A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit and Sunset Review

Government Information Technology Agency (GITA)

Sunset Review

Information Technology Authorization Committee (ITAC)

JUNE • 2005
REPORT NO. 05 - 03

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

Lisa Eddy, Manager and Contact Person
Jay Dunkleberger, Team Leader
Michael Nickelsburg

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

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

OFFICE OF THE
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

June 29, 2005

Members of the Arizona Legislature

The Honorable Janet Napolitano, Governor

Mr. Chris Cummiskey, Director
Government Information Technology Agency

Transmitted herewith is a report of the Auditor General, A Performance Audit and Sunset Review of the Government Information Technology Agency (GITA) and Sunset Review of the Information Technology Authorization Committee (ITAC). 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, GITA 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 June 30, 2005.

Sincerely,

Debbie Davenport
Auditor General

Enclosure

PROGRAM FACT SHEET

Government Information Technology Agency

Services:

Established in 1996 under A.R.S. §41-3502, GITA is responsible for state-wide information technology (IT) planning, policy setting, and consulting. GITA also plays a role in reviewing and monitoring IT projects. The GITA Director serves as the Chief Information Officer for Arizona government.

Personnel:

For fiscal year 2005, GITA is authorized 21 full-time equivalent positions and had no vacancies as of February 2005.

Facilities and equipment:

The agency owns no facilities, but pays approximately $100,000 in rent for space from the Department of Administration. This space is located in the Arizona State Office Building at 100 North 15th Avenue, Suite 440, Phoenix, Arizona. The agency owns only standard office equipment.

Mission:

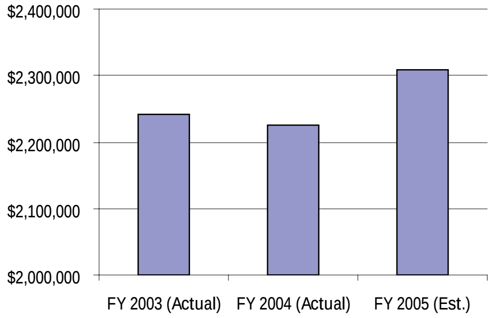
To partner with state agencies and private sector organizations to improve information technology capabilities, both technical and human, to efficiently add value and improve delivery of public services for the people of Arizona.

Program goals:

During the audit, GITA operated under a 2004 agency strategic plan. This plan contained the following seven goals:

- To maintain the current updated policies, standards, and procedures.
- Finish the Quality Assurance (QA) assessment and analysis in calendar year 2004.
- To train an additional 40 to 50 agency IT personnel in current security practices and technology within 6 months. Ten classes have been scheduled to date.
- To increase participation in the Web portal and improve Web site utilization by state agencies.
- To streamline and improve the IT planning and inventory process.
- To improve review times for projects and project timeliness.
- To have an operational 211 Web site by April 2005.

Program revenue:[1]



[1] GITA is funded entirely from a 0.15 percent charge on state agency payroll expenditures.

Adequacy of goals and performance measures:

GITA's 2004 strategic plan's 7 goals and 14 performance measures related to some of its statutory responsibilities. These goals include reviewing agencies' proposed IT projects, determining whether agencies' IT projects are completed on time and within budget, and completing IT policies and standards for agencies to follow. However, there are several improvements that GITA should make to its goals and performance measures in its next strategic plan:

- Not all goals strategic—Three of GITA's goals are narrow in scope and time frame, rather then being strategic. For example, one goal is to finish the QA assessment and analysis in calendar year 2004. According to the Governor's Office of Strategic Planning and Budgeting's *Managing for Results: 1998 Strategic Planning and Performance Measurement Handbook,* goals should encompass at least a 3-year period. GITA should broaden goals to reflect its strategic issues and ensure they reflect long-term planning.

- Not all types of performance measures adequately used—GITA does not use all types of performance measures and should develop some more meaningful measures. For example, GITA lists the number of policies completed or revised (output), but does not measure the number of these policies adopted by agencies (outcome), except for the Web site policies. Also, there are no measures evaluating GITA's performance.

- Some performance measures do not reflect GITA's performance—GITA should focus on performance measures that demonstrate its involvement. Currently, 9 of the 14 performance measures rely on other organizations' activities. For example, one performance measure tracks the number of transactions available on the Internet. Since other agencies provide these services, and not GITA, it is not clear how GITA's efforts affect this measure. GITA should develop measures that evaluate their efforts to influence these other organizations.

As of June 2005, GITA had developed a new set of goals and is planning to create performance measures for these goals.

Source: Auditor General staff compilation of information from statutes; unaudited information from the Governor's Office of Strategic Planning and Budgeting's *The Master List of State Government Programs* for fiscal years 2003-2005; Arizona Financial Information System's (AFIS) *Accounting Event Transaction File* for the years ended June 30, 2003 and 2004; agency-prepared financial estimates for the year ending June 30, 2005; agency interviews, organization charts, and strategic planning documents; agency and Governor's Office of Strategic Planning and Budgeting Web sites; and auditor analysis of the agency goals and performance measures.

SUMMARY

The Office of the Auditor General has conducted a performance audit and sunset review of the Government Information Technology Agency (GITA) and a sunset review of the Information Technology Authorization Committee (ITAC) 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.

Established in 1996 under A.R.S. §41-3502, GITA is responsible for state-wide information technology (IT) planning and policy. These duties include developing a state-wide IT plan, adopting state-wide IT standards, reviewing and monitoring IT projects undertaken by state agencies, providing consulting services to agencies, and studying emerging technologies and their impact on the State. GITA's Director is the State's Chief Information Officer.

ITAC was established in the same legislation that created GITA and is composed of members from the Legislature; state, federal, and local governments; and private industry. ITAC has a number of responsibilities related to information technology, such as working with GITA to review and approve agency information technology projects over $1 million, reviewing established state-wide information technology standards, and monitoring information technology projects it considers major or critical.

GITA needs to improve state-wide IT management (see pages 7 through 19)

GITA, as the state-wide coordinator for information technology, should take a stronger leadership role in the following four key areas in the State's IT management:

- **Security standards**—GITA has developed a comprehensive set of IT security standards that comply with industry standards, but state agencies do not always adhere to them. For example, reports submitted to GITA by the 11 state agencies with significant IT expenditures showed that 8 had not fully

implemented at least one of GITA's standards in network security. Complying with these standards is important because state agencies have reported four instances in which unauthorized users have penetrated state networks since 2001. To help address these concerns, GITA should take the following steps used in other states: First, GITA should develop a state-wide security plan that comprehensively addresses security gaps. Second, GITA should consider designating a staff member to serve as a Chief Security Officer for the State. Thirty-one other states have formally established a security office or a chief security officer. GITA could use this position to ensure that agencies comply with security rules, policies, and procedures; coordinate the development of a state-wide security plan; and help consolidate security oversight and coordination activities such as system security audits. GITA has a position that is assigned to some security issues and should assess whether it can expand current staff's responsibilities or needs to seek legislative approval for additional staff.

- Privacy standards—GITA has developed several privacy standards for state agency information systems, but the current list is incomplete, and compliance monitoring is limited. The current standards, developed as part of the security standards, include two broad policies. One relates to how personal information is collected, maintained, used, and disseminated on state agency Web sites, and the other establishes methodology to classify state data according to its sensitivity. These standards are incomplete when compared to industry and government standards. For example, GITA's standards do not require agencies to collect only data needed to accomplish a legitimate business objective or meet a statutory or legal requirement. GITA needs to expand its standards and ensure that agencies comply with them; include privacy standards when developing a comprehensive security plan; and similar to the security recommendations above, consider designating a staff member to serve as a Chief Privacy Officer for the State.

- Training—Although statute does not specifically charge GITA with identifying and meeting state IT training needs, the agency is uniquely positioned to assess what these training needs are and to help meet them. GITA works with two IT planning groups, including the Chief Information Officer's Council, which is an advisory committee of the Chief Information Officers of 26 state agencies or other organizations. GITA annually reviews and approves state agency IT strategic plans, which can include information related to training needs, and it learns about training needs as it reviews and monitors new IT projects throughout the State. After identifying these training needs, GITA should work with the Arizona Government University (a training agency overseen by a governing board of state agencies) or with other sources to address them.

- Agency procurements—Although the Department of Administration's Enterprise Procurement Services is ultimately responsible for issuing solicitations and contracts for IT projects, GITA can play a larger role than it currently does in these procurements.[1] GITA helps coordinate IT-related purchases that cross state agencies, which it should continue to do. However, GITA has not brought its IT expertise to evaluation committees that review proposals from contractors, contending that participation in such committees would conflict with its role in monitoring IT projects. IT agencies in two other states perform this role. GITA needs to reconsider its policy and work with Enterprise Procurement Services to determine when it could participate.

GITA has improved its leadership role in the following area:

- **State-Wide Strategic IT Plan**—GITA has improved its State-Wide Strategic IT Plan by increasing the use of stakeholder input and adding performance measures. In developing the 2005 plan, which is still in its draft form, GITA used state agency IT plans and input from ITAC and CIOs to help it develop the goals. For future plans, GITA should continue to seek input from stakeholder groups. In addition, GITA added performance measures to the 2005 plan to help it measure progress made toward achieving the goals.

GITA should strengthen IT project reviews and better help agencies manage IT projects (see pages 21 through 30)

GITA should improve its IT project review-and-approval process and enhance agency IT project management efforts. GITA reviews and approves the justification for agency IT projects and monitors these systems as they are developed. However, GITA's current review-and-approval process is not focused on projects for which the costs are highest or the risks are greatest. Currently, GITA must review all projects costing $25,000 or more, a threshold that may not be as useful as a review of higher-cost, higher-risk projects. For example, in 2004 GITA reviewed a $35,000 request to replace 36 batteries used for backup telephone power at the State Capitol. While GITA's policies indicate that it more heavily scrutinizes higher-cost projects, GITA should seek legislation removing the requirement that it review all projects costing $25,000 or more and develop criteria that includes project cost and risk factors.

Besides focusing its reviews on those projects with greatest cost and/or risk, GITA should also ask agencies for more complete information to improve its review quality. For example, GITA currently requires agencies to provide a yes-or-no answer as to whether a project is consistent with GITA's state-wide standards and requires details only if the answer is "no." Requiring agencies to submit additional information about these projects would help GITA better evaluate whether a sufficient need and justification exists for the project. Finally, once it has reviewed its justification requirements and developed its review criteria, GITA should reassess its staffing and

[1] In January 2005, the Department of Administration created a new organization, Enterprise Procurement Services, which is responsible for the activities formerly performed by the State Procurement Office.

skill needs used in its project-approval process to determine if reassigning current staff or seeking additional staff is required.

After projects have been approved and funded, GITA monitors their progress. However, in spite of these efforts, projects have experienced significant cost and schedule overruns. Other states have taken a number of steps to help agencies keep their projects on track. These techniques include coordinating training programs for agency project managers and establishing standards for IT project management. For example, New York's Office for Technology has developed a project management guidebook to promote a common methodology guiding state agency IT projects. Similar efforts by GITA could help Arizona agencies avoid project delays or costly overruns on future projects.

TABLE OF CONTENTS

Sunset Factors:

continued

TABLE OF CONTENTS

.

concluded ◆

INTRODUCTION & BACKGROUND

The Office of the Auditor General has conducted a performance audit and sunset review of the Government Information Technology Agency (GITA) and a sunset review of the Information Technology Authorization Committee (ITAC) 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.

Responsibilities and staffing

GITA was established in 1996 under A.R.S. §41-3502. According to one legislative sponsor, at that time a major state IT system had experienced significant cost overruns. The establishment of GITA was intended to help prevent future projects from experiencing similar overruns. GITA has several statutory responsibilities, including adopting state-wide IT standards, reviewing and monitoring IT projects undertaken by state agencies, providing consulting services to agencies, and studying emerging technologies and evaluating their impact on the State.

As of February 9, 2005, GITA had 21 authorized FTEs, all of which were filled. GITA's Director serves as the State's Chief Information Officer. While there are no formal organizational divisions within GITA, six staff, including the Director and Deputy Director, are responsible for administration, communications, staff support, and agency direction. The remaining staff are involved in tasks such as reviewing and monitoring state agencies' IT projects; writing and revising GITA's state-wide IT standards, policies, and procedures; reviewing agencies' IT plans and developing a state-wide IT plan; reviewing agencies' self-assessments of their compliance with state security standards; coordinating and reviewing agency business continuity plans that ensure that agencies can continue to function or quickly resume functioning following a disaster; contracting for a state Web portal that electronically offers some services to the public; and supporting special projects. Examples of several special projects GITA staff have been involved with include developing a contract for a system that allows the public easier access to health and human services and emergency information by dialing 211 or through a Web site, and assisting in developing a contract privatizing telecommunications systems used at state agencies.

Information Technology Authorization Committee

ITAC was established under A.R.S. §41-3521 in the same legislation that created GITA. The GITA Director serves as the chair of ITAC, which includes members from the Legislature; state, federal, and local governments; and private industry (see text box for the Committee's composition). ITAC's responsibilities include:

- Reviewing and approving or disapproving agency information technology projects that exceed $1 million. In fiscal year 2004, ITAC reviewed 19 projects, and approved or approved with stipulations 15 of them.
- Reviewing established state-wide information technology standards and the state-wide information technology plan.
- Conducting periodic reviews on the progress of implementing information technology projects approved by ITAC.
- Monitoring information technology projects that ITAC considers to be major or critical.
- Hearing and deciding appeals made by agencies regarding GITA's rejection of their proposed information technology plans or projects.
- Reporting to the Governor, Legislature, and the Secretary of State at least annually on all matters concerning its objectives.

ITAC Membership

Membership consists of the following persons or their designees:

- Four members of private industry, appointed by the Governor and subject to senate approval.
- Two directors of state agencies, appointed by the Governor.
- The administrative director of the courts.
- Two members of private industry or state government, appointed by the Governor.
- One local government advisory member and one federal government advisory member, appointed by the Governor.
- The GITA director, who serves as chair but is also an advisory member.
- One advisory member from each branch of the Legislature, appointed by the President of the Senate and the Speaker of the House of Representatives.
- The staff director of the Joint Legislative Budget Committee.

Budget

Table 1 (see page 3) illustrates GITA's actual revenues and expenditures for fiscal years 2003 and 2004 and estimates for fiscal year 2005. GITA does not receive any funding directly from the General Fund. Instead, its revenues come from a 0.15 percent surcharge on the payroll expenditures of state agencies and the legislative and judicial branches. In fiscal year 2004, this revenue totaled $2.23 million, while GITA's expenditures totaled $2.17 million. The majority of GITA's expenditures in fiscal year 2004 were for employee salaries and benefits, which totaled $1.69 million.

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

	2003	2004	2005
	(Actual)	(Actual)	(Estimated)
Revenues:			
Charges for services [1]	$2,242,591	$2,225,770	$2,309,000
Expenditures: [2]			
Personal services and related benefits [3]	1,542,752	1,687,221	1,808,600
Professional and outside services	366,696	218,630	236,000
Travel	7,547	7,187	10,000
Other operating [4]	345,165	216,026	220,000
Capital outlay	73,855	40,751	30,000
Total expenditures	2,336,015	2,169,815	2,304,600
Excess (Deficiency) of revenues over expenditures	(93,424)	55,955	4,400
Fund balance, beginning of year	656,432	563,008	618,963
Fund balance, end of year	$ 563,008	$ 618,963	$ 623,363

[1] Consists of a 0.15 percent charge on other agencies' payroll expenditures.

[2] Includes the prior year's administrative adjustments.

[3] The agency reports that the amount increased significantly from 2003 to 2005 because it filled vacancies that included a legislatively approved position to oversee the Web portal.

[4] The 2003 amount includes approximately $108,000 reimbursed to the federal government. Laws 2001, Second Special Session, Chapter 4 required the agency to transfer $500,000 to the State General Fund in 2002. Since GITA's revenues are generated from pro rata charges on other agencies' payrolls that include federal dollars, it was required to reimburse the federal government a portion of that transfer.

Source: Auditor General staff analysis of the Arizona Financial Information System (AFIS) *Accounting Event Transaction File* for the years ended June 30, 2003 and 2004, and agency-prepared estimates for the year ending June 30, 2005.

Audit scope and methodology

This audit focused on GITA's role in coordinating activities related to several IT areas that are critical to the State and its review and oversight of state agencies' IT projects. The report presents findings and recommendations in two areas:

- GITA should take a stronger leadership role in coordinating IT security, privacy, training, and procurement for the State; and

- GITA could provide more effective reviews and monitoring of state agencies' IT projects by focusing its reviews on riskier, more expensive projects; requiring agencies to provide more detail about these projects; and adapting approaches used in other states to help keep projects on track.

To examine these audit issues, auditors used a variety of methods. These methods include reviewing applicable federal and state statutes, administrative rules, and policies and procedures; conducting interviews with GITA staff; and reviewing internal agency documents. Auditors also used the following specific methods:

- To identify IT areas critical to the State and determine how GITA and other state agencies manage these functions, auditors reviewed the National Association of State Chief Information Officers' (NASCIO) *2003-2004 Compendium of Digital Government in the States* and interviewed GITA staff and other Arizona state agency officials.[1] Auditors also asked chief information officers from four large Arizona state agencies and one medium-sized agency to evaluate how the State manages these various functions. To assess GITA's state-wide IT state standards and forms used to evaluate agency compliance with these standards, auditors compared GITA's security, privacy, and business continuity standards to the *Federal Information Systems Controls Audit Manual*, *COBIT*, *Recommended Security Controls for Federal Information Systems,* and *Practical IT Auditing*.[2-5] To identify how GITA could improve its planning process, auditors also reviewed the Governor's Office of Strategic Planning and Budgeting's *Managing for Results: 1998 Strategic Planning and Performance Measurement Handbook*.[6] Finally, to review how other states organize their IT security, privacy, and procurement efforts, auditors reviewed information from the NASCIO Compendium and reviewed programs or contacted officials in 11 states.[7]

[1] National Association of State Chief Information Officers. *2003-2004 Compendium of Digital Government in the States.* Lexington, KY: National Association of State Chief Information Officers, 2003.

[2] United States Government Accountability Office. *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6). Office. Washington, D.C.: United States Government Accountability Office, 1999.

[3] IT Governance Institute. *COBIT: Governance, Control and Audit for Information and Related Technology*. Rolling Meadows: The Institute, 2000.

[4] U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems* (Final Public Draft. NIST Special Publication 800-53). Washington, D.C.: U.S. Department of Commerce: January 2005.

[5] Champlain, Jack. *Practical IT Auditing.* New York: Warren, Gorham and Lamont, 2004.

[6] Arizona Governor's Office of Strategic Planning and Budgeting. *Managing for Results: 1998 Strategic Planning and Performance Measurement Handbook*. Phoenix: Arizona Governor's Office of Strategic Planning and Budgeting, 1998.

[7] Auditors reviewed information or contacted officials from Colorado, Florida, Michigan, Minnesota, New York, North Carolina, Oregon, Tennessee, Texas, Utah, and Washington.

- To evaluate GITA's process for reviewing, approving, and monitoring state agencies' IT projects, auditors selected a sample of eight IT projects and conducted an in-depth review of the project files. These projects represented a variety of project sizes, agency sizes, and a variety of types of projects including software replacement and the development of complicated new computer systems. Auditors also interviewed staff from the agencies that developed some of the projects and GITA staff who reviewed the project proposals or conducted oversight to gain a further understanding of these projects. To identify other states' practices in IT project evaluation, oversight, and project management, auditors also reviewed the NASCIO Compendium. To identify best practices in project management, auditors contacted officials or collected information from eight states because of their use of innovative project management or project review practices or because they employed an IT governance structure similar to Arizona's.[1] Auditors also reviewed literature such as *Project Success: A Cultural Framework,* and *A Survey of Best Practices and Utilization of Standards in the Public and Private Sectors*.[2,3] To identify project management needs, auditors interviewed CIOs from five state agencies as well as a representative from the Arizona Governor's Office.

- To develop the Introduction and Background section, auditors compiled information from state statutes and legislation, and conducted interviews with agency officials and a sponsor of the legislation that created GITA. Auditors also used unaudited records such as the Arizona Financial Information System (AFIS) *Accounting Event Transaction File* for the years ended June 30, 2003 and 2004; agency-prepared estimates for the year ending June 30, 2005; agency records concerning technology projects, and agency organizational charts.

The audit was conducted in accordance with government auditing standards.

The Auditor General and staff express appreciation to the director and staff of the Government Information Technology Agency for their cooperation and assistance throughout the audit.

[1] California, Florida, Maine, New York, North Carolina, Texas, Utah, and Washington.

[2] Korin, Kendra, and Laura J. Taplin. "Project Success: A Cultural Framework." *Project Management Journal,* April 2004. 30-45.

[3] Brotbeck, George, Tom Miller, and Dr. Joyce Statz. *A Survey of Best Practices and Utilization of Standards in the Public and Private Sectors.* Austin: State of Texas Department of Information. TeraQuest Metrics, Inc., 1999.

FINDING 1

GITA needs to improve state-wide IT management

GITA, as the State's information technology coordinator, should take a stronger leadership role in the State's IT management operations in five key areas. First, while GITA has developed security standards, it needs to do more to ensure that agencies consistently adhere to them. Second, GITA needs to augment standards it has already developed that protect the privacy of data and ensure that agencies comply with these standards. Third, GITA should use its role as the State's IT coordinator to identify and address state-wide training needs. Fourth, although GITA has a statutory role to approve and oversee agencies' IT projects, the State would benefit if GITA applied its expertise more directly in the procurements themselves. Fifth, GITA has improved its State-wide Strategic IT Plan, and for future plans GITA should ensure that it continues to obtain stakeholder input.

Five Key IT Management Areas

This audit covers GITA's involvement in five key areas of state-wide information technology management:

Security: Ensuring that agencies are following established standards that will help keep unauthorized users from breaking into the system (see pages 7 through 11).

Privacy: Ensuring that agencies do not collect personal data that they do not need and that they safeguard the personal data they collect (see pages 11 through 13).

Training: Ensuring that state IT personnel have the necessary skills to administer IT applications (see pages 13 through 15).

Procurement: Helping the State evaluate contract proposals made by vendors (see pages 15 through 17).

Planning: Providing a sound and strategic direction for addressing the State's IT needs (see pages 17 through 18).

GITA needs to ensure security standards are followed

Although GITA has developed IT security standards, many agencies do not comply with them. Further, according to the Arizona Department of Administration (DOA), there have been four successful network security attacks by unauthorized users since 2001. GITA needs to develop a comprehensive IT security plan for correcting security weaknesses at state agencies, and consider designating a staff member to serve as a Chief Security Officer to increase the focus on security issues.

GITA has created comprehensive state-wide IT security standards.

GITA has developed state-wide IT security standards—Statute requires GITA to develop information technology security standards for all state agencies to follow. GITA's standards include a broad set of policies governing 17 general IT security areas, such as creating and changing user accounts, properly controlling and monitoring access to resources and services, and protecting IT systems against viruses. Within each of these areas, agencies are required to follow specific standards, such as establishing an IT security program and ensuring that all remote computer workstations and servers that have access to the agency's internal network have appropriate virus-scanning software. Since these standards are designed to protect the State's IT assets, resources, and data from unauthorized use, disclosure, or destruction, it is important for agencies to comply with these standards.

Auditors' review of these standards indicates that the standards are comprehensive. A comparison of GITA's IT security policies, standards, and procedures to several federal and national auditing standards showed that GITA's standards address most major aspects of IT security.[1] For example, industry standards generally include protection against viruses and network security issues, such as establishing an adequate firewall to protect the system from intruders when agencies transfer inbound and outbound data.

Many agencies do not comply with the standards—State agencies do not always adhere to the standards and, as a result, are potentially exposed to serious security threats. GITA requires agencies to self-report their compliance with the security standards using Technology Security Assessment (TESA) forms. Agencies use the TESAs to report the extent to which they meet GITA's security standards. If there are any standards the agencies do not fully comply with, the agencies report how they plan to achieve compliance with the standards.

Auditors reviewed the TESA forms from 11 Arizona state agencies with significant IT expenditures, and identified areas where agencies have not adopted or implemented processes to comply with GITA's security standards. Based on this review, auditors identified several areas of particular concern, including:

- **Network security**—GITA has developed network security standards that seek to provide secure and seamless interconnection of communications networks and systems while protecting the State's computing resources and information. The standards include requirements such as ensuring intrusion detection and that prevention tools are in all appropriate devices.

  However, TESA reports show that 8 of the 11 agencies had not fully implemented at least one of GITA's ten standards. For example, one state agency indicated that it had yet to install intrusion detection and prevention tools for its networks.

Eight of 11 agencies had not fully implemented at least one of GITA's network security standards.

[1] Auditors primarily relied upon the U.S. Government Accountability Office's *Federal Information Systems Controls Audit Manual (FISCAM)*, published in January 1999, reformatted and with updated references but contents otherwise unchanged in June 2001. This source was supplemented by *COBIT: Governance, Control and Audit for Information and Related Technology*; *Recommended Security Controls for Federal Information Systems,* published by the National Institute of Standards and Technology in January 2005; and *Practical IT Auditing*.

- **Virus protection**—Similar to its standards for network security, GITA has also developed state-wide virus and malicious code protection requirements to safeguard networks, IT components, and sensitive information. GITA's standards include requirements such as ensuring that agencies have virus-scanning software that regularly scans all appropriate computer equipment.

  In this area, 5 of the 11 agencies had not fully implemented all seven GITA virus protection standards. For example, one agency indicated that it had developed procedures for regularly scanning its equipment, but was not able to install and operate anti-virus software on some of its servers.

Complying with the security standards is critical because agencies face security attacks. For example, since 2001, Arizona state agencies have reported that unauthorized users have successfully attacked and penetrated four agency networks. In one case, an agency did not follow the standards relating to passwords. As a result, an unauthorized user gained access to some of the agency's databases and erased them before the agency identified and resolved the problem. Moreover, during 2004, agencies reported 44 incidents where they were infected by viruses.

Since 2001, unauthorized users have successfully attacked and penetrated four agency networks.

More comprehensive approach needed for state-wide security—To help address these potential security weaknesses at the agencies, GITA should study the feasibility of approaches used in other states to improve state-wide IT security. Specifically, GITA should:

Develop a comprehensive security plan—GITA should develop a state-wide security plan similar to other states' plans that comprehensively addresses identified security weaknesses. GITA has some efforts under way, but they fall short of being comprehensive. First, although GITA's TESA form requires agencies to indicate how they will address areas where they do not meet state security standards, GITA has a limited process in place for reviewing these responses and ensuring they are carried out. While GITA meets with agencies to determine how they will address security deficiencies identified on the TESA form, it currently has no comprehensive method to address all deficiencies on a state-wide level. Second, a joint effort begun in 2004 with the Arizona Office of Homeland Security is studying short-term security priorities and has only recently begun to develop an action plan for addressing these items. This effort, called the Information Technology Security Advisory Committee (ITSAC), is a committee composed of personnel from several key agencies as well as members from private industry. ITSAC is intended to examine several areas related to state-wide IT security, including identifying and recommending best practices to meet the State's future security requirements. In March 2004, ITSAC identified ten areas in IT security that need to be addressed, such as ensuring that state agencies complete and submit TESA reports and report security incidents.

A state-wide security plan could comprehensively address identified security concerns.

Two other states' central IT agencies reviewed as part of this audit have developed comprehensive state-wide security plans. For example, North Carolina's Office of Information Technology Services assesses state agency compliance with security standards. As part of this assessment, a consultant for the state estimated the cost for the state and agencies to fully comply with these standards. Using this information, the office developed a plan with strategic recommendations, such as providing more funding and improving state security awareness and training. In addition, Colorado's IT agency has a state-wide information security strategy that sets IT security priorities. In addition to the state-wide plan, Colorado has implemented a policy that requires agencies to develop their own plan to address their specific security deficiencies along with time frames for achieving compliance in those areas.

GITA should consider establishing a chief security officer—Because security is such a critical issue, GITA should consider designating a staff member to serve as a Chief Security Officer for the State. Having a central point of contact for security may make it easier for GITA to ensure that agencies' IT security programs are standardized and that agencies comply with security rules, policies, procedures, and standards, which in turn will help minimize the effects of information security threats and vulnerabilities on the state network. For example, this officer could be charged with coordinating the development of a state-wide security plan, ensuring that all agencies follow the security standards, and following up with those that do not. It could also take a role in activities such as training state agencies on security awareness, ensuring that state agencies complete and follow up on formal risk assessments, coordinating ethical hacking to test the likelihood that intruders could breach the state network, and ensuring coordination of state agency computer security incident responses.

A chief security officer could help consolidate security oversight and coordination.

A chief security officer could also help to consolidate or coordinate a number of security-related oversight and coordination activities that are currently performed by GITA, DOA, or other agencies on a limited basis, or are not performed at all. For example, there is no central source conducting security audits for state agencies, and agencies are generally not performing this function themselves. According to DOA, it performs some limited security reviews of other state agencies; however, these are typically performed only upon the agency's request, and no agency ensures that they are performed for agencies state-wide. Additionally, an individual within DOA compiles information about security breaches occurring at agencies. Further, there is currently no comprehensive state-wide security plan or state-wide training program to address security awareness.

According to the National Association of State Chief Information Officers' (NASCIO) 2003-2004 *Compendium of Digital Government in the States*, 31 states have established either a centralized information security office or officer. While these offices or officers may have abilities GITA currently lacks, they represent the potential powers and abilities of a centralized security position. For example, Colorado has adopted a security policy creating a State Chief Security Information Officer. The policy also requires each agency to designate someone to coordinate agencies' security policies, and to construct and implement a security plan that addresses issues such as virus protection and intrusion detection. If agencies fail to comply with this policy, they can be denied access to the state network. North Carolina's Office of Information Technology Services has created a Chief Security Officer who reviews proposed state agency IT projects to ensure that they meet state security standards and can disconnect agencies from the state's network if they feel the agency is a security risk. Moreover, the Office has the ultimate authority to take over security operations of agencies that do not meet standards. Michigan has established a Chief Information Security Officer, and its Department of Information Technology conducts audits and risk assessments, which include evaluating agencies' security practices to verify compliance with policies. Florida's Office of Information Security performs services state-wide, including audits to identify information security risks, developing standards, and collecting information on security threats. Moreover, Utah has a Chief Information Security Officer who chairs the State Information Security Committee. This committee develops and reviews state security policies and procedures, reviews state security implementation projects, and helps ensure that state security practices and policies are appropriately implemented.

GITA has one manager assigned to some security issues, such as coordinating TESA reports and working with other agencies on Homeland Security issues. GITA should study the need, feasibility, and statutory requirements necessary to establish a security office or officer, as well as define such an office's or position's responsibilities. GITA should then assess whether it could reassign staff to these new responsibilities or seek legislative approval for additional staff.

Privacy standards need improvement

GITA needs to make its privacy standards more complete and ensure that agencies follow them. GITA could address adherence to privacy standards in conjunction with its efforts to address adherence to security standards by taking action that other states have implemented, such as establishing a chief privacy officer to assess and follow up on agencies' adherence to the standards.

Some aspects of privacy are not included in GITA's standards.

Existing IT privacy standards have gaps—As part of its state-wide IT standards, GITA has developed privacy standards for state agency information systems. These standards include two broad policies. One relates to how personal information is collected, maintained, used, and disseminated on state agency Web sites. A second establishes a methodology classifying data held by the State according to its sensitivity to protect against loss or misuse. However, GITA's privacy

standards and measurement methods are incomplete, and agencies are not consistently adhering to the standards.

A review of best practices suggests there are other aspects to IT privacy not included in GITA's standards. Specifically, a comparison of GITA's privacy standards to practices outlined in IT literature shows GITA's standards contain no requirements that:[1]

- Data on individuals should be collected only to accomplish a legitimate business objective or to meet statutory or other legal requirements.
- Data should be adequate, relevant, and not excessive in relation to the business objective.
- Sensitive data gathered on individuals should be verified before it is entered into the database.
- Data should be accurate and, where necessary, kept up-to-date.
- If there is disagreement about data on an individual, that individual's version should be noted and included in any disclosures of the file.
- Disclosure of data, other than the most routine, should be noted and maintained for as long as the data is maintained.
- Data should not be disclosed for reasons incompatible with the business objective for which it was collected and should be in compliance with statutory or other legal requirements.

Limited monitoring of and compliance with privacy standard—GITA uses the information reported in the agencies' TESAs to assess their compliance with some privacy standards. However, the TESA form only measures agency practices for classifying data as either public or confidential. While this is one important aspect of privacy, the TESA form does not measure whether agencies adequately protect personal information on state agency Web sites.

Some agencies are not complying with the privacy standards that are addressed by the TESA form. Specifically, auditors' review of agencies' TESAs found that 3 of the 11 agencies with significant IT expenditures were not adhering to one or more of these standards. For example, while one standard calls for data to be classified as either confidential or public information, one large agency indicated that it was not complying with this standard.

[1] Champlain, Jack. *Practical IT Auditing*. New York: Warren, Gorham and Lamont, 2004.

GITA needs to strengthen privacy standards, testing, and compliance—GITA should make its privacy standards complete, revise its TESA form to include agency's adherence to privacy standards, and take steps to ensure that state agencies follow them. In conducting its review, GITA should compare its standards to those generally used by government and private industry and ensure that they include all of the important requirements for agencies to follow. In addition, GITA should review the TESA form and make sure that it includes all aspects of privacy and therefore provides a comprehensive assessment of agencies' compliance with privacy standards.

Once GITA has ensured that its privacy standards are complete, it should take similar steps to those identified earlier to help state agencies comply with security standards. Adherence to privacy standards could be included in the comprehensive security plan and security audits discussed previously. For example, Colorado's Information Security Strategy plan includes an information privacy program, which includes initial and periodic information privacy risk assessments and ongoing monitoring of agencies' compliance with privacy standards. Further, GITA should explore designating a staff member as the Chief Privacy Officer (CPO) for the State. Currently, the State has no state-wide CPO. According to the American Institute of Certified Public Accountants, a crucial step in developing a privacy program is to create a privacy officer, who should determine whether systems that store information have the capacity to track and record who has access to information, assess the gaps in current privacy practices, develop appropriate policies and procedures, and be responsible for privacy compliance. Some states have established a central position to coordinate privacy standards state-wide and to ensure that agencies follow them. According to the NASCIO *Compendium of Digital Government in the States,* 20 states have established a chief privacy officer or similar position. Moreover, according to GITA, such a position would be valuable to ensure that agency privacy concerns are adequately addressed and that the issue is given greater prominence. Therefore, similar to steps identified earlier to improve state-wide IT security, GITA should explore the need, feasibility, statutory, and staffing requirements necessary to establish a CPO, either using existing staff or seeking legislative approval for a new position.

A Chief Privacy Officer is a critical step in developing a privacy program.

GITA positioned to identify and address state agencies' IT training needs

Although GITA is not specifically charged by statute with identifying and meeting state IT training needs, the agency is uniquely positioned to assess what these training needs are and to help meet them. GITA should take advantage of its relationship with IT planning groups and its knowledge of current and planned agency IT systems to identify future IT training needs. It should then work with the

Arizona Government University (AzGU) and/or other sources to help address these needs.

GITA and AzGU provide IT training—Both GITA and the AzGU provide IT training for state agencies, although GITA's training is limited to a few specific areas. For example, GITA provides training to agencies in designing their Web sites so that they are consistent with GITA's standards.

AzGU, which is overseen by a governing board of state agencies, designs, implements, and administers a state-wide employee training program. AzGU offers training on a variety of subjects that are applicable to many agencies. These include IT-application training, such as the Arizona Financial Information System (AFIS), and Microsoft applications such as Windows and Word. Courses also include nontechnical training such as stress management and leadership courses.

GITA uniquely positioned to identify state-wide IT training needs—While there is no systematic method in place to identify training needs, GITA could help identify and address these needs. Auditors' interviews with IT officials in other state agencies indicated that some agencies have unmet training needs. For example, five agency Chief Information Officers (CIO) interviewed for this audit indicated that additional training in project management could be beneficial. One CIO indicated that there should be a basic project management standard for IT project managers and that GITA could ensure there is adequate training to meet agency needs.

Although GITA is not charged by statute to address training, it has access to a variety of information that could help it systematically identify state agency training needs. For example,

- **GITA works with two IT planning groups that could assist it in identifying future agency training needs**. Specifically, GITA staff chair the state CIO Council. The CIO Council is an advisory committee consisting of the CIOs representing 26 state agencies or other organizations. The Council provides GITA with advice and support on IT issues affecting agencies state-wide. As representatives of their agencies, the CIOs could also provide input as to the IT training needs of their agencies. GITA also participates in ITSAC, which has identified a number of IT security needs, including the need to develop an awareness program for the State's security standards. While ITSAC is developing an awareness program, GITA could work with ITSAC to determine if a more formal training program is necessary.

- **GITA receives information from agencies that could help identify their future training needs**. Specifically, GITA annually reviews and approves agencies' IT strategic plans. These plans include information on the state agency's long-term plans, issues that face the agency, and their future goals that could reveal the agency's training needs. Moreover, GITA also reviews and approves agency IT projects. As such, GITA is in a position to identify agency training needs based on its knowledge of agency planned software and hardware purchases. By reviewing these plans and future purchases for all agencies, GITA can attempt to identify and address cross-agency training needs.

At least one state contacted as part of this audit identifies agency training needs based on agencies' long-range strategic plans. According to an official from Tennessee's Office of Information Resources, it has developed a training program based on the needs identified within state agency IT technology plans, as well as a review of the current IT technology employed by the state's agencies.

Once it has identified Arizona's training needs, GITA should work with AzGU or other sources to address them. AzGU operates interagency committees that determine which courses to offer state agencies each year and what information should be taught in the courses. According to an AzGU manager, bringing identified state-wide training needs to AzGU through these committees would be a way for GITA to provide input into future AzGU training courses. GITA could work with AzGU to meet these needs or identify other sources, such as outside vendors, to provide or identify sources for technical IT training on a variety of topics. For example, Texas' Department of Information Resources has identified and contracted with private vendors from which state agencies can procure IT training in areas such as IT network security fundamentals and e-business.

GITA should work with AzGU and other sources to address agency IT training needs.

GITA should assist Enterprise Procurement Services with IT procurements

GITA, which has an extensive role in reviewing and monitoring new IT projects, takes a deliberately small role in lending its expertise to the procurement process. For example, it does not assist the DOA's Enterprise Procurement Services (EPS) with evaluating bids for potential IT projects.[1] However, there are opportunities for GITA to contribute more extensively without compromising its review and monitoring role.

GITA and Enterprise Procurement Services have defined their roles in IT procurement

—A 2003 Auditor General report (Auditor General Report No. 03-1) addressed problems with GITA's negotiation of a $30.6 million software contract and recommended that GITA develop written policies and procedures to guide its development and procurement of state-wide information technology projects. GITA and EPS subsequently agreed to an Interagency Service Agreement that outlined their roles related to IT procurements. EPS is responsible for issuing

[1] In January 2005, the Department of Administration created a new organization, Enterprise Procurement Services, which is responsible for the activities formerly performed by the State Procurement Office.

solicitations and contracts and acts as the contract administrator. GITA can inquire with EPS about agency-specific as well as state-wide IT procurement-related matters, and upon request offer consulting and coordination support to EPS.

GITA retains an important role in helping coordinate IT-related purchases and projects that cross state agencies. For example, as required by the Legislature, GITA helped develop a proposal to consolidate state agency telecommunications services through a private vendor. This effort is intended to provide cost-effective, reliable telecommunications services and a foundation for a state-wide network. GITA worked with the DOA and agency stakeholders to draft the proposal. This contract was awarded on January 21, 2005. GITA also coordinated a pilot project of a Web-based license renewal system that other state agencies can adopt. According to a GITA manager, several state agencies identified the need to make their licensing processes available through the Internet. As a result, GITA helped the Department of Real Estate obtain funding and work with a vendor to develop the project. As of February 2005, GITA officials said two other agencies have committed to adopting this program rather than independently developing their own systems. GITA should continue to identify opportunities to coordinate IT procurements across agencies and should consider steps taken in other states to identify additional opportunities. For example, Minnesota's Office of Technology works with a committee of governmental entities in the state to identify technology products and services that can benefit from timely, aggregated purchasing.

GITA can provide expertise to help review vendor proposals.

GITA has the opportunity to provide expertise to more procurements

—While GITA has pursued opportunities to identify and coordinate IT purchasing opportunities, it has not brought its expertise to assist in the contracting process itself. More specifically, GITA could help review vendor proposals by participating in the formal evaluation committees that are composed of three to five experts to review vendor proposals and recommend which vendors should be selected. GITA has declined to participate in these evaluation committees, citing its concern that participation might affect its ability to oversee the project development. As Finding 2 (pages 21 through 30) discusses, GITA has a statutory responsibility to monitor the completion of IT projects. However, there is no legal conflict in these roles, and GITA's participation on these committees may be very useful. For example, according to one EPS official, GITA can provide valuable technical assistance to these committees to help ensure that the State selects the best vendor possible.

Two IT agencies in other states employ a process that involves them in procurement decisions, while still carrying out oversight duties once the project commences. For example, Texas' Department of Information Resources participates in a team that reviews solicitations for any contract over $1 million. The same team also oversees projects after they begin development. In addition, according to one Florida official, their State Technology Office participates in evaluation committees that recommend vendors for selection, and also selects projects to monitor as they are implemented. Therefore, GITA should reevaluate its practice of not participating in evaluation committees and develop criteria with EPS to define when it will participate on these committees.

GITA has improved its State-Wide Strategic IT Plan

GITA has improved its State-Wide Strategic IT Plan by increasing the use of stakeholder input and adding performance measures. In developing the 2005 plan, which is still in its draft form, GITA used state agency IT plans and discussed the plan with stakeholders to help it develop the goals. For future plans, GITA should continue to seek input from stakeholder groups such as ITAC and the CIO Council. In contrast to the 2004 plan, GITA has also added performance measures to the 2005 plan to help it measure progress made toward achieving the goals.

IT strategic plan designed to set direction for the State—GITA developed a 2004 State-Wide Strategic IT Plan and is in the process of updating this plan for 2005. The plan sets forth broad goals that set the strategic direction for Arizona's use of IT in targeted areas in 2005 and for several years after. Auditors reviewed and evaluated the plan by comparing it to the Office of Strategic Planning and Budgeting (OSPB) *Managing for Results: 1998 Strategic Planning and Performance Measurement Handbook*. GITA's draft 2005 plan includes some appropriate planning features, such as core values that reflect what qualities the plan holds important and guiding principles used to accomplish a state-wide IT vision. The plan also includes five broad, future-oriented goals that reflect the desired end result of using IT in targeted areas over the next 2 to 3 years: making government more accessible, enhancing economic development, increasing privacy and security, sharpening efficiency, and improving governmental effectiveness.

GITA has improved stakeholder input into the planning process—GITA annually reviews and approves agencies' strategic IT plans that include information on agency IT trends, issues, and goals. While GITA did not incorporate these agency-identified issues into the 2004 State-Wide Strategic IT Plan, the 2005 plan includes key issues identified by individual agencies in their strategic IT plans and in some cases quantifies the percentage of agencies that identified particular issues. For example, GITA found that nearly one-third of state agency strategic IT plans included a goal to develop or improve online access to agency information or services. According to a GITA official, in response to this information, GITA increased its emphasis on making electronic government services accessible to Arizona citizens by making it a goal in the 2005 plan.

GITA has enhanced the use of stakeholder input in developing the State-Wide Strategic IT Plan by involving ITAC and the CIO Council. According to a GITA official, GITA discussed the 2005 State-Wide Strategic IT Plan with agency CIOs and ITAC.

The discussions focused on the information contained in the plan and how it could be made more helpful to agencies. For future plans, GITA should continue to seek input from stakeholder groups such as ITAC and the CIO Council. Involving these stakeholders in the process is valuable in further identifying issues found in multiple agencies and further ensures the State-Wide Strategic IT Plan addresses goals important to the agencies. According to OSPB's handbook, obtaining input from key stakeholders is important and can provide valuable information during the planning process.

GITA has improved its ability to measure plan progress—Although GITA's 2004 State-Wide Strategic IT Plan lacked important features designed to help ensure that the plan and its goals were implemented, the 2005 plan has added performance measures. While the 2004 plan set broad state-wide goals, it lacked performance measures to measure progress toward achieving the goals. However, according to the OSPB's handbook, these are important components of strategic plans. By contrast, in the 2005 plan, GITA has added performance measures to each of the five goals. For example, GITA's goals to make services accessible to citizens include a measure of the number of transactions available on the Internet via the State's Web portal.

Recommendations

1. GITA needs to take the following steps to improve state agency compliance with security and privacy standards:

   a. Develop a state-wide security plan that comprehensively addresses identified security and privacy weaknesses.
   b. Consider designating a staff member to serve as a Chief Security Officer for the State.

2. GITA should take the following steps in order to strengthen IT privacy standards:

   a. Revise its privacy standards to ensure that they are comparable to those used by government and private industry.
   b. Revise its TESA form to ensure it requires agencies to report compliance with all aspects of state privacy standards.
   c. Explore designating a staff member to serve as the Chief Privacy Officer for the State.

3. GITA should take the following steps to identify and address state agency IT training needs:

   a. Use IT planning groups, such as the CIO Council, and information from state agencies, such as their IT strategic plans, to systematically identify agencies' IT training needs.
   b. Work with AzGU or other training sources to address these needs.

4. GITA should take the following steps to increase its role in IT procurements:

   a. Identify opportunities to coordinate IT purchasing across agencies, including considering steps taken by other states to identify these opportunities.
   b. Reevaluate its practice of not participating on IT proposal evaluation committees and develop criteria with Enterprise Procurement Services defining when it will participate.

5. For future State-Wide Strategic IT Plans, GITA should continue to seek input from stakeholder groups such as ITAC and the CIO Council.

FINDING 2

GITA should strengthen IT project reviews and better help agencies manage IT projects

GITA should make some improvements to its IT project review-and-approval process and better assist agencies with project management. Although GITA's project review-and-approval process addresses several key areas of agencies' proposed projects, it could be improved if GITA sought statutory changes and developed criteria allowing it to focus its reviews on more expensive, potentially risky projects. Additionally, GITA should require more detail from agencies in order to better evaluate the justification for each project. Once these changes have been made, GITA should reassess the staffing needs and skills required for its project review function to ensure the most effective review. Finally, auditors identified a number of steps used in other states to help keep projects on track, such as conducting training programs for agency project managers and establishing standards for project management. Similar efforts by GITA could help Arizona agencies avoid project delays or costly overruns on future projects.

GITA and ITAC responsible for reviewing and monitoring state-wide IT projects

GITA or ITAC reviews and approves agency IT projects.

GITA reviews and approves the justification for major IT projects and monitors these systems as they are developed. According to one former legislator who sponsored the legislation, at that time a major state IT system had experienced significant cost overruns. The project review process was intended to help prevent future projects from experiencing similar overruns.

Although GITA is responsible for reviewing all projects costing $25,000 or more, ITAC must approve some projects in order for the Joint Legislative Budget Committee and the Office of Strategic Planning and Budgeting to recommend funding for it. Statute requires GITA to review and approve all IT projects costing from $25,000 up to $1 million. While GITA reviews and makes recommendations concerning projects that cost more than $1 million, ITAC retains the authority to approve these projects.[1] According to GITA's records, in fiscal year 2004, agencies submitted 87 projects, and GITA approved, or approved with stipulations, 66 and forwarded 19 to ITAC. ITAC approved or approved with stipulations 15 of them.

As part of the review-and-approval process, agencies must submit an analysis of each project's justification on a Project Investment Justification (PIJ) form. This form requires agencies to provide a variety of information, such as a project description and a justification of its value to the State. A GITA staff member then reviews this information and follows up with the agency if the PIJ is incomplete or if additional information is required to evaluate the project. In 1999, the National Association of State Information Resource Executives recognized Arizona's PIJ process by granting an award for outstanding achievement. Other states have adopted similar processes in which the head of a comparable agency reviews agency IT projects. According to the NASCIO *2003-2004 Compendium of Digital Governments in the States*, 41 other states have an approach similar to Arizona's for reviewing projects.

After project approval, GITA monitors the project's implementation.

After GITA or ITAC approves the project and the agency submitting the application obtains funding and procures any necessary materials or expertise, GITA then monitors the project's implementation. The agency is responsible for implementing the project and reports its status to GITA. According to GITA, the frequency and the level of reporting required is based on a number of factors, including the project's size and complexity. For example, a small, straightforward project such as replacing PCs may require a report from the agency to GITA only at the end of the project. In contrast, a software development project could require quarterly or even monthly status reports. If a project falls behind schedule or exceeds its budget, GITA may increase the reporting frequency. GITA has statutory authority to temporarily suspend project expenditures if it determines that the project is at risk. However, GITA management indicated that taking this action involves complicated elements, such as the State's best interests and contractual obligations that must be addressed before taking that action. According to GITA management, when it determines that projects are at risk, it will work with the agency to identify the most appropriate course of action and, if necessary, suggest that the agency voluntarily suspend the project without GITA's intervention. While GITA indicated it is willing to suspend projects where appropriate, agencies have willingly suspended their projects without GITA intervention.

IT project review process can be improved

Although GITA's project review and approval process is relatively comprehensive, GITA can further improve it. The current $25,000 statutory threshold for a required GITA review means that GITA must review many relatively low-cost projects. A higher

[1] ITAC is established in A.R.S. §41-3521 and relies on GITA staff to assist with its duties.

threshold, together with appropriate financial and risk-based criteria, would help focus reviews on the more significant projects. Requiring agencies to submit additional information about these projects would also help in evaluating whether a sufficient need and justification exists for the project. Finally, GITA needs to evaluate whether the current review process focuses sufficient expertise on the project.

PIJ form addresses several key areas—The project review process requires that state agencies show the need for their IT project including planning requirements, and represents an independent review of the proposed project. According to one agency CIO interviewed during the audit, simply requiring agencies to develop this information could help agencies plan their IT projects. Specifically, GITA requires agencies to use the PIJ form to report planning information about a proposed project in several areas:

- **Business and Technology Assessment**—The agency must submit a narrative project overview; a description of the existing situation and problem; the proposed changes and objectives; a general description of the proposed technology; a yes-or-no response to whether the project complies with GITA's Enterprise Architecture standards (along with an explanation if it answers "no"); viable alternatives to the proposed project; a list of major deliverables, personnel roles, and responsibilities; and the project schedule.

Enterprise Architecture (EA) is a common set of software, hardware, network, and other IT standards adopted by GITA that agencies are required to follow. The EA standards facilitate IT applications to business objectives by describing a direction for state IT activities based on principles, standards, and best practices.

- **Summary of the Public Value and Benefits**—The agency must assign a self-assessed rating of the degree to which the improved management or performance brings new value to citizens. The score can range from 0 (no public benefit) to 5 (extensive benefit), and the agency must provide written justification of a score of 4 (substantial benefit) or 5. The agency must also identify the benefits to be gained by completing the project and estimate any potential dollar savings. The agency must submit detailed calculations for any item showing savings greater than $50,000.

- **Financial Assessment**—The agency must submit an estimate of the development and operating costs, special terms and conditions, a funding timeline, and funding sources.

- **Risk Assessment**—Depending on the project's value, the agency must conduct a self-assessment of the project's risk in six categories, such as whether the agency has assessed the impact of the project on its business processes, and the level of the agency's skills necessary to complete the project. If the project is over $1 million, a more detailed risk assessment must be performed. The items are structured as yes-or-no questions; "no" responses require an explanation if the project's cost exceeds $1 million.

- **Project Approvals**—The agency must attest that agency management has approved the project; that it is for a critical system; and that it complies with agency policies, rules, and other requirements.

GITA's $25,000 statutory review threshold may be too low.

Focusing project approval on more costly, higher-risk projects may be beneficial

—GITA must conduct reviews on all projects costing $25,000 or more—a threshold that may now be too low. Auditors interviewed project managers from six Arizona agencies who oversaw IT projects and all said the amount was too low. One commented that his agency could easily exceed this limit simply by replacing half of its 65 personal computers. In addition, two agency CIOs also stated that the amount was too low.

A low threshold may mean that GITA must spend considerable time on reviews that may not be as useful as reviews of higher-cost, higher-risk projects. According to GITA records, nearly half of the 87 projects GITA reviewed in 2004 were under $200,000. They included, for example, a $35,000 request to replace 36 batteries used for backup telephone power at the Capitol and a request to spend about $30,000 to add 28 digital phones to one agency's field office in Cottonwood. GITA reviews projects in the order they are received. However GITA's policies require higher-valued projects to be scrutinized more extensively. In the projects auditors reviewed, GITA appeared to perform a more thorough review of more expensive projects as evidenced by the number and type of questions asked. Nevertheless, GITA is required to review and process all PIJs that fit the statutory dollar definition.

GITA should focus on projects with greatest cost and/or risk.

A more cost-effective approach would be for GITA to focus its reviews on those projects that may present the greatest cost and/or risk. This could include project cost, project size and complexity, and the IT capability of agency personnel. Determining whether to review a project's risk based on cost alone may not be effective because in a large agency, a significant amount of money might be spent on a relatively low-risk project. For example, according to GITA records, one large state agency submitted a request to purchase nearly $1.3 million in personal computers so its remote offices could access state agency data systems. On the other hand, a less costly project in a smaller agency, such as a network upgrade or a new software system, may require more scrutiny. Since the current threshold of $25,000 exists in statute, GITA would need to seek a statutory change that would allow it to review only higher-cost and/or higher-risk projects and projects that met other specific criteria.

Agencies with approval authority in some other states have adopted criteria that focus review efforts on more expensive or higher-risk projects. For example, the Kentucky Commonwealth Office for Technology only reviews agencies' IT project proposals over $400,000. California's Department of Finance assigns each state agency a customized threshold under which the agency is not required to submit a project for approval. This threshold is based on the Department of Finance's assessment of each agency's financial capabilities. Washington considers risk factors such as the IT experience and capability of the agency personnel, the size and complexity of the project, and whether the project affects basic infrastructure or multiple agencies in determining whether a proposed project should be reviewed.

Additional information could benefit review process.

Requiring additional information on the PIJ could improve the project approval process—Additional information about the project would also help GITA better evaluate a project's need. In several areas covered in the PIJ, GITA requires agencies to submit only limited justification for their proposals. Specifically:

- Business and Technology Assessment—Although the PIJ form requires agencies to provide a yes-or-no answer as to whether a project is consistent with GITA's Enterprise Architecture standards, an agency must provide details only if it answers "no." An agency answering "yes" is not required to submit information that would allow independent evaluation of the project's adherence to Enterprise Architecture standards. These standards are important because they provide all state agencies with a common framework for information technology. Moreover, according to GITA, the PIJ process is the most important tool the agency has to ensure that agencies meet Enterprise Architecture standards. Therefore an accurate assessment of projects' compliance with these standards is crucial. For example, New York's State Office for Technology requires agencies to describe the technology used in the project and provide enough information for the office to independently determine whether the project meets state standards. According to a New York official, the information is forwarded to experts within this office to assess the project according to their standards. GITA should require agencies to submit more detailed descriptions, regardless of whether they answer "yes" or "no."

- Summary of the Public Value and Benefits—While the PIJ form requires agencies to rate a project's value and benefit in six areas, such as how it will improve customer service and product quality, it requires no justification for a score lower than 4 on a 0-to-5 scale. For example, GITA approved one $48,000 project to upgrade a Web-based database. While the agency indicated that its goal was to better serve the agency and the public, it recorded a 3 (considerable impact on state customers, clients, and citizens) in each area measuring the public value and benefit of the project. As a result, the agency proceeded with the project without ever justifying the project's value. In contrast, Florida's State Technology Office requires agencies to describe how and when the customer, the agency, and the state will realize the business value. GITA should alter the PIJ form to require agencies to provide more detail regardless of the score assigned.

- Risk Assessment—While agencies are required to assess the potential risk of projects to the agency, these assessments are answered with a "yes" or "no," and no explanation is required except for a “no” answer on a project costing more than $1 million. Obtaining detailed answers could help GITA and ITAC better evaluate the agency’s ability to carry out difficult, complex projects. GITA should revise the PIJ form to require detailed information, regardless of how the assessments are answered.

A more formal, comprehensive approach to measuring a project’s risk is taken in Washington. Washington’s Department of Information Services meets with agencies to jointly evaluate and assign each project a risk level. Based on that analysis, agencies are required to develop a risk-management plan for riskier projects.

GITA should reassess the staffing and skills needed to review projects.

GITA should review the staffing and skills required for project approval—If GITA increases the depth of its review, it should also reassess its approach for staffing the review process. GITA currently assigns one staff member to review all proposed projects—87 in 2004. However, thorough review may require additional technical expertise. For example, if GITA requires agencies to provide more information about whether their projects comply with state enterprise architecture standards, review of that information may require increased technical expertise of additional technical staff, or potentially from outside sources. For example, if GITA does not currently possess the technical expertise within its agency, it has the authority to contract for outside assistance. New York relies upon a variety of staff with different skills to assess compliance with state-wide IT standards. For example, according to a New York Office for Technology official, his office draws upon the expertise of more than 20 experts in various IT fields in reviewing each project’s technical merits.

GITA should enhance agency project management efforts

To help ensure that projects stay on schedule and within budget, GITA should take steps to enhance agencies’ IT project management. Good project management techniques are important to project success. Although GITA monitors the progress of projects, there is no guarantee that a project will not experience significant delays or cost overruns. GITA should consider adopting techniques used by other states, such as coordinating project management training, developing guides, adopting project management industry standards, and requiring certified project managers for major IT projects.

Despite monitoring, some projects have delays and overruns—GITA's project monitoring is generally a combination of receiving reports and, when necessary, attempting to work with agency personnel to correct wayward projects. GITA personnel receive status reports from agencies that include the agency's assessment of whether the project is meeting its scheduled deliverables and outcomes. GITA staff may meet with the agency if a project appears to be behind schedule or exceeding its budget, but agency staff continue to manage the project. Despite these monitoring efforts, projects can still face significant budget and schedule overruns. For example, in 1999, the Department of Administration (DOA) began work on identifying, designing, and implementing a new state human resources system that would provide a single system for the administration of payroll, personnel, employee benefits, and other functions for state agencies. To fund the project, DOA issued certificates of participation, which generated approximately $35 million for this project, and obtained a total of $7.5 million in legislative appropriations in fiscal years 2002 and 2003. The certificates were intended to fund the purchase, installation, consulting services, and training costs associated with the development and implementation of the system. According to the contract awarded to IBM, project completion was scheduled no later than July 2003. Because of the project's size and scope, GITA made extensive efforts to monitor this project, including receiving monthly status reports and submitting recommendations to DOA on how to improve the project. However, as of April 2005, not all of the project components were fully implemented, and the project had consumed almost all of its funding.

While GITA has the statutory authority to temporarily suspend the expenditures for the project, it decided not to do so. According to GITA management, it weighed the costs and benefits of suspending the project and decided not to do so because it believed that action was not in the State's best interest. GITA management believed that the State was financially committed to the project, and that suspending the project would lead to unnecessary delays in implementation. Instead of suspending the project, GITA indicated that it worked with the project manager to adjust the project deliverables as necessary to complete the project. While some features were implemented in December 2003, other features of the project have not yet been fully implemented as of April 2005.

GITA could do more to encourage effective agency project management—GITA could help agency efforts to implement projects on time and under budget by adopting techniques used in other states to help facilitate good agency project management. According to four of the five Arizona agency CIOs interviewed, the State could benefit from GITA's providing increased assistance to agencies in project management.

GITA could help facilitate good agency IT project management.

Other states' central IT agencies have implemented several practices designed to help their state agencies manage IT projects. For example:

- **Coordinate training and offer resources to state agency project managers**—According to a 2004 report, a review of project management literature identified success factors that contribute to projects being on time, within budget, and of good quality, including a project manager's skill and competency.[1] To help agencies develop good project management skills, GITA could offer advice and training to state agency IT project managers. For example, New York's Office for Technology has a project management mentoring program that combines classroom lecture with practical experience to create a group of experienced project managers who can manage increasingly complex and expensive projects at state agencies. It also sponsors agency project manager forums to share lessons learned. GITA currently has the authority to adopt state-wide standards or provide consulting services to assist with state agency IT project management.

  GITA could also consider adopting methods to make project management resources more readily available to agency personnel. Specifically, while GITA offers a one-page project management checklist on its Web site, New York's Office for Technology has developed a project management guidebook to promote a common project management methodology for state agencies, which includes information on how to manage procurement and contractors. This guidebook is based on the Project Management Institute's "Project Management Body of Knowledge" (PMBOK), a nationally recognized set of project management best practices.

- **Project Management Standards**—GITA could also follow practices used in other states to ensure that projects are developed using national IT project management standards. A standardized project management system is one such approach used in several states. According to a 1999 Texas survey, 11 states have adopted one or more standards such as the Institute of Electrical and Electronic Engineer's Software Engineering Standards (IEEE) or the Software Engineering Institute's Capability Maturity Model (CMM).[2] For example, following a failed Child Support Enforcement IT project, in 1998, Kansas created state-wide IT project management standards that all agencies were required to adopt. To develop these standards, a governing board researched national and industry best practices. In addition, the state developed a 350-page textbook. The state reports that it saved approximately $6.5 million in just three projects that used the new standards because the projects were completed ahead of schedule or because they avoided federal penalties.

[1] Korin, Kendra, and Laura J. Taplin. "Project Success: A Cultural Framework." *Project Management Journal,* April 2004. 30-45.

[2] Brotbeck, George, Tom Miller, and Dr. Joyce Statz. *A Survey of Current Best Practices and Utilization of Standards in the Public and Private Sectors*. Austin: State of Texas Department of Information Resources, TeraQuest Metrics, Inc., 1999. Kansas, Michigan, Minnesota, North Carolina, Ohio, Tennessee, and Washington adopted CMM standards, California, Missouri, North Carolina, North Dakota, Oregon and Tennessee have adopted PMBOK; California, Michigan, North Carolina, Tennessee, and Washington have adopted the IEEE standards; and California and Washington have adopted the International Organization for Standardization standards.

- **Certified Project Managers**—In addition, some states have developed programs to certify agency project managers, or provide skilled project management assistance. To support its project management methodology, Kansas has created a 120-hour training program for project managers. At the end of the program, participants are certified as Kansas IT Project Managers. Further, according to California's *Statewide Information Management Manual*, medium- and high-risk projects must have independent oversight teams with members trained in industry standard project management and system development methodologies. In addition, Michigan's Department of Information Technology offers a group of senior project managers who are available to manage large information technology projects within agencies. Finally, according to a Texas Department of Information Resources representative, their office assists Texas agencies by maintaining a list of vendors from which agencies can contract for help if needed.

GITA has taken some first steps in this regard. According to GITA, it has decided to adopt a project management standard intended to improve agency IT project management, and is currently exploring how to incorporate an industry model such as the Capability Maturity Model Integration (CMMI). CMMI, the latest development of the CMM standards, provides a model for standardizing and improving processes used to develop systems such as IT software. Organizations meeting CMMI requirements can be evaluated by authorized appraisers as being proficient in using the model. For example, according to an Arizona Health Care Cost Containment System official, it is in the process of being reviewed under CMMI. According to GITA, after it finishes exploring the CMMI standards it may develop standards requiring agencies to use advanced project management methods and techniques for major or critical projects.

Recommendations:

1. GITA should seek legislation removing the requirement to review all projects costing $25,000 or more.

2. GITA should develop criteria that includes project cost and other risk factors to determine which projects should be reviewed.

3. GITA should review its current project investment justification information requirements and require agencies to provide:

   a. More detailed descriptions of how the project will meet state Enterprise Architecture standards in order to independently evaluate whether the project meets these standards.
   b. More details on each project's public value and benefits.
   c. Details on how agencies will measure and address risk factors involved in the projects in order to verify that agencies have appropriately considered and addressed project risk.

4. Once it has reviewed its justification information requirements and developed its review criteria, GITA should reassess its staffing and skill needs for its project-approval process and reassign staff or seek legislative approval for additional staff as appropriate.

5. GITA should ensure that IT projects come in on time and under budget, by reviewing and implementing techniques used in other states' IT agencies to help enhance agency project management, including:

   a. Coordinating project management training and offering resources such as project management guidelines to assist state agency project managers.
   b. Continuing to explore how to incorporate an industry model for standardizing and improving processes used to develop IT systems.
   c. Ensuring that agencies employ qualified project managers, and continuing to explore options for certifying project managers.

SUNSET FACTORS

Government Information Technology Agency

In accordance with A.R.S. §41-2954, the Legislature should consider the following 12 factors in determining whether the Government Information Technology Agency (GITA) should be continued or terminated.

1. **The objective and purpose in establishing the agency.**

   GITA was established in 1996 under A.R.S. §41-3502. GITA has several statutory responsibilities, including adopting state-wide IT standards, providing consulting services to agencies, and studying emerging technologies and evaluating their impact on the State.

   GITA is also charged with evaluating and approving or disapproving proposed agency IT projects. Specifically, GITA reviews IT projects that cost $25,000, or more, while projects that cost over $1 million are reviewed by GITA and submitted to the Information Technology Advisory Committee (ITAC) for review and approval. GITA also monitors agency information technology projects, including expenditure and activity reports, and provides periodic review of these projects.

2. **The effectiveness with which the agency has met its objectives and purpose and the efficiency with which it has operated.**

   Although in general GITA satisfactorily carries out its responsibilities, it can do more to increase its effectiveness. Specifically, in 1998, GITA began developing a set of technical standards for IT, including IT security measures called Enterprise Architecture standards that are intended to provide state agencies with a common framework for information technology. As of February 2004, GITA has adopted over 50 policies, standards, and procedures on a variety of IT subjects such as software, e-mail, and Internet usage standards. Auditors reviewed GITA's Enterprise Architecture policies and related documents for IT security, privacy, and business continuity. The standards appear to be appropriate and provide comprehensive guidelines for agencies to manage IT security systems. However, GITA needs to improve its privacy standards and its process for verifying that privacy standards are met (see Finding 1, pages 11 through 13).

Additionally, GITA's IT project-approval process requires agencies to report planning information such as a business and technology assessment, a summary of public value and benefits, and a risk assessment. However, GITA's current review-and-approval process does not formally focus on projects for which the costs are highest and/or the risks are greatest. GITA should seek legislation removing the requirement that it review all projects costing $25,000 or more, and develop criteria that include project cost and risk factors, as is seen in other states (see Finding 2, pages 22 through 26).

For the projects that meet these new criteria, GITA should require additional information to better evaluate a project's value. For example, GITA currently requires agencies to provide a yes-or-no answer as to whether a project is consistent with GITA's state-wide standards, and only requires details if the answer is "no." Requiring agencies to submit additional information about these projects would also permit a better evaluation of whether the project actually meets these standards. Finally, GITA should reassess whether the staffing and skills dedicated to review these projects are appropriate (see Finding 2, page 26).

GITA should consider adopting techniques used in other states to help ensure IT projects stay on schedule and within budget. Other states have adopted a number of steps to help agencies keep projects on track. GITA should consider techniques such as coordinating project management training for state agency staff, developing guides, adopting project management industry standards, and requiring certified project managers for major IT projects (see Finding 2, pages 27 through 29).

Moreover, although not specifically charged by statute, GITA can further its objectives and purpose by assessing state IT training needs and by helping agencies get the needed training. GITA works with several IT planning groups and has access to state agency IT strategic plans, both of which can help identify state agency training needs. GITA should comprehensively identify these needs, then work with the Arizona Government University (AzGU) to determine whether these needs can be met through AzGU or other sources (see Finding 1, pages 13 through 15).

3. **The extent to which the agency has operated within the public interest.**

GITA operated in the State's best interest by participating in several efforts that involved consolidating purchasing for state agencies. For example, at the request of the Legislature, GITA helped develop a proposal to consolidate state agency telecommunications services through a private vendor. This contract was awarded on January 21, 2005. GITA also coordinated a pilot project of a Web-based license renewal system that can be adopted by other state agencies. According to GITA, two other agencies have committed to adopting this system rather than developing their own. Additionally, GITA staff have been involved with developing a contract for a system that allows the public easier access to health and human services information by phone or through a Web site. Further, as of February 2004, GITA has adopted over 50 policies, standards, and procedures called Enterprise Architecture Standards that serve as guidelines for state agencies. Finally, GITA contracts with IBM to operate the Arizona@Your Service Web portal. This portal is a Web site where users can access electronically delivered state government services. The portal hosts four applications. One sells driver's license information to insurance companies, another issues permits for the Department of Environmental Quality, a third collects DUI information for the Governor's Office of Highway Safety, and the final application is a geographic information system.

However, GITA needs to take steps to address compliance with security standards because state agencies do not always adhere to GITA's security standards. Complying with these standards is important because agencies have experienced penetrations to their IT systems. GITA should take steps used in other states to address identified security concerns, such as developing a state-wide security plan, and consider designating a staff member to serve as a Chief Security Officer for the State (see Finding 1, pages 10 through 11).

Second, GITA needs to take similar steps to address state privacy standards. GITA has developed some privacy standards for state agency information systems. However, GITA's standards for privacy have gaps. For example, there is no requirement that agencies collect only the data needed to accomplish a legitimate business objective or meet a statutory or legal requirement. Therefore, GITA should make sure its privacy standards are complete. Further, GITA should ensure agencies report their compliance with all appropriate privacy standards (see Finding 1, pages 11 through 13).

GITA could also do more to support state IT procurements. For example, while GITA reviews and monitors IT projects, it declines to lend its IT expertise to evaluate bids for potential IT projects. While GITA considers participating in these committees a conflict with its role in monitoring IT projects, there is no legal conflict, and other states use their IT agencies to assist in procurement. Therefore, GITA should reconsider its practice and work with the Department of Administration's Enterprise Procurement Services to develop criteria defining when it will participate on evaluation committees (see Finding 1, pages 15 through 16).[1]

Finally, GITA has not yet developed needed standard contract terms and conditions as recommended in a July 23, 2004, Auditor General management letter. The Auditor General recommended that GITA work with Enterprise Procurement Services to develop standard contract terms and conditions requiring an independent assurance review when state agencies hire vendors to provide certain electronic government services. Such reviews are generally performed by independent audit firms and are an effective means of ensuring that government services are provided in a well-controlled and secure manner. While GITA indicated that these reviews can be helpful, it noted they are costly and should not be undertaken in every contract. As a result, GITA indicated that it would study the feasibility of this as part of adopting a state-wide IT project management methodology, which provides a model for standardizing how to develop projects. GITA is in the process of studying industry models it could use to develop its methodology.

4. **The extent to which the rules adopted by the agency are consistent with legislative mandate.**

   GITA has taken steps to align its rules with its statutes and, according to the Governor's Regulatory Review Council (GRRC), GITA has promulgated all rules required by statute. However, GITA reviewed its rules and found that some need to be amended so as to not conflict with statute. As a result, in April 2004, GITA initiated rulemaking to correct these conflicts.

5. **The extent to which the agency has encouraged input from the public before adopting its rules and the extent to which it has informed the public as to its actions and their expected impact on the public.**

   GITA encourages public input prior to adopting rules by holding public meetings to allow input into its rule-writing efforts. For example, GITA scheduled a public hearing on August 2004 to discuss proposed rule amendments, although no public comments were received.

[1] In January 2005, the Department of Administration created a new organization, Enterprise Procurement Services, which is responsible for the activities formerly performed by the State Procurement Office.

6. **The extent to which the agency has been able to investigate and resolve complaints that are within its jurisdiction.**

   This factor is not applicable, since GITA does not have investigative or regulatory authority.

7. **The extent to which the Attorney General or any other applicable agency of state government has the authority to prosecute actions under enabling legislation.**

   This factor is not applicable because GITA is not a regulatory agency with enforcement or oversight responsibilities relating to the public.

8. **The extent to which the agency has addressed deficiencies in their enabling statutes, which prevent them from fulfilling their statutory mandate.**

   According to GITA, it has never requested additional legislation to address deficiencies in its enabling statutes. However, it has adopted administrative rules as required by statute, and published policies and standards to provide technical guidance to executive branch agencies.

9. **The extent to which changes are necessary in the laws of the agency to adequately comply with the factors in the sunset laws.**

   GITA should seek legislation removing the requirement that it review all projects costing $25,000 or more. Currently, GITA must review projects costing as little as $25,000, some of which are relatively low-risk projects. Some states have a higher threshold for review or include criteria that also require examination of factors such as risk or the experience of the agency developing the project. Changing the criteria should allow staff to focus their review efforts on projects with higher costs and/or risk (see Finding 2, pages 24 through 25).

   Also, the Legislature should consider reviewing GITA's statute to determine whether it should continue to require GITA to develop a state-wide IT disaster recovery plan. GITA is required by A.R.S. §41-3504(A) to develop a state-wide IT disaster recovery plan for the agencies. However, in January 2003, the Governor issued an executive order requiring all agencies to develop emergency response plans. This requires agencies to develop a plan specifying how they will continue the delivery of essential state services and the security of their customers in the event of a human-made or natural disaster. The plans include an information technology component, and agencies submit these plans for review by the Department of Emergency and Military Affairs (DEMA), the Department of Administration, and GITA. According to DEMA and GITA, because of these plans and the new process, there could be a need for the

Legislature to review the statutory requirement for a single, state-wide IT disaster recovery plan.

10. **The extent to which the termination of the agency would significantly harm the public health, safety, or welfare.**

    Terminating GITA would not harm the public health, safety, and welfare. However, it would remove an external review of proposed agency IT projects. State agencies rely on IT projects to aid in the administration of a wide variety of programs, including public safety, medical care, and economic assistance. Evolving requirements in these areas, such as the federal Health Insurance Portability and Accountability Act requirements for medical care, require that these systems be updated to continue to meet public needs. The IT project-approval process is a valuable part of protecting the State's investment in such IT projects and is one of the main reasons GITA was created. Moreover, according to GITA, without appropriate reviews, projects may be more likely to fail to meet their intended purposes, meet deadlines, or experience cost overruns. The process is also designed to coordinate state-wide IT resources and to evaluate the merits of proposed IT projects. As a result, the process encourages a more thorough and systematic consideration of projects at the agency level and provides increased visibility for projects at the state level.

    GITA also plays an important role in establishing standards for a common framework for information technology across state agencies, including standards designed to protect state data and IT systems. As a result, the overall security and privacy of information could be compromised. In 1998, GITA began developing a set of Enterprise Architecture standards to establish a common framework for information technology policies and practices. These standards address areas such as security, privacy, password policies and procedures, firewalls, encryption, and intrusion-detection mechanisms.

11. **The extent to which the level of regulation exercised by the agency is appropriate and whether less or more stringent levels of regulation would be appropriate.**

    This factor does not apply since GITA is not a regulatory agency.

12. **The extent to which the agency has used private contractors in the performance of its duties and how effective use of private contractors could be accomplished**.

    GITA uses private contractors for a variety of purposes, and the audit did not identify any additional functions to contract out. According to GITA, it has used the services of several special IT consultants for various initiatives and projects, such as assisting GITA in developing its Enterprise Architecture standards, developing a proposal for privatizing the State's telecommunications system, and assistance in a project that would allow citizens easier access to social services and emergency information by dialing 211 or accessing a single Web site.

SUNSET FACTORS

Information Technology Authorization Committee

In accordance with A.R.S. §41-2954, the Legislature should consider the following 12 factors in determining whether the Information Technology Authorization Committee (ITAC) should be continued or terminated.

1. **The objective and purpose in establishing the agency.**

ITAC was established under A.R.S. §41-3521 in 1996 and has a variety of duties related to IT. ITAC's primary responsibilities include:

- Reviewing and either approving or disapproving all proposed agency IT projects exceeding $1 million;
- Reviewing GITA's state-wide information technology standards and GITA's state-wide information technology plan;
- Monitoring information technology projects that the committee considers to be major or critical;
- Conducting periodic reviews on the progress of implementing IT projects it approves; and
- Reporting to the Governor, the Legislature, and the Secretary of State at least annually on its activities.

ITAC may also hear and decide appeals made by state agencies regarding GITA's rejection of their proposed IT projects that are less than $1 million. It may also temporarily suspend an IT project's funding if it

ITAC Membership

Membership consists of the following persons or their designees:

- Four members of private industry, appointed by the Governor and subject to senate approval.
- Two directors of state agencies, appointed by the Governor.
- The administrative director of the courts.
- Two members of private industry or state government, appointed by the Governor.
- One local government advisory member and one federal government advisory member, appointed by the Governor.
- The GITA director, who serves as chair but is also an advisory member.
- One advisory member from each branch of the Legislature, appointed by the President of the Senate and the Speaker of the House of Representatives.
- The staff director of the Joint Legislative Budget Committee.

determines a project is at risk of failing to meet its objectives or if it does not comply with the requirements outlined in GITA and ITAC statutes.

2. **The effectiveness with which the agency has met its objectives and purpose and the efficiency with which it has operated.**

ITAC appears to be meeting its objective and purpose. ITAC met 11 times in 2004, and one of its primary duties is to review and approve all proposed IT projects exceeding $1 million. Since 1997, ITAC has reviewed and approved over 100 projects that have been completed or that are currently in progress, with a total development cost of nearly $480 million. During fiscal year 2004 alone, ITAC approved 15 of the 19 projects reviewed.

Finally, ITAC plays a role in state-wide IT strategic planning. GITA is in the process of revising its information technology strategic plan, and according to GITA, as part of that process GITA is asking ITAC to review drafts and intends to include their suggestions in the plan.

3. **The extent to which the agency has operated within the public interest.**

ITAC generally operates in the public interest by reviewing all proposed IT projects exceeding $1 million. As part of this process, ITAC examines the agency's justification for the projects and can try to improve them by attaching conditions that the agency must comply with before the project can proceed. For example, ITAC required that the Arizona Health Care Cost Containment System (AHCCCS) use an approach in its AHCCCS Customer Eligibility project to make the software being developed available for use by other state agencies in similar applications. Further, ITAC occasionally requires agencies to perform additional analysis and provide additional justification for proposed projects. For example, in 2001, ITAC initially disapproved the Arizona Department of Administration's (DOA) Human Resources Information System because the 14-month implementation schedule appeared to be overly optimistic and ITAC wanted a contingency plan to extend the life of the current system if the new system did not become operational by January 2003. The DOA's contingency plan called for the continued use of the current system. Because the Human Resources Information System did not become operational as scheduled, the previous system had to remain in use.

4. **The extent to which the rules adopted by the agency are consistent with legislative mandate.**

   ITAC does not have its own administrative rules, but it is mentioned in GITA's rules as the reviewer of GITA-processed PIJ submissions that fall within its jurisdiction.

5. **The extent to which the agency has encouraged input from the public before adopting its rules and the extent to which it has informed the public as to its actions and their expected impact on the public.**

   ITAC does not have rules of its own and as such has not sought public comment.

   ITAC meetings are open to the public. According to ITAC, its meetings are attended by persons such as agency representatives and vendors.

6. **The extent to which the agency has been able to investigate and resolve complaints that are within its jurisdiction.**

   This factor is not applicable since ITAC does not have investigative or regulatory authority.

7. **The extent to which the Attorney General or any other applicable agency of state government has the authority to prosecute actions under enabling legislation.**

   This factor is not applicable, since ITAC does not have regulatory authority.

8. **The extent to which the agency has addressed deficiencies in the enabling statutes, which prevent them from fulfilling their statutory mandate.**

   ITAC has not identified any statutory deficiencies.

9. **The extent to which changes are necessary in the laws of the agency to adequately comply with the factors in the sunset laws.**

   This audit did not identify any changes needed to ITAC's statutes.

10. **The extent to which the termination of the agency would significantly harm the public health, safety, or welfare.**

    Terminating ITAC would not harm the public health, safety, or welfare. However, it would remove an independent review of agency IT projects exceeding $1 million. ITAC, which is composed of members from state government, the Legislature, and the public, has some important responsibilities related to reviewing and approving large IT projects for agencies that have a significant impact on the health, safety, and welfare of Arizona's citizens. By removing this review, the State would lose these individuals' perspectives. Agencies that have had IT projects approved include AHCCCS, the Department of Public Safety, and the Department of Revenue.

11. **The extent to which the level of regulation exercised by the agency is appropriate and whether less or more stringent levels of regulation would be appropriate.**

    This factor does not apply because ITAC is not a regulatory agency.

12. **The extent to which the agency has used private contractors in the performance of its duties and how effective use of private contractors could be accomplished.**

    This factor does not apply because ITAC does not directly contract for services.

AGENCY RESPONSE

JANET NAPOLITANO
GOVERNOR

CHRIS CUMMISKEY
DIRECTOR

STATE OF ARIZONA
GOVERNMENT INFORMATION TECHNOLOGY AGENCY
100 N. 15th Avenue, Suite 440
Phoenix AZ 85007

TO: Debbie Davenport, Auditor General

CC: Melanie Chesney, Director, Performance Audit Division
Lisa Eddy, Performance Audit Manager
Jay Dunkleberger, Performance Audit Senior
Max Ivey, Deputy Director, GITA
DJ Harper, Communication & Outreach Manager, GITA

FROM: Chris Cummiskey

DATE: June 23, 2005

SUBJECT: Response to Sunset Audit Report

The Government Information Technology Agency appreciates the work of the Office of the Auditor General in conducting this sunset audit. The professionalism of the auditors should be commended.

GITA agrees with the findings in the report and will implement eight of the recommendations. In Finding Two, Recommendations 1 and 2, GITA will conduct an assessment before deciding on a course of action. Specific responses to your findings are found on pages 2-4.

There is one point of concern. In several places, the report compares GITA with other IT agencies across the country. Though GITA believes this is a good method to determine best practices, it should be noted that the organizational structure and levels of authority vary widely from state to state. For example, while GITA is mostly a strategic planning and oversight agency, many state IT agencies have strategic planning, oversight, and operational responsibilities. This difference in agency mission/organization allows other states access to tools in managing IT that are not available to GITA.

GITA Response to Finding One

1. GITA needs to take the following steps to improve state agency compliance with security and privacy standards:

a. Develop a state-wide security plan that comprehensively addresses identified security and privacy weaknesses.

The finding is agreed to and the recommendation will be implemented.

b. Consider designating a staff member to serve as a Chief Security Officer for the State.
The finding is agreed to and the recommendation will be implemented.

2. GITA should take the following steps in order to strengthen IT privacy standards:

a. Revise its privacy standards to ensure that they are comparable to those used by government and private industry.

The finding is agreed to and the recommendation will be implemented.

b. Revise its TESA form to ensure it requires agencies to report compliance with all aspects of state privacy standards.

The finding is agreed to and the recommendation will be implemented.

c. GITA should explore designating a staff member to serve as the Chief Privacy Officer for the State.

The finding is agreed to and the recommendation will be implemented.

3. GITA should take the following steps to identify and address state agency IT training needs:

a. Use IT Planning groups, such as the CIO Council, and information from state agencies, such as their IT strategic plans, to systematically identify agencies' IT training needs.

The finding is agreed to and the recommendation will be implemented.

b. Work with AzGU or other training sources to address these needs.

The finding is agreed to and the recommendation will be implemented.

4. GITA should take the following steps to increase its role in IT procurements:

a. Identify opportunities to coordinate IT purchasing across agencies, including considering steps taken by other states to identify these opportunities.

The finding is agreed to and the recommendation will be implemented.

b. Reevaluate its practice of not participating on IT proposal evaluation committees and develop criteria with Enterprise Procurement Services defining when it will participate.

The finding is agreed to and the recommendation will be implemented.

5. For future Statewide Strategic IT plans, GITA should continue to seek input from stakeholder groups such as ITAC and the CIO Council.

   The finding is agreed to and the recommendation will be implemented.

GITA Response to Finding Two

1. GITA should seek legislation removing the requirement to review all projects costing $25,000 or more.

   The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

   GITA agrees that the $25,000 threshold may be too low, however GITA values the broad view of IT that is made possible by reviewing all projects over $25,000. GITA will work with stakeholder agencies to conduct an assessment of possible remedies to ensure that GITA continues to receive adequate information regarding State IT projects, while attempting to reduce the workload for State agencies and allow GITA to focus on higher risk projects.

2. GITA should develop criteria that include project cost and other risk factors to determine which project should be reviewed.

   The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

   GITA agrees that project cost and risk factors should be considered when choosing which projects should be reviewed and how much oversight they will incur during implementation. GITA will work with stakeholder agencies to conduct an assessment of possible remedies to ensure that GITA continues to receive adequate information regarding State IT projects, while attempting to reduce the workload for State agencies and allow GITA to focus on higher risk projects.

3. GITA should review its current project investment justification information requirements and require agencies to provide:

   a. More detailed descriptions of how the project will meet state Enterprise Architecture standards in order to independently evaluate whether the project meets these standards.

      The finding is agreed to and the recommendation will be implemented.

   b. More details on each project’s public value and benefits.

      The finding is agreed to and the recommendation will be implemented.

   c. Details on how agencies will measure and address risk factors involved in the projects in order to verify that agencies have appropriately considered and addressed project risk.

      The finding is agreed to and the recommendation will be implemented.

4. Once it has reviewed its justification information requirements and developed its review criteria, GITA should reassess its staffing and skill needs for its project approval process and reassign staff or seek legislative approval for additional staff as appropriate.

   The finding is agreed to and the recommendation will be implemented.

5. GITA should ensure that IT projects come in on time and under budget, by reviewing and implementing techniques used in other states' IT agencies to help enhance project management, including:

   a. Coordinating Project management training and offering resources such as project management guidelines to assist state agency project managers.

      The finding is agreed to and the recommendation will be implemented.

   b. Continuing to explore how to incorporate an industry model for standardizing and improving processes used to develop IT systems.

      The finding is agreed to and the recommendation will be implemented.

   c. Ensuring that agencies employ qualified project managers, and continuing to explore options for certifying project managers.

      The finding is agreed to and the recommendation will be implemented.

Performance Audit Division reports issued within the last 24 months

03-05	Department of Economic Security—Child Protective Services—Foster Care Placement Stability and Foster Parent Communication
03-06	Arizona Board of Appraisal
03-07	Arizona Board for Charter Schools
03-08	Arizona Department of Commerce
03-09	Department of Economic Security—Division of Children, Youth and Families Child Protective Services—Caseloads and Training
04-L1	Letter Report—Arizona Board of Medical Examiners
04-L2	Letter Report—Gila County Transportation Excise Tax
04-01	Arizona Tourism and Sports Authority
04-02	Department of Economic Security—Welfare Programs
04-03	Behavioral Health Services' HB2003 Funding for Adults with Serious Mental Illness
04-04	Department of Emergency and Military Affairs and State Emergency Council
04-05	Department of Environmental Quality—Water Quality Division
04-06	Department of Environmental Quality—Waste Programs Division
04-07	Department of Environmental Quality—Air Quality Division
04-08	Department of Environmental Quality—Sunset Factors
04-09	Arizona Department of Transportation, Motor Vehicle Division— State Revenue Collection Functions
04-10	Arizona Department of Transportation, Motor Vehicle Division—Information Security and E-government Services
04-11	Arizona Department of Transportation, Motor Vehicle Division—Sunset Factors
04-12	Board of Examiners of Nursing Care Institution Administrators and Assisted Living Facility Managers
05-L1	Letter Report—Department of Health Services—Ultrasound Reviews
05-01	Department of Economic Security—Unemployment Insurance
05-02	Department of Administration Financial Services Division

Future Performance Audit Division reports

Department of Economic Security—Division of Technology Services

Department of Economic Security—Service Integration