AUDITOR GENERAL

WILLIAM O. MONROE, CPA

STATE BOARD OF ADMINISTRATION
PEOPLESOFT FINANCIALS SYSTEM

Information Technology Audit

SUMMARY

The State Board of Administration (SBA) uses the PeopleSoft Financials System to manage and record its financial activities. Our audit focused on evaluating selected information technology (IT) functions and determining the effectiveness of general and application controls during the period September 1, 2004, through January 31, 2005, including selected actions taken from July 1, 2003. Our primary focus was on controls related to the PeopleSoft General Ledger Module, the Module's interfaces with corresponding systems, and its supporting network. The General Ledger Module of the Financials System is used to journalize and summarize financial activities.

The results of our audit are summarized below:

Finding No. 1: SBA's business continuity plan was under development and did not contain all the elements needed to ensure the continued performance of all the organization's mission essential functions.

Finding No. 2: SBA did not maintain current formal policies and procedures pertaining to various functions within the IT environment.

Finding No. 3: PeopleSoft Financials application program change controls needed improvement.

Finding No. 4: Deficiencies were noted in the administration of access privileges within the PeopleSoft Financials application.

Finding No. 5: Improvements were needed in certain security controls protecting the PeopleSoft Financials System and its supporting network environment, in addition to matters discussed in Findings No. 2, 3, and 4.

BACKGROUND

The State Board of Administration is a constitutional body responsible for the investment management of State of Florida and various other governmental assets. As of June 30, 2004, assets managed by SBA were valued at approximately $130.7 billion. The financial position of SBA is reported in the Florida Comprehensive Annual Financial Report as a blended component unit.

Several IT applications are used in the investment management and financial reporting activities of SBA, including Eagle Straight Through Accounting & Record-keeping (STAR), PeopleSoft Financials, and the Florida Accounting Information Resource Subsystem (FLAIR). The Eagle STAR application integrates with the PeopleSoft General Ledger Module to post all monetary and investment transactions made by SBA. The PeopleSoft application was implemented in 2002, with its web-based version being implemented in 2004. General ledger information is transferred periodically from the PeopleSoft General Ledger Module to FLAIR, the official Statewide accounting system.

Finding No. 1: Business Continuity Plan

A business continuity plan is an effort within an organization to ensure the continued performance of minimum essential functions during a wide range of potential emergencies. This is accomplished through the development of plans, comprehensive procedures, and provisions for alternate facilities, personnel, resources, interoperable communications, and vital records/databases.

Standard business practices provide that the IT portion of the business continuity plan, the IT disaster recovery plan, be a written plan containing, at a minimum, elements such as emergency procedures to ensure the safety of all affected staff members and response and recovery procedures meant to bring the IT operations back to the state they were in before the incident or disaster. An entity's continuity methodology most often incorporates an identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. A formal contract for these types of services is usually required.

During our review of SBA's business continuity plan (plan), we determined that:

- SBA did not document its risk analysis in its development of the plan.
- The plan had not been fully tested.
- The plan was not specifically dated to indicate its creation date or the effective dates of any changes to the plan.

Additionally, during our review of SBA's IT disaster recovery planning efforts, we determined that:

- The business continuity plan did not include an IT disaster recovery plan.
- The business continuity plan listed the Department of Management Services' Shared Resource Center as SBA's alternative back-up or hot site. However, as of January 18, 2005, SBA had not executed an agreement with DMS to use the Shared Resource Center as a back-up site in the event that SBA's data center was not operational.
- System back-ups were performed on a daily basis, but were retained on-site for a duration of one week before being moved to off-site storage.

SBA's ability to continually perform all of its critical functions is at risk without a complete, up-to-date, and tested business continuity plan that includes appropriate business continuity and IT disaster recovery planning provisions.

Recommendation: SBA should continue in its efforts to complete all elements of its business continuity plan, including provisions for orderly and timely restoration of IT services and written policies and procedures for maintaining and testing the plan on a periodic basis.

Finding No. 2:
IT Policies and Procedures

Effective policies are adjusted regularly to accommodate changing conditions. The re-evaluation of existing policies, at least annually or upon significant changes to the operating or business environment, helps ensure their adequacy and appropriateness.

During the audit period, SBA was in the process of updating its IT policies and procedures, which were last updated more than five years ago. Subsequent to our inquiries, new policies and procedures were implemented on February 1, 2005. During our review of both old and new policies and procedures, we determined that certain specific activities necessary to control the IT environment were not adequately documented in either version. Specific examples include:

- Systems software changes performed by consultants, including the update of the PeopleSoft Financials System to Version 8.4.
- Program logic changes to the PeopleSoft Financials System performed by SBA personnel.
- Acceptance testing of program changes to the PeopleSoft Financials System.
- Supervisor and user approval of changes to both systems software and application software.
- Third-party maintenance contracts of systems software components.
- PeopleSoft Financials security administration functions such as the granting, updating, and terminating of user access; the resetting of user passwords; the periodic review of user

access; and the monitoring of security events such as unsuccessful access attempts.

The lack of current, appropriate policies and procedures may reduce the assurance that management's expectations for controlling the IT environment will be achieved.

Recommendation: SBA should continue in it efforts to update its policies and procedures to include all major processes of the IT environment.

Finding No. 3:
PeopleSoft Program Change Controls

Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all new programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled.

Adequately controlled software libraries help ensure that there is (1) a copy of the "official" approved version of a program available in case the integrity of an installed version is called into question, and (2) a permanent historical record of old program versions. A log of past program change activities is particularly important when examining the change control process, as it provides a record of changes that have been implemented. Adequate testing is required before a modified object is placed into the production environment. SBA PeopleSoft Customization standards require that the programmer record the current date, the programmer's initials, a description of the modification, and the reason for the modification.

PeopleSoft Financials System program changes were logged to one of two tracking systems – the Production Version Control System (PVCS) or the Magic Total Service Desk System which was normally used for Help Desk issues or quick fixes. Our audit disclosed the following:

- ➢ Four of the five items we tested logged to PVCS had incomplete program change records. For two of the four items, we were able to determine what was changed and the date changed, but we could not determine the related change request number or the developer responsible for the change.
- ➢ For program changes logged in the Magic Total Service Desk System, no record of changes was maintained.
- ➢ An applied patch and an application timeout modification were made to the PeopleSoft Financials application but were not entered into either of the two tracking systems.
- ➢ SBA did not document developer acceptance testing, quality assurance acceptance testing, or user acceptance testing for program changes made to the PeopleSoft Financials application.
- ➢ Six individuals (two database administrators, the applications and development manager, the security administrator, and two developers) had access to PeopleSoft Financials via a super user ID which provided full access to the PeopleSoft Financials application, including the ability to move PeopleSoft objects into production. Subsequent to our inquiries, SBA changed the password associated with the super user ID on January 6, 2005, and the new password was disclosed to only three individuals (two database administrators and the applications and development manager).
- ➢ Prior to December 15, 2004, SBA did not have procedures for documenting the movement of programs to production. Subsequent to our inquiries, SBA implemented a manual procedure requiring all changes to be tracked in PVCS, which documents the date the modification was moved to production and the person who performed the move.
- ➢ For Visual Basic programs that interface with the PeopleSoft Financials application, developers had update access to production and were compiling and moving their own modified programs to production.

When the program modification process is not adequately controlled, there is an increased risk that unauthorized or erroneous programs may be moved into the production environment without timely detection, increasing the likelihood of fraud or errors.

Recommendation: SBA should implement formal PeopleSoft Financials change controls to ensure the integrity of its application software environment.

Finding No. 4:
PeopleSoft Access Privileges

Effective security administration includes, in part, a security structure to control the granting and revoking of system, data, and resource access privileges and to report and monitor security activity. A complete historical record enables the tracking of security actions from the result to the origin and vice versa.

Proper management of access privileges of terminated or transferred users includes procedures to notify the security administration function of changes in employee status and related provisions for the timely cancellation of access privileges to critical areas, to specific data systems, and to the installation as a whole. In addition, periodic review of access privileges is necessary to ensure their continued appropriateness.

During our review of PeopleSoft Financials security, we determined the following:

- When a user ID is deleted from the system, all of the information in the tables associated with that user ID is also deleted unless the bypass tables option is utilized. Prior to October 1, 2004, the bypass tables option was not utilized.
- Prior to November 22, 2004, the application security administrator was not notified of terminated employees. In response to our audit inquiries, as of November 22, 2004, the application security administrator was notified via e-mail. Our testing indicated that, as of December 6, 2004, one terminated SBA employee was not deactivated in a timely manner. Subsequent to our inquiries, the terminated employee was deactivated on December 7, 2004, which was 53 days after termination.
- The application security administrator was not notified when employees transferred and access needed to be removed or modified. Our testing indicated that three employees with update access to the PeopleSoft General Ledger Module transferred to new positions but did not have their access modified in a timely manner. Subsequent to our inquiries, these user IDs were correctly modified between 695 and 714 days after the date of the employee's transfer.
- User access lists were not periodically reviewed by supervisors for appropriateness.

Granting access that has not been authorized and failing to revoke or modify unnecessary employee access to system resources creates a potential for malicious or unintentional disclosure, modification, or destruction of system resources. Deletions of security logs when user IDs are deleted increases the risk that inappropriate changes may be made to the data and not be detected in a timely manner. Foregoing a periodic review of granted user access increases the risk that the integrity and confidentiality of information systems data and resources may be compromised.

Recommendation: SBA should continue to enhance its access control procedures in the above described areas to increase the assurance of integrity, confidentiality, and availability of information systems and data. Specifically, SBA should monitor and review access privileges to ensure they are timely removed, modified, and remain appropriate.

Finding No. 5:
Systems Security

A division of roles and responsibilities which excludes the possibility for a single individual to subvert a critical process helps to ensure the integrity of the IT environment. Segregation of duties, whereby personnel can perform only those duties stipulated for their respective jobs and positions, can be enforced through good IT security controls. IT system security helps safeguard information from unauthorized use, disclosure, modification, or loss by, among other things, limiting system access to authorized users with an official need for the information maintained therein.

We identified deficiencies in certain SBA security control features relating to the PeopleSoft Financials application and its associated network support systems, in addition to the matters described in Findings No. 2, 3, and 4. Deficiencies were noted in the areas of segregation of duties, security administration, and excessive access privileges. Specific details of the security control deficiencies are not disclosed in this report to avoid the possibility of compromising SBA information. However, the appropriate SBA personnel have been notified of the deficiencies.

Recommendation: SBA should implement the specified security control features to ensure the continued integrity, confidentiality, and availability of the PeopleSoft Financials data and computer resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls related to the PeopleSoft Financials System. Our scope focused on evaluating selected information technology functions applicable to the PeopleSoft Financials System during the period September 2004 through January 2005, with selected SBA actions taken from July 1, 2003.

In conducting the audit, we interviewed appropriate SBA personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test the selected controls related to the PeopleSoft Financials System.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

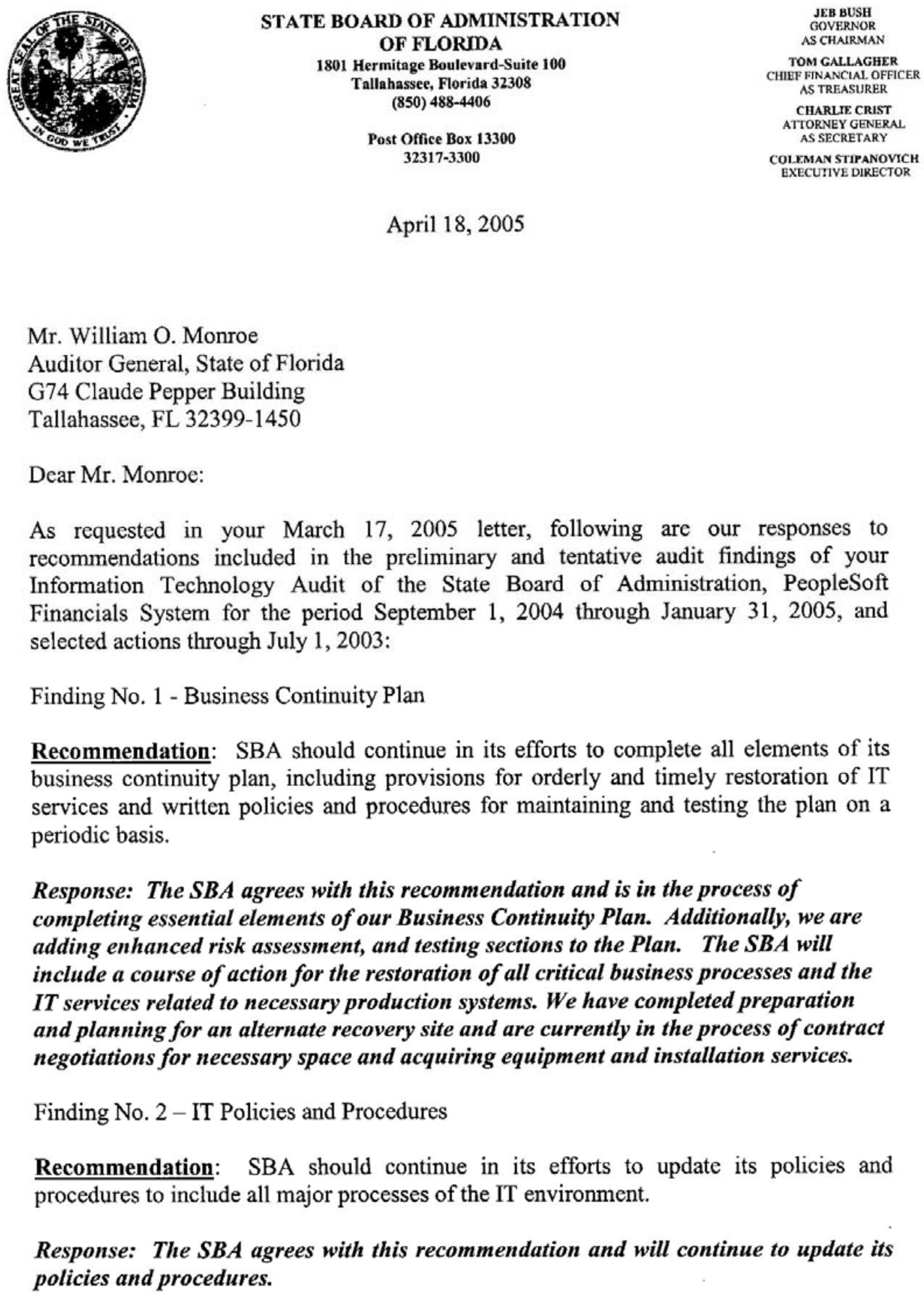
AUDITEE RESPONSE

In a letter dated April 18, 2005, the Executive Director of the State Board of Administration provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Van Weinman, CPA*, CISA, and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.



STATE BOARD OF ADMINISTRATION
OF FLORIDA
1801 Hermitage Boulevard-Suite 100
Tallahassee, Florida 32308
(850) 488-4406

Post Office Box 13300
32317-3300

JEB BUSH
GOVERNOR
AS CHAIRMAN

TOM GALLAGHER
CHIEF FINANCIAL OFFICER
AS TREASURER

CHARLIE CRIST
ATTORNEY GENERAL
AS SECRETARY

COLEMAN STIPANOVICH
EXECUTIVE DIRECTOR

April 18, 2005

Mr. William O. Monroe
Auditor General, State of Florida
G74 Claude Pepper Building
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

As requested in your March 17, 2005 letter, following are our responses to recommendations included in the preliminary and tentative audit findings of your Information Technology Audit of the State Board of Administration, PeopleSoft Financials System for the period September 1, 2004 through January 31, 2005, and selected actions through July 1, 2003:

Finding No. 1 - Business Continuity Plan

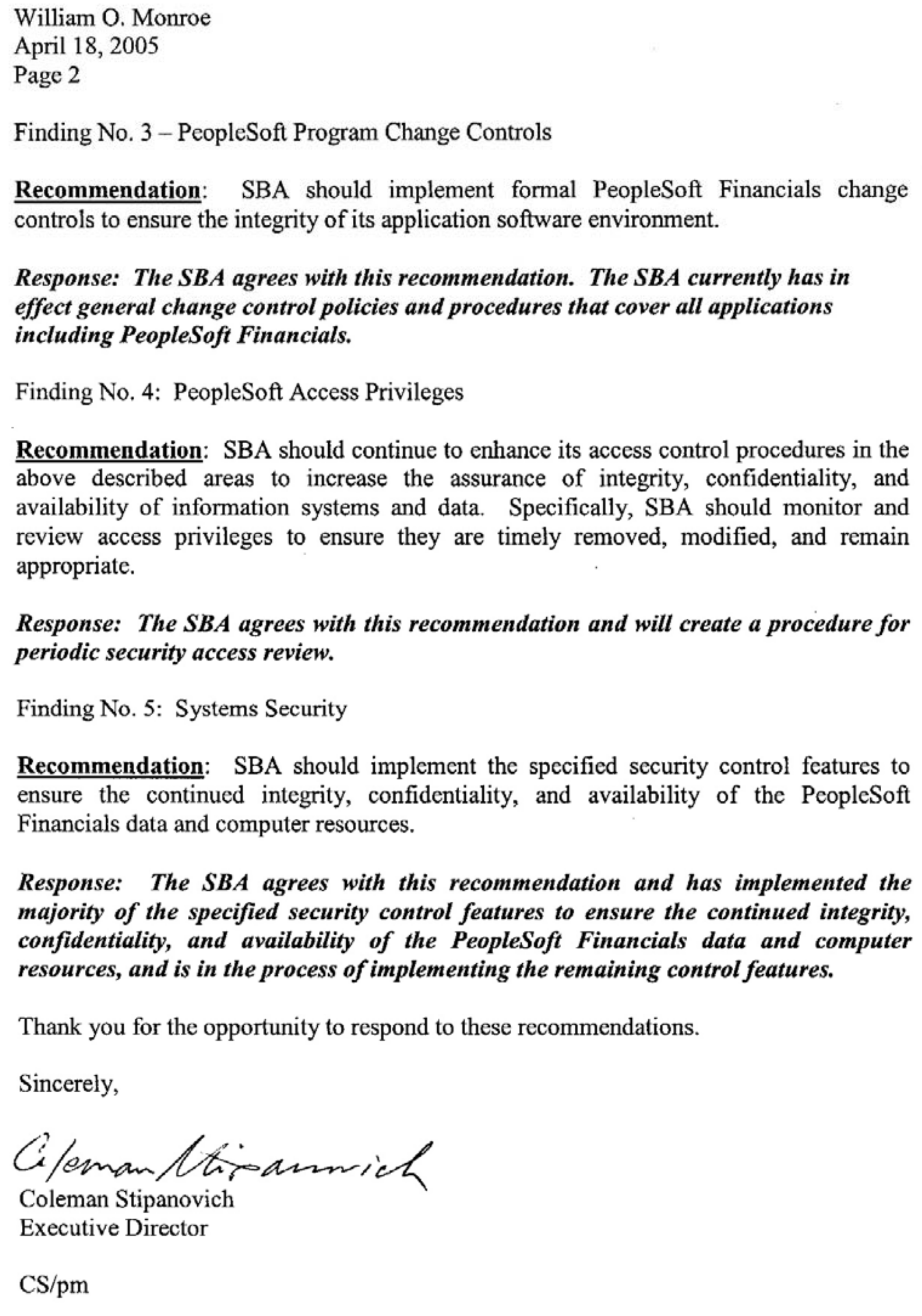
Recommendation: SBA should continue in its efforts to complete all elements of its business continuity plan, including provisions for orderly and timely restoration of IT services and written policies and procedures for maintaining and testing the plan on a periodic basis.

Response: The SBA agrees with this recommendation and is in the process of completing essential elements of our Business Continuity Plan. Additionally, we are adding enhanced risk assessment, and testing sections to the Plan. The SBA will include a course of action for the restoration of all critical business processes and the IT services related to necessary production systems. We have completed preparation and planning for an alternate recovery site and are currently in the process of contract negotiations for necessary space and acquiring equipment and installation services.

Finding No. 2 – IT Policies and Procedures

Recommendation: SBA should continue in its efforts to update its policies and procedures to include all major processes of the IT environment.

Response: The SBA agrees with this recommendation and will continue to update its policies and procedures.



William O. Monroe
April 18, 2005
Page 2

Finding No. 3 – PeopleSoft Program Change Controls

Recommendation: SBA should implement formal PeopleSoft Financials change controls to ensure the integrity of its application software environment.

Response: The SBA agrees with this recommendation. The SBA currently has in effect general change control policies and procedures that cover all applications including PeopleSoft Financials.

Finding No. 4: PeopleSoft Access Privileges

Recommendation: SBA should continue to enhance its access control procedures in the above described areas to increase the assurance of integrity, confidentiality, and availability of information systems and data. Specifically, SBA should monitor and review access privileges to ensure they are timely removed, modified, and remain appropriate.

Response: The SBA agrees with this recommendation and will create a procedure for periodic security access review.

Finding No. 5: Systems Security

Recommendation: SBA should implement the specified security control features to ensure the continued integrity, confidentiality, and availability of the PeopleSoft Financials data and computer resources.

Response: The SBA agrees with this recommendation and has implemented the majority of the specified security control features to ensure the continued integrity, confidentiality, and availability of the PeopleSoft Financials data and computer resources, and is in the process of implementing the remaining control features.

Thank you for the opportunity to respond to these recommendations.

Sincerely,

Coleman Stipanovich

Coleman Stipanovich
Executive Director

CS/pm