



AUDITOR GENERAL

DAVID W. MARTIN, CPA



STATE BOARD OF ADMINISTRATION

EAGLE STAR AND PEOPLESOFT FINANCIALS SYSTEMS

Information Technology Audit

SUMMARY

The State Board of Administration (SBA) utilizes an Eagle Investment Systems, LLC, software solution, Eagle-Straight-Through Accounting and Recordkeeping (Eagle STAR), as its investment accounting system. PeopleSoft Financials is utilized to perform SBA's overall financial accounting and reporting.

Our audit focused on evaluating selected information technology (IT) controls applicable to Eagle STAR and PeopleSoft Financials during the period August 2007 through October 2007 and selected SBA actions taken from July 1, 2006. In addition, we determined the status of corrective actions regarding Finding Nos. 2 through 4 and selected deficiencies in Finding No. 5 disclosed in audit report No. 2005-171.

The results of our audit are summarized below:

Finding No. 1: SBA change management controls for Eagle STAR, PeopleSoft Financials, and supporting applications needed improvement.

Finding No. 2: We noted instances of excessive or inappropriate system access privileges. In addition, certain aspects of SBA practices for managing access privileges needed improvement.

Finding No. 3: We noted instances where SBA did not timely remove the access privileges of terminated employees.

Finding No. 4: SBA did not log modifications to PeopleSoft Financials access privileges.

Finding No. 5: Certain security controls related to Eagle STAR, PeopleSoft Financials, and the supporting network environment at SBA, in addition to the matters discussed in Finding Nos.

2 through 4, needed improvement. Specific details of these issues are not disclosed in this report to avoid any possibility of compromising SBA data and IT resources.

Finding No. 6: SBA did not maintain current procedures pertaining to various functions within the Accounting Information Systems (AIS) Section of the Financial Operations Division of SBA.

BACKGROUND

SBA is a constitutional entity of State government that provides a variety of investment management services to various State entities and units of local government. As of June 30, 2007, assets managed by SBA were valued at approximately \$184 billion. Pursuant to Section 215.44, Florida Statutes, it shall be the duty of SBA to see that moneys invested are at all times handled in the best interests of the participants.

SBA is governed by a Board of Trustees (Board), which has fiduciary responsibility for the management and oversight of SBA. The Board is comprised of the Governor, as Chair; the Chief Financial Officer, as Treasurer; and the Attorney General, as Secretary. The Board has ultimate authority and oversight for the SBA's overall strategy. The Board is also responsible for appointing six members to serve on the Investment Advisory Council, which reviews the investments made by SBA staff and makes recommendations to SBA regarding investment policy, strategy, and procedures. The Board delegates authority to an Executive Director, who is responsible

for managing and directing all administrative, personnel, budgeting, and investment functions.

SBA staff utilize several IT applications in the performance of their investment activities, including Eagle STAR, PeopleSoft Financials, and the Florida Accounting Information Resource (FLAIR) Subsystem. The Eagle STAR application interfaces with PeopleSoft Financials to post investment transactions made by SBA. General ledger accounting information is transferred on an annual basis from PeopleSoft Financials to FLAIR, the official Statewide accounting system.

Eagle STAR and PeopleSoft Financials are both commercial off-the-shelf software products purchased by SBA. The Accounting Information Systems (AIS) Section of the Financial Operations Division serves as functional owner of the two systems. The Applications & Development and Network Services Sections of the Information Technology Division are responsible for support and routine maintenance of the systems and their components.

Finding No. 1: Change Management Controls

Proper controls over changes to application programs and systems are intended to ensure that only authorized and properly functioning changes are implemented. Change management controls include procedures to ensure that all changes are properly authorized, tested, and approved for implementation. Examples of change management controls that are typically employed to ensure the continued integrity of application systems include:

- Providing written evidence of the authorization of changes by the applicable system owner.
- Conducting program testing in a separate test environment that does not affect production programs or data.
- Avoiding the use of production (live) data for testing changes.
- Thorough testing and approval of changes by a person or group independent of the individual making the changes.

- Segregating the responsibility for moving approved changes into the production environment and database responsibilities from the individuals who developed the changes.

Our audit disclosed aspects of SBA change management controls for Eagle STAR, PeopleSoft Financials, and supporting applications that needed improvement. In a test of 30 changes, we noted:

- One that lacked written evidence of prior authorization by the functional owner.
- Twenty-five for which the testing was documented by the developer who made the change but not by an independent person.
- One that was tested in the production environment with live data rather than in a separate testing environment with testing data.
- Twelve that had not been approved for implementation by staff of the AIS Section or other appropriate persons independent of the Applications & Development Section.
- Twenty-nine for which the developer making the change also moved the change into the production environment.

We further noted that SBA did not have written procedures for application software patch management. Although SBA had a written procedure for change control, activities considered by SBA to be routine maintenance, such as applying vendor-provided software patches, were not covered in the change control procedure.

In addition, an individual working in the Applications & Development Section had inappropriate super user access privileges that provided complete access to PeopleSoft Financials. This access included the ability to move PeopleSoft Financials objects, such as PeopleCode programs, records, panels, and fields, into the production environment. The individual was a developer for PeopleSoft Financials who also served as a database administrator as part of his assigned duties. This combination of duties and access privileges did not maintain an appropriate segregation of duties.

The above-described conditions increased SBA's risk that unauthorized or erroneous programs, including

changes or patches thereto, could be moved into the production environment without timely detection.

Recommendation: SBA should establish independent testing and approval of all program changes prior to implementation, use a separate test environment for program testing, and establish a process for persons other than the developer to move programs into the production environment. In addition, SBA should develop written procedures for application software patch management and review the necessity of the above-mentioned individual in the Applications & Development Section to have super user access to PeopleSoft Financials and database administrator responsibilities.

**Finding No. 2:
Management of System User Access Privileges**

An important aspect of IT security management is the establishment of system access privileges that restrict users to only those system functions necessary to perform their assigned duties. Properly configured access privileges help minimize the risk of inappropriate or unauthorized system actions.

As a part of our current audit, we requested and SBA staff provided us with listings of user access privileges in the Eagle STAR and PeopleSoft Financials applications and corresponding databases. Our review of the access privileges disclosed the following:

- Eighteen of the 52 active Eagle STAR application user accounts for accessing specific system functions had, as of September 10, 2007, inappropriate access privileges including privileges that were no longer being used, provided unnecessary access to consultants, or compromised an appropriate segregation of duties. Ten of the 18 users, organizationally placed in the Fixed Income group, had access privileges in Eagle STAR that allowed them to change the values of manually priced securities, which provided for an inappropriate segregation of duties.
- One of the 52 active Eagle STAR application user accounts was being shared by multiple persons, limiting the individual user accountability for system actions performed with the account.

- Eagle STAR database access privileges were inappropriate for 12 of the 14 individuals with access accounts defined in the database as of October 5, 2007. The access privileges of 8 of the 12 individuals provided limited access rights to the database that were not necessary for their job functions, and the access privileges of the other 4 individuals provided administrator rights to the database that were not necessary for their job functions.
- PeopleSoft Financials database access privileges were inappropriate for six of the nine individuals with access accounts defined in the database as of October 23, 2007. The access privileges of the six individuals provided administrator rights to the database that were not necessary for their job functions. In response to audit inquiry, SBA staff indicated that the access privileges of two of the individuals were no longer necessary after the May 2007 upgrade of PeopleSoft Financials and were removed on November 9, 2007.
- Although limited reviews of selected types of user access privileges had been performed by SBA staff, comprehensive periodic reviews of access privileges granted to users of Eagle STAR had not been performed to ensure that user access continues to be appropriate.
- User groups were established by SBA so that access capabilities to Eagle STAR activities could be granted to groups of individuals. However, SBA had not documented the access privileges associated with the user groups, increasing the risk that individual users would be erroneously assigned to user groups having access capabilities greater than what was needed by the users to perform their jobs.

Inappropriate and excessive access privileges increase the risk of malicious or unintentional disclosure, modification, or destruction of data and IT resources.

Recommendation: SBA should ensure that the access privileges of personnel are commensurate with their job duties and enforce an appropriate segregation of duties.

**Finding No. 3:
Terminated Employee Access Privileges**

It is important when employees leave an entity that their access privileges are timely removed to reduce

the risk of access privileges being misused by the terminated employees or others. As a part of our current audit, we requested and SBA staff provided us with a list of 48 employees who terminated their employment during the period July 1, 2006, through August 28, 2007. Our comparison of this list to users with access privileges to Eagle STAR, PeopleSoft Financials, and the SBA network disclosed the following:

- Three employees still had a PeopleSoft Financials access account as of October 2, 2007, which was 155 to 216 days after their termination dates.
- One employee still had network access privileges as of September 10, 2007. In response to audit inquiry, SBA staff demonstrated that SBA removed the network access privileges of this terminated employee on September 27, 2007, or 128 days after termination.
- For the remaining terminated employees who previously had PeopleSoft Financials or network access privileges, the privileges were removed as of the dates of our tests. However, SBA could not demonstrate that the access privileges had been removed timely because SBA had not maintained a record of changes to the access privileges of these terminated employees. This matter is discussed further in Finding No. 4 below.

Although SBA had implemented policies and procedures to monitor inactive and disabled accounts, no review of user accounts was conducted by SBA staff to determine if the network access privileges of terminated employees were being timely removed. Without timely deletion of access privileges of employees who terminated employment with SBA, the risk is increased that access privileges could be misused by the former employees or others.

Recommendation: SBA should ensure that access privileges of terminated employees are removed in a timely manner to minimize any risk of compromising SBA data and information resources.

Follow-Up to Management Response

In its response, SBA stated that Active Directory logging is enabled and logs changes to accounts, such as terminations and disabling of accounts, and that the logs were inadvertently not provided to the audit team.

Subsequent to receiving SBA's response to our preliminary and tentative findings, we requested the logs that were inadvertently not provided to us during our audit field work. We reviewed the logs and determined that 14 terminated employees did not have their network access privileges deleted in a timely manner. The accounts were disabled from 2 to 119 days after the employees' termination dates.

Finding No. 4: Security Logs

Proper IT security practices include maintaining an automated log of security administration activity to determine how, when, and by whom specific actions were taken. Security logs provide the ability to, among other things, selectively identify access modifications made by security personnel.

SBA did not log modifications to access privileges in PeopleSoft Financials. Specifically, PeopleSoft Financials software did not provide the capability to log changes to access privileges.

SBA's ability to pinpoint accountability for an inappropriate or unauthorized change to access privileges, should it occur, may be hindered by the absence of logs.

Recommendation: SBA should retain a record of modifications made to user access privileges in PeopleSoft Financials.

Finding No. 5: Other Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data and IT resources. During our audit, we identified certain SBA security controls related to Eagle STAR, PeopleSoft Financials, and the supporting network environment, in addition to the matters described in Finding Nos. 2 through 4, that needed improvement. Specific details

of these issues are not disclosed in this report to avoid the possibility of compromising SBA data and IT resources. However, appropriate SBA staff have been notified of the specific issues. Without adequate security controls, the integrity, confidentiality, and availability of data and IT resources may be compromised, increasing the risk that SBA’s data and IT resources may be subject to improper disclosure, destruction, or modification.

Recommendation: SBA should implement the appropriate security controls to ensure the continued integrity, confidentiality, and availability of SBA data and IT resources.

**Finding No. 6:
IT Procedures**

Complete, well-documented IT procedures serve to document and communicate management’s expectations for how functions and activities are to be performed and controlled. Effective procedures are adjusted regularly to accommodate changing conditions. The reevaluation of existing procedures, at least annually or upon significant changes to the operating or business environment, helps ensure their adequacy and appropriateness.

Procedures relating to the functions of the Accounting Information Systems Section were not complete or current. Specifically:

- Written PeopleSoft Financials security administration procedures were needed for granting access privileges to new users, modifying the access privileges of existing users, and removing access privileges of terminated employees.
- Procedures for the upload of financial information to FLAIR did not describe the current frequency of updating FLAIR or the current practices for the upload process. In response to audit inquiry, SBA staff indicated that they had not updated the procedures because the processes were still evolving throughout the year-end cycle.

The lack of current and complete procedures increases the risk that management’s expectations for

controlling the IT environment will not be clearly communicated, understood, or consistently achieved.

Recommendation: SBA should enhance its procedures in the aforementioned areas to provide additional assurance that management’s expectations are clearly communicated to employees.

PRIOR AUDIT FINDINGS

Finding Nos. 1 through 6 above included issues repeated from our audit report No. 2005-171. Other IT deficiencies noted in the prior audit that were within the scope of this audit have been corrected or were in the process of being corrected.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls related to Eagle STAR and PeopleSoft Financials and to determine whether SBA had corrected, or was in the process of correcting, Finding Nos. 2 through 4 and selected deficiencies in Finding No. 5 disclosed in audit report No. 2005-171.

The scope of our audit focused on evaluating selected IT controls related to Eagle STAR, PeopleSoft Financials, interfaces with other systems, and the supporting network, during the period August 2007 through October 2007 and selected SBA actions taken from July 1, 2006.

This IT audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. In conducting our audit, we interviewed appropriate SBA personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to Eagle STAR and PeopleSoft Financials.

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.



David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated April 9, 2008, the Interim Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as [Appendix A](#).

This audit was conducted by Daniel Pearce 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.myflorida.com/audgen/>); by telephone (850-487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

APPENDIX A
MANAGEMENT RESPONSE



**STATE BOARD OF ADMINISTRATION
OF FLORIDA**

1801 HERMITAGE BOULEVARD
TALLAHASSEE, FLORIDA 32308
(850) 488-4406

POST OFFICE BOX 13300
32317-3300

CHARLIE CRIST
GOVERNOR
AS CHAIRMAN
ALEX SINK
CHIEF FINANCIAL OFFICER
AS TREASURER
BILL MCCOLLUM
ATTORNEY GENERAL
AS SECRETARY
BOB MILLIGAN
INTERIM EXECUTIVE DIRECTOR

April 9, 2008

Mr. David W. Martin
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Our responses to the preliminary and tentative findings and recommendations which may be included in your report on the Information Technology (IT) Audit of the SBA, Eagle STAR and PeopleSoft Financial Systems, for the period August 2007 through October 2007 are discussed below.

Finding No. 1:
Change Management Controls

Recommendation: SBA should establish independent testing and approval of all program changes prior to implementation, use a separate test environment for program testing, and establish a process for persons other than the developer to move programs into the production environment. In addition, SBA should develop written procedures for application software patch management and review the necessity of the above-mentioned individual in the Applications & Development Section to have super user access to PeopleSoft Financials and database administrator responsibilities.

Response: The SBA agrees that independent testing and approval of program changes prior to implementation and the use of a separate test environment are appropriate. The SBA does obtain independent verification and approval for all user initiated requests. In the future, the SBA will obtain independent verification and approval for system processes as well. The SBA does work within a test environment except when a test environment does not exist or the version/release is not current. The change control policy has been modified to incorporate hot fixes and patches and the security for the systems will be reviewed periodically.

Finding No. 2:
Management of System User Access Privileges

Recommendation: SBA should ensure that the access privileges of personnel are commensurate with their job duties and enforce an appropriate segregation of duties.

Response: The SBA will continue to review these areas periodically for appropriate access. The AIS section has already taken action with documentation of all user groups in the Eagle STAR database. The AIS section will also implement a periodic review process of Eagle STAR access. The risks associated with the 12 accounts are understood by the SBA and are minimal and controlled using compensating controls by limiting access to the Unix operating system. Additionally, we are in the process of reviewing the appropriateness of network access.

Mr. David W. Martin
April 9, 2008
Page 2

**Finding No. 3:
Terminated Employee Access Privileges**

Recommendation: SBA should ensure that access privileges of terminated employees are removed in a timely manner to minimize any risk of compromising SBA data and information resources.

Response: The SBA will continue to ensure that access privileges of terminated staff are removed in a timely manner. The Active Directory is enabled and logs changes to accounts like terminations/disabling accounts, etc. These logs inadvertently were not provided to the audit team, but do provide evidence of timely network account modifications. We will try to document this better within our support tracking system.

**Finding No. 4:
Security Logs**

Recommendation: SBA should retain a record of modifications made to user access privileges in PeopleSoft Financials. SBA should also implement a network logging mechanism.

Response: The SBA will review options of recording modifications of user access privileges in PeopleSoft Financials.

**Finding No. 5:
Other Security Controls**

Recommendation: SBA should implement the appropriate security controls to ensure the continued integrity, confidentiality, and availability of SBA data and IT resources.

Response: Security controls will be reviewed and tightened as required.

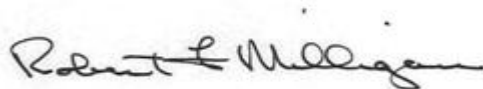
**Finding No. 6:
IT Procedures**

Recommendation: SBA should enhance its procedures in the aforementioned areas to provide additional assurance that management's expectations are clearly communicated to employees.

Response: The SBA will review all IT procedures for accuracy. The SBA will modify and update procedures on an annual basis.

Thank you for the opportunity to respond to these findings and recommendations. If you have any questions, please do not hesitate to contact Ms. Rivera-Alsing at (850) 413-1259 or me at (850) 413-1250.

Sincerely,



Robert F. Milligan
Interim Executive Director

cc: Gwenn Thomas, Chief Operating Officer
Flerida D. Rivera-Alsing, Chief of Internal Audit
Bruce R. Meeks, Inspector General