STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Government Information Technology Agency

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Subject

GITA was established in 1996 to adopt state-wide information technology (IT) standards, approve and monitor state agency IT projects, provide consulting services to agencies, and study emerging technologies and evaluate their impact.

Our Conclusion

GITA needs to provide stronger leadership for the State's IT security, privacy, training, and procurement. In addition, GITA could improve its review of agency IT projects by focusing on riskier and/or more expensive projects, and by requiring more detail about projects during the review-and-approval process.

2005

June • Report No. 05 – 03

GITA Needs To Provide Stronger Leadership on State IT Issues

As the State's central IT agency, GITA is the only agency in a position to provide leadership in five critical areas of IT management:

- **Security**—Ensuring that agencies follow standards to keep hackers from breaking into IT systems.
- **Privacy**—Ensuring that agencies protect personal information they collect and do not collect more personal information than they need.
- **Training**—Ensuring that state IT personnel are trained.
- **Procurement**—Helping the State evaluate IT contract proposals.
- **Planning**—Providing sound, strategic direction for state-wide IT needs.

Ensuring that agencies follow IT security standards

GITA has established a comprehensive set of standards covering such areas as creating and changing user accounts, controlling and monitoring who accesses state agency systems, and protecting against viruses.

Many agencies do not comply with standards—Many agencies are exposing their IT systems to potential attacks by failing to adhere to the State's network security standards.

GITA requires agencies to self-report compliance with the 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. Based on a review of the reports from 11 agencies with significant IT spending, we discovered that 8 had not fully implemented at least 1 of the 10 network security standards.

Logo: Provided by GITA.

One agency did not follow standards regarding passwords. A hacker gained access to some of the agency's databases and erased them before the agency detected and resolved the problem.

Many agencies are also failing to comply with virus protection standards. Five of the 11 agencies had not fully implemented the standards for virus protection. In 2004, agencies reported 44 incidents of virus infections.

GITA should develop a state-wide security plan—Although GITA has taken some steps to address security deficiencies with individual agencies, it has not developed a comprehensive plan to address security on a state-wide level. Other states have plans that assess the number of security deficiencies and the training and funding needed to address them.

Because security is such a critical issue, GITA should consider designating a staff member to serve as the State's Chief Security Officer. Thirty-one states have an IT security officer who coordinates agencies' security policies and develops and implements a state-wide IT security plan.

Strengthening privacy standards

GITA's privacy standards do not address several important aspects of privacy. Further, agencies do not always follow the limited standards that exist.

Standards are incomplete—The standards include two broad policies. One relates to how personal information is collected, maintained, and used on state agency Web sites. The other establishes a method for classifying data according to its risk of loss or misuse.

However, the standards do not contain requirements that agencies:

- Limit data to only that which is relevant, adequate, and not excessive for legitimate business purposes.
- Verify sensitive data about individuals before it is entered in a database.
- Ensure that data is accurate and, where necessary, kept up-to-date.
- Prohibit disclosure for reasons other than the business purpose for which it was collected.

Ensuring agency compliance—Three of the 11 agencies reviewed are not complying with one or more of the existing privacy standards.

To ensure agencies protect the privacy of individuals' data, GITA should also explore designating a staff member to serve as the State's chief privacy officer (CPO). A CPO could take the lead in developing more comprehensive privacy standards, assess gaps in privacy practices, and help agencies come into compliance. Twenty states have established a CPO or similar position.

Identifying training needs

Although GITA is not statutorily required to address state agencies' IT training needs, it is in a unique position to help assess and meet those needs. For example, GITA staff chair the Chief Information Officer's Council, an advisory committee composed of the chief information officers of 26 state agencies and other organizations. The Council could provide GITA with information on IT training needs. In addition, GITA annually reviews and approves agencies' IT strategic plans. These reviews put GITA in a position to identify training needs based on new software and hardware purchases.

Once it has identified IT training needs, GITA should work with the Arizona Government University, a training agency overseen by a governing board of state agencies, or other training sources to address them.

Helping evaluate IT procurements

GITA reviews and approves new IT projects and assists the Department of Administration's Enterprise Procurement Services (EPS) Division in developing proposals. For example, it helped develop the proposal to consolidate agency telecommunications services through a private vendor.

However, GITA has declined to help EPS in evaluating potential vendors. GITA believes that it may not be able to impartially monitor projects if it participates in selecting vendors. However, there is no legal conflict in these roles, and, according to EPS, GITA can provide valuable technical assistance in helping select the best vendors. IT agencies in other states, such as Texas and Florida, evaluate proposals and still perform project monitoring.

GITA has improved the State-Wide Strategic IT Plan

During the course of this audit, GITA drafted a 2005 strategic IT plan setting forth broad goals to guide the State's IT direction. GITA has improved on the processes it followed in developing the prior year's plan. For 2005, GITA obtained and incorporated more stakeholder input by using other state agencies' IT strategic plans, the Information Technology Authorization Committee (ITAC), and other agencies' CIOs.

In addition, in contrast to the 2004 plan, this year's plan includes performance measures that track progress made toward achieving the plan's goals.

Recommendations

GITA should:

- Develop a state-wide IT security plan.
- Consider designating a chief security officer.
- Develop more complete privacy standards.
- Consider designating a chief privacy officer.
- Identify and help address state IT training needs.
- Assist Enterprise Procurement Services in evaluating prospective IT vendors.

GITA Should Strengthen IT Project Reviews and Better Help Agencies Manage Projects

GITA can help the State achieve greater success in implementing major IT projects. GITA can improve its review of proposed IT projects and help agencies to better manage projects after they are approved.

Project reviews

GITA reviews and approves the justification for major IT projects proposed by state agencies. Statute requires that GITA review projects valued at between $25,000 and $1 million. For projects valued at more than $1 million, GITA reviews and makes recommendations to ITAC, which has approval responsibility for these projects.

The Project Investment Justification (PIJ) form that agencies use to justify their IT projects addresses several key areas, including:

- A business assessment describing the current situation and need.
- An assessment of whether the project complies with the software, hardware, network, and other standards prescribed by GITA.
- A summary of the project's public value and benefits.
- A financial assessment of the project cost, the funding sources, and when funding is needed.
- A risk assessment of certain areas such as the agency's skills needed to complete the project.

GITA should base reviews on risk—Per statute, GITA reviews projects that cost at least $25,000. However, this threshold may now be too low. Almost half of the projects it reviewed in 2004 were under $200,000.

A more effective approach would be for GITA to focus on projects with the greatest cost and/or risk. For example, one low-risk, high-priced request was by an agency purchasing $1.3 million in personal computers to provide remote offices with access to the agency's data systems. However, a smaller agency's new software system or network upgrade may cost less but require more scrutiny.

Low-Cost/Low-Risk Projects

- A $35,000 project proposed to replace 36 batteries used for backup telephone power at the Capitol.
- A $30,000 project proposed to add 28 digital phones to a field office in Cottonwood.

GITA should obtain more information—GITA's evaluation of proposed projects is based on limited information. Many of the questions on the PIJ form require an agency to provide details only if the agency answers "no" to the question. For example, an agency that answers "yes" to the question about whether the project complies with GITA's standards does not have to provide any information to show whether it really does comply. Regardless of whether an agency answers "yes" or "no," GITA should obtain sufficient detailed information for each of its questions to allow it to review whether a project is compliant.

Improving IT project management

GITA's monitoring of IT projects is generally a combination of receiving reports and, when necessary, working with an agency to get its project back on track. GITA receives status reports on the progress of projects, but projects can still face significant budget and schedule overruns.

However, project management literature and interviews with agency CIOs suggests GITA can have even greater impact on the success of projects by helping ensure agencies have trained project managers. GITA should explore strategies used in other states to increase project managers' skills. GITA can do this in a variety of ways, including offering advice and training, providing materials such as project management guidebooks, providing consulting, and adopting standards. For example, one state has a project management mentoring program using experienced managers and also holds project management forums to share "lessons learned." Other states have developed certification programs for project managers.

Recommendations

GITA should:

- Seek legislation to remove the requirement that it review all projects costing $25,000 or more.
- Develop criteria including cost and risk to decide which projects to review.
- Review its PIJ form and require more justification from agencies.
- Help develop project management skills among agencies' staff.

TO OBTAIN MORE INFORMATION

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

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

Contact person for this report:
Lisa Eddy

Government Information Technology Agency (GITA)

REPORT HIGHLIGHTS
PERFORMANCE AUDIT
June 2005 • Report No. 05 – 03