A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Management Letter

State of Arizona

Year Ended June 30, 2006

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.

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.azauditor.gov

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

October 31, 2007

William Bell, Director
State of Arizona
Department of Administration
100 North 15th Avenue
Phoenix, AZ 85007

Dear Mr. Bell:

In planning and conducting our single audit of the State of Arizona for the year ended June 30, 2006, we performed the following as required by *Government Auditing Standards* (GAS) and Office of Management and Budget (OMB) Circular A-133:

- Considered the Department's internal controls over financial reporting,
- Tested its internal controls over major federal programs, and
- Tested its compliance with laws and regulations that could have a direct and material effect on the State's financial statements and major federal programs.

Specifically, we performed tests of cash receipts, receivables, cash disbursements, payables, transfers, payroll, purchasing, buildings and equipment, financial reporting, the Schedule of Expenditures of Federal Awards, the Statewide Cost Allocation Plan, and the Donation of Federal Surplus Personal Property Program.

All audit findings that are required to be reported in the GAS or OMB Circular A-133 reports have been included in the State of Arizona's Single Audit Reporting Package for the year ended June 30, 2006, and have been communicated to your staff. In addition, our audit disclosed internal control weaknesses and instances of noncompliance with laws and regulations that do not meet the reporting criteria. Management should correct these deficiencies to ensure that it fulfills its responsibility to establish and maintain adequate internal controls and comply with laws and regulations. Our recommendations are described in the accompanying summary.

This letter is intended solely for the information of the Arizona Department of Administration and is not intended to be and should not be used by anyone other than the specified party. However, this letter is a matter of public record, and its distribution is not limited.

Should you have any questions concerning its contents, please let us know.

Sincerely,

Dennis L. Mattheisen, CPA
Financial Audit Director

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

TABLE OF CONTENTS

The Benefits Office should strengthen controls over claims payment processing for the State's self-funded health insurance program

Beginning in fiscal year 2005, the State implemented a self-funded health insurance program for its employees and retirees, and their dependents. The Department of Administration's Benefits Office is responsible for administering this program. For healthcare claim payments, the Benefits Office contracted with four vendors to process and pay all medical and prescription drug claims for the program. These contractors processed approximately $552 million in medical and prescription drug claims during the fiscal year. Therefore, it is critical that the Benefits Office require these vendors to have an effective system of internal control in place to ensure that claim payments are accurate and appropriate. However, the Benefits Office did not fully accomplish this objective. Specifically, three vendors that were responsible for repricing medical claims did not receive independent audits to ensure that this was done in accordance with their contracts with the State because the Benefits Office did not include the audit provision in the vendors' contracts. Further, the Benefits Office did not perform its own audit of claims paid because these vendors did not provide the Benefits Office with their fee schedules used for payments to medical providers. Finally, the Benefits Office did not compare billing statements from the vendors to the supporting claims reports.

To strengthen controls over the medical and prescription drug claims payment process, the Benefits Office should establish and follow the policies and procedures listed below:

- Establish contractual provisions requiring vendors that reprice medical claims to have an effective internal control system to accurately and appropriately reprice medical claims in accordance with the contracts. Additionally, obtain an independent annual audit of their repricing processing controls to determine whether controls have been placed in operation and are operating effectively.

- Establish verification procedures to ensure the data's appropriateness, completeness, and accuracy. In addition, perform a comparison of vendor billing statements to supporting claims reports in a timely manner.

- Develop procedures and conduct audits of claims-payment data to ensure that claims are paid for allowable services to eligible plan members only, in accordance with vendor fee schedules and the proper application of copayments.

A similar recommendation was previously provided in our Management Letter to the Department of Administration, Benefits Office, dated June 26, 2006.

The State should prepare a disaster recovery and business continuity plan for SPIRIT

The State uses an Internet application called the SPIRIT system to manage its procurement process, including requesting goods and services, publishing bid solicitations, receiving and analyzing vendor bids, and awarding contracts. Therefore, it is vital that the State Procurement Office (SPO) have a contingency plan so that state agencies can still purchase goods and services in the event of a major computer hardware, software, or telecommunications failure. However, SPO did not have a disaster recovery and business continuity plan for SPIRIT.

To help ensure that the State can provide for the continuity of its procurement operations and to help prevent data loss in the event of a major system, equipment, or telecommunications failure, the SPO should develop and implement a disaster recovery and business continuity plan. The plan should include the following:

- Roles and responsibilities of employees assigned to disaster recovery teams and emergency telephone numbers to reach them.

- A written equipment-backup agreement to support hardware needs and software requirements, including a designated physical facility.

- A list of highest-to-lowest priority applications, required recovery times, and expected system performance.

- A list of specific hardware, software, peripherals, and supplies needed, and a source for obtaining these items.

- System- and user-operating procedures.

- A list of procedures for processing critical transactions, including forms and other necessary documents.

A similar recommendation was previously provided in our Management Letters to the Department of Administration, State Procurement Office, dated June 26, 2006 and February 7, 2005.

The State Procurement Office should implement controls over the SPIRIT database management and operating system software

Proper configuration of SPIRIT's database management and operating system software helps prevent intruders and unauthorized users from making changes to programs and databases, and prevents virus attacks. Although the SPO, the Information Processing Center, and the Data Resource Management Group have taken steps to address security risks, some controls were inadequate to properly secure data and system access. For example, some system utilities were not enabled to help ensure that file access rights were controlled to prevent unauthorized access to critical areas within the system. Also, software updates, critical patches, and network anti-virus software were not installed, which could leave the system and data vulnerable to attacks. In addition, audit log files were not reviewed regularly to detect unauthorized access or changes to the database or operating system. As a result, unauthorized activity could occur and go undetected.

The SPO should ensure that controls built into the database management and operating system software are implemented to adequately safeguard SPIRIT from unauthorized use and changes. The following controls will help to secure the system:

- Ensure that file access rights are controlled to prevent unauthorized access to critical areas within the system.
- Install and maintain critical patches as they are released.
- Install upgraded database and operating systems software in a timely manner.
- Use logs and system activity reports to detect any unauthorized changes.

A similar recommendation was previously provided in our Management Letters to the Department of Administration, State Procurement Office, dated June 26, 2006 and February 7, 2005.

The State's financial statements should include an accrual for all sick leave liability

When the Department of Administration, General Accounting Office (GAO), prepares the State of Arizona's Comprehensive Annual Financial Report, only the current portion of sick leave liability due to retiring employees is accrued. Generally, the

Governmental Accounting Standards Board's Statement No. 16—Accounting for Compensated Absences requires the accrual of sick leave liability for all employees be reported in the financial statements.

To help ensure the compensated absence liability in the State's financial statements is properly stated, the GAO should develop a method to calculate this liability based on past data accumulated or arrange for an actuarial valuation of the liability. Otherwise, the GAO should provide evidence that this liability is immaterial to the State's financial statements.

The State's disaster recovery plan for AFIS should be completed

The Department of Administration, Information Services Division, operates the Arizona Financial Information System (AFIS). Should the AFIS fail, the State would be unable to process critical transactions necessary to ensure its daily operations. Therefore, it is vital that the State maintains an AFIS disaster recovery plan so that state agencies can continue to process transactions in the event of a major computer hardware, software, or telecommunications failure. However, the AFIS disaster recovery plan has not been completed.

To help ensure that critical jobs can be processed in the event of a major hardware, software, or telecommunications failure, the Information Services Division should complete the AFIS disaster recovery plan as soon as possible. The plan needs to be revised or completed to include the following:

- A current disaster recovery call list, including telephone numbers for personnel for all of the Department of Administration groups.
- Detailed steps documenting how critical functions would be restored.
- Sections that are fully integrated and written in a user-friendly format.

The State needs to fully develop and test a disaster recovery plan for its HRIS system

The State uses the Human Resources Information Solution (HRIS) to maintain human resources records and prepare payroll. Therefore, it is vital for the State to ensure that it can continue to operate in the event of a system or equipment failure by developing, implementing, and testing a disaster recovery plan. A properly designed disaster recovery plan helps ensure that proper procedures are in place to provide for continuity of operations and that electronic data files are not lost in the event of a disaster. However, HRIS did not have a current and complete disaster recovery plan.

In addition, disaster recovery tests with the contracted provider in July 2005 and January 2006 were unsatisfactory as the HRIS team was not able to adequately restore the HRIS system within a reasonable amount of time. The disaster recovery service contract was canceled on June 1, 2006, due to unresolved problems with the services the contractor provided. As of the end of the fiscal year, there were no formal, off-site, alternative processing arrangements. Consequently, payroll might not be accurately processed if a disaster occurs.

To help ensure that the State can provide for its operations continuity in the event of a major system or equipment failure, the State should fully develop, document, maintain, and test a disaster recovery plan for the HRIS system. The plan should include the following:

- A list of personnel assigned to disaster teams and each team member's emergency phone number.
- Operating procedures.
- Arrangements for a designated physical facility.
- A risk analysis identifying the critical applications, exposures, and an assessment of the impact on the State.
- Arrangements with vendors to support the needed hardware and software requirements.
- Any necessary documents and forms.

Further, this plan should be stored off-site with the backup files, and updated and tested on an annual basis.

The State should strengthen controls over HRIS account management

Account management, which includes the request, approval, establishment, suspension, and termination of user accounts, is an integral part of system security. Therefore, it is vital that the State develop and implement policies and procedures for account management over its HRIS system. However, the State did not have comprehensive policies and procedures over account management for operating system accounts, application administrator accounts, or database management system accounts. In addition, existing policies and procedures were not always followed as some agency users were granted application access without completing all necessary trainings, and in one instance noted, an access request form was not

maintained to document a user's access approval. Further, some agency users were given application access that did not allow for proper segregation of duties, and there was no documented explanation of compensating controls from the users' agencies on file with HRIS. Also, certain operating system accounts, application administrator accounts, and database management accounts are shared among HRIS team members; however, the passwords for these accounts are not routinely changed, and current HRIS policies do not address this issue. Finally, some operating system accounts were not disabled in a timely manner.

To strengthen controls over HRIS account management, the State should strengthen existing HRIS policies and procedures and ensure they are followed to help ensure that:

- All types of user accounts are properly managed.
- Agency users are granted application access only after they have completed the necessary trainings.
- All types of user accounts have a corresponding access request forms, which are maintained to document the proper approval for user access.
- Agency user access facilitates the proper segregation of duties among employees, to the extent practical. If users must be assigned incompatible access rights, the reasons for the assignment and any compensating controls in effect should be documented in the HRIS records.
- All types of user accounts are not shared and passwords are changed on a routine basis.
- Operating system accounts are disabled promptly upon an employee's termination or change in assigned duties.

The State should improve controls over HRIS system changes

Changes to computer programs must be monitored and tested to ensure that a computer system is functioning properly. However, the State did not have adequate written policies and procedures for all types of system changes to its HRIS system, including those that address operating system changes and the testing of application changes. Adequate documentation of these changes was not always maintained. In addition, the system did not generate a log to help monitor such changes.

To help strengthen controls over changes to the HRIS system, the State should:

- Develop adequate written policies and procedures for all types of program changes, including those that address operating system changes and testing of application changes. Further, these policies and procedures should address design, testing, approval, documentation, and implementation of system changes.

- Document all system changes, including an identifying number, program code modifications, test results, approvals, and implementation dates. This documentation would be a valuable resource for planning additional system changes or if a system failure occurred.

- Develop a system-generated log and periodically review it to ensure that all changes were authorized, tested, and properly implemented.

JANET NAPOLITANO
GOVERNOR

WILLIAM BELL
DIRECTOR

ARIZONA DEPARTMENT OF ADMINISTRATION
OFFICE OF THE DIRECTOR
100 NORTH 15th AVENUE • SUITE 401
PHOENIX, ARIZONA 85007
Phone: (602) 542-1500

September 28, 2007

Dennis L. Mattheisen, CPA
Financial Audit Director
State of Arizona
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Mr. Mattheisen:

Attached is the Arizona Department of Administration's response to the Fiscal Year 2006 Single Audit Management letter recommendations. The attached document presents the summary list of recommendations followed by the corresponding division response.

Should you have any questions or concerns please contact us.

Sincerely,

William Bell
Director

cc: Jean Clark
Kathy Peckardt
Patrick Quain
Phil Hamilton
D. Clark Partridge

Arizona Department of Administration
Responses to Audit Findings

Recommendation 1: The Benefits Office should strengthen controls over claims payment processing for the State's self-funded health insurance program

ADOA Response
We concur that the Benefit Services Division (BSD) should take steps necessary to strengthen controls over all aspects of claims processing. To that end, BSD has instituted several procedures, including:

- The actuarial and analytical review of medical claims—individually and collectively—to detect and identify possible fraud, abuse, non-compliance, or insufficient utilization oversight.

- The reconciliation of claims payments to vendor billing requests has begun. The process has been completed for the integrated model from plan inception to current; the process has begun for the non-integrated model.

We concur with the necessity of establishing contractual provisions for vendors that reprice medical claims to establish and maintain adequate internal controls and will be considered as we enter into new contracts. Because contracts are in place and are difficult and costly to modify between RFP cycles, BSD has not reached agreement with all contractors to institute outside audits and provide these to BSD. However, we have been able to modify the Plan Year 2007 agreements with Walgreens Health Initiative (WHI), Harrington Benefit Services, and Unitedhealthcare to provide us with copies of their SAS 70 audit results (collectively accounting for the majority of the State's healthcare claims costs)..

We also concur with the necessity of conducting or having conducted an audit of the internal controls over claims repricing, eligibility, and copayments. It is intended that many of these engagements will be undertaken by the BSD's internal audit unit.

Recommendation 2: The State should prepare a disaster recovery and business continuity plan for SPIRIT

ADOA Response
ADOA, State Procurement Office (SPO) obtained an off-site disaster recovery site as of September 1, 2006 through ADOA's Information Services Division(ISD) with the State's Tri-Agency Disaster Recovery Vendor, IBM. The IBM contract expires on February 29, 2008. Our first disaster recovery (DR) exercise was held in January of 2007, which demonstrated the successful recovery of the Solaris Operating System and the establishment of network connectivity to the Boulder DR site utilizing their hardware and software. The next DR exercise is scheduled for December 2007. The December DR test will include the recovery of all system and application software by ISD technical staff as well as the verification of SPIRIT application functionality by state procurement personnel.

During the meantime, SPO will continue to rely on regular reports generated through SPIRIT containing pertinent solicitation and contract information, so that business continuity can be maintained utilizing a manual, paper based system as used prior to the implementation of SPIRIT.

Recommendation 3: The State Procurement Office should implement controls over the SPIRIT database management and operating system software

The Solaris operating system software and maintenance (release 10) and the Domino software and maintenance (release 7) were successfully implemented in January 2007. The JASS server hardening utility was executed during the Solaris upgrade process. The utility removes all unnecessary utilities/services to ensure the highest level of system security. Regular monitoring of messages and last logins are performed by the ISD system administrators. DRM staff regularly monitors Domino logs. Trend Micro's ScanMail for Domino has been purchased and the installation of the product will be scheduled as soon as the product is received.

Recommendation 4: The State's financial statements should include an accrual for all sick leave liability

We understand the issue associated with the accrual of the sick leave liability for retiring employees. However, the General Accounting Office believes the amount of the liability is not material to the State's financial statements. The benefit achieved in presenting this information in the State's financial statements would be outweighed by the cost of conducting an actuarial study or developing a methodology to calculate the liability.

Recommendation 5: The State's disaster recovery plan for the AFIS should be completed

We concur. We have already updated the disaster recovery call list and will address the other recommendations as we move forward. ADOA continues to make strides in addressing the AFIS disaster recovery risks. Specifically:

- The GAO/AFIS group in conjunction with ISD has conducted AFIS Disaster Recovery testing approximately once per year since September of 2003.
- Detailed technical test plans and schedules were developed each year. A series of tests were performed to address Business Continuity and Disaster Recovery functions with the goal of being able to run a successful batch run in the AFIS and produce warrants from an off-site location.
- Both GAO/AFIS and ISD continue to refine and improve the AFIS Disaster Recovery process each year with increasing success. A successful batch run has not been performed as of yet, but we are hoping to achieve this with the next scheduled set of tests. If a successful batch run is not accomplished, we will refine the test plan and schedule more tests that will occur approximately 8-10 months later.
- The GAO/AFIS and ISD also continue to work with the State agencies on AFIS Disaster Recovery procedures.

The next AFIS Disaster Recovery testing run is scheduled for 12/04/07-12/06/07 through on off-site location in Colorado (same as was used for testing in January of 2007).

Recommendation 6: The State needs to develop and test a disaster recovery plan for its HRIS system

The Department agrees with the recommendation; however we offer the following for clarification:

As recommended by the auditors, HRIS has shifted to a dedicated infrastructure strategy (i.e. "hot site") with a phased approach to data replication. Dedicated servers have been purchased and agreements are being finalized for locating the servers at a secure facility in Tucson.

Recommendation 7: Account access to the HRIS system should be controlled

The Department agrees with the recommendation; however we offer the following comments for the purpose of clarification.

HRIS has instituted a policy of changing passwords to needed operational accounts within the HRIS team on a regular basis, and scripts are being created to remove the need for sharing such passwords in any event; SUDO and other selective-root programs have been purchased and are being used to provide limited, controlled access to such accounts without divulging their passwords, which will be maintained by the HRIS systems administrators. Also, where proper segregation of duties is not possible (in very small agencies), HRIS will ensure that the documented explanation of compensation controls from the users' agencies is on file with HRIS.

Further, HRIS will follow the recommendation to ensure that these new policies and procedures are followed and well-documented.

Recommendation 8: Program changes to the HRIS system should be controlled

The Department agrees with the recommendation; however we offer the following comments for the purpose of clarification.

All HRIS application changes go through a rigorous approval and testing process, including review by the HRIS Change Control Board, strict check-in/check-out procedure for code modules, unit testing with peer-review, and user acceptance testing. Additionally, any substantive changes to the underlying AIX operating system or ancillary programs must be documented and approved via an HRIS Change Control Form (CCF). However, the underlying policy about when to create such CCFs was not documented. HRIS has added two additional systems administrators who are creating more specific policy and procedural documentation for all infrastructure configuration.

Also, HRIS has worked with ISD Security to re-install the latest version of Tripwire on HRIS servers, which provides detailed daily reports on any changes to HRIS, both programmatic and OS-related. ISD has assigned a skilled technician to administer Tripwire management. These Tripwire reports serve as a remote system log and will be closely reviewed on a daily basis to track any changes to HRIS programs or operating systems.

HRIS has also acquired ClearCase version-control and project management software, which will enhance our ability to closely document program code changes, including modifications, test results, approvals, and implementation dates. This will replace our current tracking system, IBM Project Office.