A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Management Letter

Department of Administration

Enterprise Procurement Services

(Formerly the State Procurement Office)

Year Ended June 30, 2004

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.auditorgen.state.az.us

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

February 7, 2005

Betsey Bayless, Director
Department of Administration
100 North 15th Avenue
Phoenix, AZ 85007

Dear Ms. Bayless:

In planning and conducting our audit of the State of Arizona for the year ended June 30, 2004, we considered the Department of Administration, Enterprise Procurement Services' (formerly the State Procurement Office) internal controls over financial reporting as required by *Government Auditing Standards* (GAS), issued by the Comptroller General of the United States.

Specifically, we performed a limited review of internal controls over the paperless electronic procurement system known as SPIRIT.

There are no audit findings that are required to be reported by GAS. However, our audit disclosed internal control weaknesses 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. Our recommendations are described in the accompanying summary.

This letter is intended solely for the information of the Department 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

Background

In January 2004, the Department of Administration, Enterprise Procurement Services (EPS) implemented an online paperless electronic procurement system known as SPIRIT. The system was developed by a technical service and software company. SPIRIT is an Internet application that manages the procurement process, including requesting goods and services, publishing bid solicitations, receiving and analyzing vendor bids, and awarding contracts. The application includes a central supplier registration that enables vendors to create and maintain their own account profiles and indicate the goods or services that they can sell to the State. State agencies prepare requisitions online for desired goods and services. Using SPIRIT, EPS employees work with the agencies to prepare and publish solicitations that notify vendors through e-mail and the EPS Web site of these requests for goods or services. Vendors respond electronically to the solicitation, entering bids and making changes until the closing deadline. Bid information is secured within SPIRIT and remains confidential, until the bid opening. After the solicitation is closed, state employees can evaluate vendor bids online to determine the bid that is most advantageous to the State. Beginning in January 2005, more state agencies will have access to SPIRIT for purchases as EPS begins allowing agencies to contract for goods and services below their delegated purchasing limits.

SPIRIT uses an underlying database management software program for its user access controls, user collaboration, and file and database controls. The software and the related databases and files are run on a server at the Department's Information Processing Center, and the server is maintained by the Department's Information Technology Services Division. The Information Technology Services Division, Data Resource Management Group operates the database management software program.

System administrator access to the database should be restricted

In an online paperless electronic procurement system, controlling and monitoring system access is critical to ensure that vendor bids are confidential and cannot be changed. However, EPS did not have adequate access controls since it did not monitor system administrator activity. Specifically, system administrators had direct access to the SPIRIT databases and could read and change data without being logged into the SPIRIT application. In addition, there were no audit logs generated to

monitor changes to the databases. Also, EPS did not perform criminal background or credit checks on employees who have access to sensitive data. These checks help identify individuals who might be predisposed to or have reason to commit fraud or otherwise change sensitive data.

To help strengthen controls and ensure that unauthorized changes are not made to the procurement system, EPS should establish the following procedures to control and monitor system administrator activity within SPIRIT:

- Require a supervisor to review system activity and monitor system administrator activity for unauthorized changes.
- Remove system administrators from the administrator user group since they should not have direct access to the SPIRIT databases.
- Perform criminal background and credit checks on all employees who have access to sensitive data.

Computer program changes should be controlled

To help ensure that a computer system functions properly, it is essential that changes to computer programs be monitored and tested. However, EPS did not have adequate procedures to control program changes. Specifically, EPS did not have a log or other tracking system to control program changes that are made by the software company, tested by EPS, and placed into operation. A log or tracking system would help control changes and ensure that they are authorized, tested, and properly implemented. In addition, even though EPS tested program changes, it did not document and retain specific program code changes and test results. This documentation would be a valuable resource for planning additional program changes or if a system failure occurred.

EPS should implement the following procedures to help strengthen controls over changes to the SPIRIT system:

- Document all program changes, including an identifying number, program code modifications, test results, and approval and implementation dates.
- Periodically review the log or other tracking system to ensure that all changes were authorized, tested, and approved.

A disaster recovery and business continuity plan should be prepared

When fully implemented, the SPIRIT system will be the State of Arizona's primary procurement system and, as a result, will become critical to the State's operations. Therefore, it is vital that EPS 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, EPS did not have a disaster recovery and business continuity plan for SPIRIT.

EPS should prepare a disaster recovery and business continuity plan as soon as possible to help ensure that electronic data is secured and minimize the length of interrupted computer operations. When completed, the plan should be updated and tested annually. 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 help ensure processing continuity of procurement transactions, including a designated physical facility.
- A listing of highest-to-lowest priority applications, required recovery times, and expected system performance.
- A listing of specific hardware, software, peripherals, and supplies needed and a source for obtaining these items.
- System and user operating procedures.

Database management and operating system software should be controlled

Proper configuration of the database management software and SPIRIT's operating system software prevents intruders and unauthorized users from making changes to programs and databases and prevents virus attacks. Although EPS, 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 unnecessary default system files were not deleted, inappropriate access rights to certain critical files were not removed or disabled, and updated security patches and network anti-virus software

were not installed. 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.

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

- Delete unnecessary default system files and ensure that file access rights are controlled to prevent unauthorized access to critical areas within the system.
- Install updated database and operating system security patches in a timely manner.
- Install and maintain updated network anti-virus software.
- Use logs and system activity reports to detect any unauthorized changes.

JANET NAPOLITANO
Governor

BETSEY BAYLESS
Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

100 NORTH FIFTEENTH AVENUE • ROOM 401
PHOENIX, ARIZONA 85007

(602) 542-1500

January 24, 2005

Ms. Debbie Davenport
Auditor General
2910 North 44th Street
Phoenix, Arizona 85018

Re: Response to Audit Report; SPIRIT

Dear Ms. Davenport:

The Arizona Department of Administration extends its thanks to your staff for the professionalism displayed during the audit of the Enterprise Procurement Services. In response to the recent audit findings, the Department concurs with the findings and plans to implement the recommendations as follows:

1. System Administrator Access to the Database should be Restricted

A process will be implemented for tracking administrator modifications which will include documentation and an approval by an authorized individual for the required modifications. Access cannot be denied as service will be impacted; however, the recommended background and credit checks will be performed. Also, a budget request for FY06 has been submitted for the modification of the application to enable the corrections to be controlled and tracked via the application to facilitate the removal of the system administrators from the system administrator user group.

2. Computer Program Changes should be Controlled

Enterprise Procurement Services will implement a procedure with applicable signature approvals for the tracking and authorization for program changes. The procedure will provide for a log, tracking system and approval process.

3. Disaster Recovery and Business Continuity Plan should be Prepared

Enterprise Procurement Services will work with the Department's internal Information Services Division to develop a plan. The plan will be based upon developing a procedure that captures

snapshots of pertinent SPIRIT information at regular intervals, which could if necessary be utilized by Enterprise Procurement Services to conduct business in a manual, paper process method until such time as normal computer operations are restored.

4. Database Management and Operating System Software should be Controlled

Enterprise Procurement Services will coordinate with the Department's internal Information Services Division to implement the recommended system controls that do not compromise SPIRIT application functionality. To achieve the enhanced database management resources required to facilitate the proper administration and monitoring of the underlying database environment, a budget submittal for FY06 has been submitted, which requests an additional FTE to support the SPIRIT application.

Should you have any questions, please feel free to contact my office.

Very truly yours,

Betsey Bayless
Director

c: Tim Boncoskey, Assistant Director
Paul Shannon, Budget Office