgets or accounted for all of their telecommunications costs, the Department conducted a study to estimate agency telecommunications expenditures during fiscal year 2004. This study estimated that agencies paid $39.9 million for telecommunications services in fiscal year 2004.

As part of its proposal, the contractor has agreed to hold each individual agency's telecommunications costs at or near their estimated fiscal year 2004 amounts for fiscal years 2006 and 2007. In addition to developing an estimate of state-wide expenditures for telecommunications services, the department study also found that agencies paid drastically different rates for telecommunications services. For example, during fiscal year 2004, the Department of Corrections spent approximately $45 per seat in telecommunications costs, while the Department of Game and Fish spent over $140 per seat. According to a department official, these cost differences result from agencies' differing telecommunications services needs. However, these costs also served as the basis for agency telecommunications budgets in fiscal years 2006 and 2007. Therefore, the TPO indicates that if the contractor's prices were charged to each agency immediately, some agencies would significantly exceed their telecommunications budgets, while others would be well under their budgets. As a result, for fiscal years 2006 and 2007, the contractor will adjust agency bills to make them consistent with their estimated fiscal year 2004 expenditures.

Estimated Contract Costs

Fiscal Year	Amount
2006[1]	$21,418,000
2007	39,659,000
2008	39,499,000
2009	39,000,000
2010	39,000,000

1 Fiscal year 2006 costs are lower because state agencies will not be completely transitioned to contractor-provided services.

Source: Contractor's contract pricing workbook.

Revised estimates result in need for additional agency spending—An ongoing analysis of recent agency spending suggests agencies may need to find ways to increase their telecommunications funding to match what they will be charged under the contract. After the contract was awarded, the Department updated its 2004 study and as of August 2005, estimated that agencies spent only about $35 million for telecommunications services in fiscal year 2005. In addition to the contractor costs, as previously mentioned, the Department plans to charge agencies approximately $3 million in administrative costs to oversee the contractor,

operate a help desk, and pay for other costs, such as rent for office space. This represents a more than $8 million difference between estimated agency expenditures in 2005 and the fiscal year 2006 and 2007 contract and administrative costs.

The Department is proposing several actions to address this funding deficit for fiscal years 2006 and 2007. First, according to department staff, the Department is proposing to deter $3.1 million in contractor charges for fiscal year 2006 until fiscal year 2007 or later. State agencies will eventually need to pay their amount plus interest. To address the remaining fiscal year 2006 deficit, department staff indicated that the Department is working with the Governor's Office of Strategic Planning and Budgeting and the contractor to develop other options, including using up to $1.7 million in carrier cost savings to offset agencies' costs. For fiscal year 2007, the Department is proposing that agencies approach the Legislature for a supplemental budget request to fund the approximately $8 million deficit between estimated agency spending and the contract costs, and to begin to pay the $3.1 million deferred from fiscal year 2006. According to department staff, the Department plans to continue to work with agencies to revise agency spending estimates, and intends to submit a proposal to the TEGC in September 2005 for addressing the deficit.

Beginning in fiscal year 2008, the contractor will stop adjusting each agency's bills to match 2004 spending. Recognizing that agencies' costs may change, the Legislature passed Laws 2005, Chapter 301, requiring the Department to report to the Joint Legislative Budget Committee a consolidated telecommunications budget report demonstrating the previous fiscal year's actual payments and the next year's anticipated payments for state agency telecommunications services. Since all agencies will be affected by this pricing change starting in fiscal year 2008, some agencies may need to adjust their budgets to reflect the changes in telecommunications costs.

What Are Carrier Cost Savings?

According to the contractor, the move to a single, privatized telecommunications network should result in some cost savings that originally were to be reinvested in the state-wide network. Prior to this new contract, state agencies could purchase their voice or data connections independently, creating multiple and separate telecommunications network connections. Cost savings would result from the contractor consolidating unneeded voice and data connections and adding new technologies allowing agencies to route interagency calls through the telecommunications network to save on telephone toll charges. The Department originally planned to use this savings to support various agency telecommunications projects, such as upgrading agency equipment attached to the network, but has since proposed using this money to assist with transition pricing.

AGENCY RESPONSE

Janet Napolitano
Governor

Jerry A. Oliver, Sr.
Interim Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

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

(602) 542-1500

September 21, 2005

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

Dear Ms. Davenport:

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

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

Sincerely,

Jerry A. Oliver
Interim Director

Enclosure

ADOA Agency Response, by Section and Finding

Auditor General Recommendations - ISD

1. *The Department should designate a central authority, such as its state-wide security manager, with the responsibility for developing a comprehensive security program for the Department's internal information resources and network, as well as the data center. The Department should then ensure that the program addresses:*

    a. *Developing a policy governing network scanning, monitoring, and testing, including how it should be done, the frequency, and follow-up procedures to correct identified vulnerabilities;*

Agency Response:

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

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

Agency Response:

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

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

Agency Response:

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

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

Agency Response:

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

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

Agency Response:

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

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

Agency Response:

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

2. *The Department should determine if it needs additional staff, funding, and technical resources to perform additional security duties and if so, assess whether it could reassign existing staff and resources or take other steps, as appropriate, to seek additional staff and resources.*

Agency Response:

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

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

Agency Response:

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

4. *The Department should enhance its interagency service agreements with state agencies that use the data center to define the Department's and the agencies' security responsibilities The agreements should:*

    a. *Delineate the Department's responsibility to provide access to the state data center and the state agency's responsibility to meet specific, minimum security requirements; and*

Agency Response:

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

b. *Define the circumstances under which a state agency may face actions for failure to comply with those security requirements, and the actions the Department can take to better ensure that corrupted computers in one agency do not compromise other agencies' systems and data.*

Agency Response:

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

5. *The Information Services Division should better ensure that it does not publish sensitive information on its Web site by developing a policy requiring central review and approval of Web site content. The Division should also review current Web content to ensure that sensitive information has not remained on its Web site, and instead maintain any sensitive information in a more secure environment, such as the Department's internal network that is not available to the public.*

Agency Response:

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

6. *The Department should configure its information system resources, such as routers, switches, and servers, to comply with GITA standards to provide greater safety from external threats.*

Agency Response:

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

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

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

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

Agency Response:

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

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

Agency Response:

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

2. *The Department should ensure that the contractor develops an adequate network security plan that includes the following:*

    a. *Requirements stipulated by the contract, including security service level agreements, compliance with GITA's state-wide security standards, and periodic security awareness and training for agency personnel; and*

Agency Response:

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

    b. *Other relevant aspects of an appropriate information technology security plan, such as defining clear security monitoring and enforcement processes, and how potential security breaches or other incidents will be identified, reported and monitored.*

Agency Response:

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

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

Agency Response:

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

Performance Audit Division reports issued within the last 24 months

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 Medical Board

04-L2 Letter Report—Gila County Transportation Excise Tax

04-L3 Letter Report—Department of Economic Security—Population Estimates

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—Division of Employment and Rehabilitation Services—Unemployment Insurance Program

05-02 Department of Administration—Financial Services Division

05-03 Government Information Technology Agency (GITA) & Information Technology Authorization Committee (ITAC)

05-04 Department of Economic Security—Information Security

05-05 Department of Economic Security—Service Integration Initiative

05-06 Department of Revenue—Audit Division

05-07 Department of Economic Security—Division of Developmental Disabilities

05-08 Department of Economic Security—Sunset Factors

05-09 Arizona State Retirement System

05-10 Foster Care Review Board

Future Performance Audit Division reports

Department of Administration—Human Resources Division

Department of Administration—Sunset Factors