STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Department of Administration
Information Services Division and Telecommunications Program Office

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Subject

The Information Services Division provides information technology services and support to the Department of Administration (Department) and to other state agencies. The Telecommunications Program Office oversees the contractor that is responsible for the privatization of telecommunications for all executive branch state agencies.

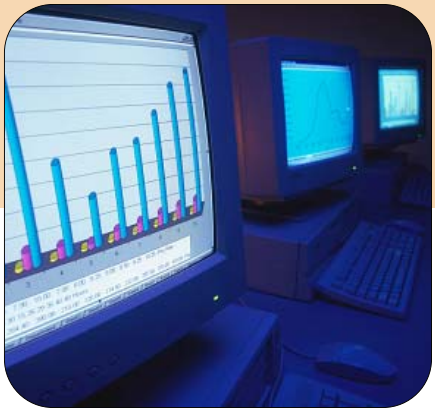
Our Conclusions

The Department needs to improve its information security procedures and request that the Legislature give it authority to enforce security requirements for AZNET. The Telecommunications Program Office needs to oversee the inventory of telecommunications equipment and ensure the contractor develops an appropriate security plan for AZNET.

2005

September • Report No. 05 – 11

Department Needs To Further Ensure Information Security



The Information Services Division (ISD) provides a variety of services to the Department and other state agencies, including:

- Processing millions of transactions or queries each week for the Department, the Motor Vehicle Division, the Department of Revenue, and the Arizona Health Care Cost Containment System.
- Overseeing a state-wide network providing voice and data communications.
- Providing Web page design, data processing, and technical support.

The Department is responsible for ensuring the security of its and other agencies' information. Information security includes restricting and granting access to the systems, setting up hardware and software, maintaining secure locations for the hardware and software, and conducting background checks of those who work with information systems.

Department lacks a coordinated security program—The Department performs some security functions well, such as ensuring that desktop computers have up-to-date virus protection and security updates. In addition, it ensures that user access to the mainframe computer system is controlled.

However, the Department does not meet national standards for many security functions. For example, it has not consistently monitored and tested its internal network. The National Institute of Standards and Technology (NIST) recommends that organizations do this regularly—and in some cases continuously—to guard against intrusions by unauthorized users.

In addition, NIST recommends that organizations obtain an independent security assessment at least every 3 years. The Department last obtained an assessment in 2001.

The Department should also regularly conduct risk assessments. Risk assessments identify and evaluate the risks of system vulnerabilities to determine the potential impact of those vulnerabilities and how to mitigate them. Although the Department has a policy on how to conduct a risk assessment, it has not performed a comprehensive assessment.

In addition to these shortcomings, the Department has not implemented many of the recommendations from its 2001 security assessment, which found many problems, such as the availability of sensitive information on its Web site. It

also does not have comprehensive security policies in place and does not conduct ongoing security awareness training.

A coordinated information security program is needed—The Department should centralize its security functions. As a first step, it should designate a person to serve as a state-wide security officer to administer a security program that would include:

- Network scanning, testing, and monitoring.
- An independent security assessment at least every 3 years.
- Regular risk assessments.
- Followups on weaknesses and risks.
- Annual training.

In addition, to protect the information systems maintained in its data center, the Department should ensure each agency using the center complies with minimum security standards. Because the data center involves shared resources, an agency that does not follow security standards potentially exposes other agencies using the data center to data loss or unauthorized intrusion.

Agencies using the data center sign interagency service agreements (ISAs). The Department should define in the ISAs the minimum security standards agencies must comply with and how the Department will monitor compliance and enforce standards. In addition, the Department should request statutory authority from the Legislature to enforce security requirements for agencies using AZNET. The Department should also work with the Government Information Technology Agency, which is responsible for establishing state-wide security standards for agency information systems, to ensure sufficient operational security standards are in place for AZNET.

Department also needs to limit access to sensitive information—Because ISD does not centrally control its Web site, sensitive information is available on the Internet. ISD has been aware of this problem since 2001, but has not taken action to remove this information from its Web site.

Recommendations

The Department should:

- Designate a person to serve as the state-wide security officer to establish a comprehensive security program.
- Revise ISAs to specify responsibilities for meeting minimum security requirements.
- Request the Legislature to grant it statutory authority to enforce security standards for AZNET.
- Ensure ISD does not publish sensitive information on its Web site.

DOA Needs To Improve Oversight of The Privatized Network

TPO Telecommunications Program Office

Source: Logo from: http://tpo.az.gov/.

In 2003, the Legislature directed the Department to privatize telecommunications services for all state agencies, including creating a single state-wide voice and data network called AZNET. In 2005, the Department awarded a 5-year, approximately $40 million annual contract to carry out this mandate. Also in 2005, the Legislature created the Telecommunications Program Office (TPO) within the Department to manage and oversee the contract.

Prior to the contract, the Department's Arizona Telecommunications System

(ATS) provided about 30 percent of voice and data telecommunications services to state agencies. The other 70 percent of services were purchased separately. The purpose of privatizing telecommunications is to consolidate the management of state agency telecommunication services under one contractor, thereby enabling agencies to take advantage of new technologies and potentially reducing costs.

With the substantial completion of phase one in July 2005, the contractor began offering services to and billing the agencies that previously received services from DOA. Phase two began in August 2005 and should be finished in March 2006. To make this transition, the contractor needs to:

- Implement its management processes and software systems.
- Resolve the current agency contracts by managing them until they expire, terminating them, or retaining the contract where appropriate, especially where there is a substantial termination penalty.
- Conduct an inventory of each agency's telecommunications assets.

Inventory can impact contract costs—The inventory is a critical component of the telecommunications contract. The service costs will depend on the types of phones that agencies have in their inventory. For example, a single-line phone will cost approximately $40 per month less than a multi-button phone, such as those used by call center supervisors. Because estimates only of the numbers and types of phones in service were available, the contract provides that the contractor can negotiate with the State to adjust the contract prices if the inventory is significantly different from the estimates.

In addition, some phone system equipment will have to be upgraded. The inventory will determine which equipment the contractor will upgrade and which equipment the agencies will upgrade. The agency will have to replace the equipment that the manufacturer no longer supports because the contract does not cover replacement.

Because the inventory is so important, the Department needs to oversee this process. However, the Department has not dedicated personnel to oversee the inventory. More importantly, the Department has not retained an employee who is knowledgeable about the equipment being inventoried who can oversee this process and assist in accurately identifying and categorizing the equipment.

Department should also improve oversight of network security—While the Department and the contractor share responsibility for securing the network, the Department has delegated to the contractor the duties of maintaining firewalls and operating intrusion detection equipment. However, the contractor has not developed an adequate security plan that includes all contractually required features.

The Department has begun to work with the contractor to develop a security plan by late 2005. This plan should incorporate national standards and benchmarks for effective network security management.

Recommendations

The Department should:

- Reassign staff or hire a technology expert to oversee the inventory process.
- Work with the contractor to develop an adequate security plan.

Contractor Billing System Will Bring Changes

In response to legislative inquiry, auditors also collected information on the billing process and costs under the new contract.

Billing process—The contractor will use a new billing system that will require agencies to pay for telecommunications services more quickly. Under the former system, agencies had 60 days after receiving the bill from the carrier to pay the invoice. Under the new system, agencies will have 30 days from the bill's date to pay the contractor.

The contractor will also charge monthly fees for each telephone set. An agency will be allowed to make one change (an addition or a move) that does not require a service call per set every year without a charge. The agency is also permitted one service call per five phones per year. The contractor will charge additional fees if it needs more changes or service calls.

Contract costs—The agencies' telecommunications costs for fiscal years 2006 and 2007 will depend on their estimated fiscal year 2004 costs. Because agencies have not historically created separate telecommunications budgets or accounted for all of their telecommunications costs, the Department estimated these costs for fiscal year 2004. These costs vary widely among agencies. For example, the Department of Corrections spent approximately $45 per telephone set in fiscal year 2004, while the Game and Fish Department spent $140 per set. If the contractor's new charges went into effect immediately, some agencies would exceed their budgets. Therefore, the 2004 costs will be used until the agencies have had time to adjust to the new, actual costs.

The contractor's actual prices will go into effect in fiscal year 2008. Since some agencies' costs for telecommunication services will be higher and some will be lower than what they are currently paying, this allows those agencies time to adjust their budgets.

TO OBTAIN MORE INFORMATION

A copy of the full report can be obtained by calling
(602) 553-0333

or by visiting our Web site at:
www.auditorgen.state.az.us

Contact person for this report:
Dale Chapman