REPORT NO. 2013-180
MAY 2013

STATE BOARD OF ADMINISTRATION

SELECTED FINANCIAL SYSTEMS

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

STATE BOARD OF ADMINISTRATION

The State Board of Administration's Board of Trustees is composed of the Governor, as Chair; the Chief Financial Officer; and the Attorney General. The Trustees delegate administrative and investment functions, among other things, to an appointed Executive Director. Mr. Ashbel Williams served as Executive Director during the period of our audit.

The audit team leader was Robert McKee, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Nancy M. Reeder, CPA, CISA, CFE, Audit Manager, by e-mail at nancyreeder@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

STATE BOARD OF ADMINISTRATION

Selected Financial Systems

SUMMARY

The State Board of Administration (SBA) utilizes Eagle Investment Systems, LLC, software solution, Eagle-Straight-Through Accounting and Recordkeeping (Eagle STAR) as its investment accounting system. In addition, SBA utilizes PeopleSoft Financials to perform SBA's overall financial accounting and reporting. SBA also utilizes Florida PRIME, an investment service for public funds. Florida PRIME is used to provide eligible participants an investment vehicle for their surplus funds. The Local Government Surplus Funds Trust Fund for which Florida PRIME is used was created pursuant to Section 218.405(1), Florida Statutes, and currently serves over 800 participants.

Our audit focused on evaluating selected information technology (IT) controls applicable to Eagle STAR and PeopleSoft Financials. We also evaluated controls over the interface between Florida PRIME and Eagle STAR. In addition, we determined the status of corrective actions regarding audit findings included in our report No. 2008-170.

The results of our audit are summarized below:

Finding No. 1: As similarly noted in our report No. 2008-170, some Eagle STAR users had been granted unnecessary access privileges. In addition, SBA review of Eagle STAR and PeopleSoft Financials access privileges needed improvement.

Finding No. 2: Some SBA administrators shared the same user identification codes (user IDs) and passwords for Eagle STAR database and application servers rather than being uniquely identified and authenticated to the system.

Finding No. 3: SBA security controls related to Eagle STAR, PeopleSoft Financials, and the supporting network environment in the areas of user authentication and firewall patch management needed improvement. Some of these issues were communicated to SBA management in connection with our report No. 2008-170.

BACKGROUND

SBA is a constitutional entity of State government that provides a variety of investment management services to various State entities. As of June 30, 2012, assets managed by SBA were valued at approximately $151 billion. Pursuant to Section 215.44(2)(a), 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 State.

SBA is governed by a Board of Trustees (Board), which has fiduciary responsibility for the management and oversight of SBA. The Board is composed 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 SBA's overall strategy. The Board is also responsible for appointing nine members to serve on the Investment Advisory Council, which, pursuant to Section 215.444(1), Florida Statutes, provides independent oversight of SBA funds and investment responsibilities 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, investment policy, and investment functions.

SBA staff utilize several IT applications in the performance of their investment activities, including Eagle STAR, PeopleSoft Financials, Florida PRIME, and the Florida Accounting Information Resource Subsystem (FLAIR). Eagle STAR 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, PeopleSoft Financials, and Florida PRIME are commercial off-the-shelf software products purchased by SBA. The Accounting Information Systems (AIS) Section of the Financial Operations Division serves as the functional owner of Eagle STAR and PeopleSoft Financials, while the Investment Operations Section of the Financial Operations Division serves as the functional owner of Florida PRIME. 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.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Access Privileges

Effective access controls include measures that limit user access privileges to only what is necessary in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Upon audit inquiry, SBA staff provided us with listings of user access privileges in Eagle STAR and PeopleSoft Financials and corresponding databases. Our review of the access privileges disclosed that some Eagle STAR users had been granted unnecessary access privileges and that SBA review of Eagle STAR and PeopleSoft Financials access privileges needed improvement. Specifically:

- Of the 24 Eagle STAR users with access to the PriceBatch template, which allows manual changes to prices within Eagle STAR, 12 employees in the Financial Operations Division had been granted inappropriate access privileges to the manual pricing function through the batch templates. The 12 Financial Operations Division employees did not require access to the manual pricing function to perform their assigned job duties.
- Of the 27 Eagle STAR users with access to the Issue Prices panels (screens), 1 user, an SBA consultant, had been granted access privileges to manually change prices directly through the application. The consultant did not require the ability to manually change prices to perform his assigned job duties.
- SBA management had not performed periodic reviews of access privileges to the Eagle STAR PriceBatch template for interchanges.
- Although SBA management performed periodic reviews of access privileges for the PeopleSoft Financials, some supervisors were responsible for reviewing their own access privileges without an independent review.

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

Recommendation: SBA should limit user access privileges to only what is necessary for the performance of assigned job duties. Additionally, SBA should ensure that periodic reviews of access privileges to the Eagle STAR PriceBatch template are performed and that all supervisor access privileges in PeopleSoft Financials are independently reviewed.

Finding No. 2: User Identification

Effective access controls include a process for the unique identification and authentication of system users. The unique identification of system users allows management to affix responsibility for system activity to an individual person.

Our review of the administrator access privileges to the Eagle STAR database and application servers disclosed that some employees shared the same user IDs and passwords rather than being uniquely identified and authenticated to the system. Specifically:

- One primary administrator and one backup administrator within the Network Services Section administered the Eagle STAR database by sharing a vendor-provided user ID and corresponding password. In response to audit inquiry, SBA staff created unique database user IDs for the primary administrator and the backup administrator on November 16, 2012, and January 11, 2013, respectively.
- Two administrators within the Network Services Section had the ability to access certain Eagle STAR application servers by sharing the root (administrator) user ID and corresponding password.

Without the ability to uniquely identify database and server administrators, the ability of SBA to establish accountability for database and server administration actions may be limited.

Recommendation: SBA should assign unique user IDs to all individual users, including all administrators who are authorized to perform database and server administration functions.

Finding No. 3: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain SBA security controls related to Eagle STAR, PeopleSoft Financials, and the supporting network environment in the areas of user authentication and firewall patch management needed improvement. We are not disclosing specific details of these issues in this report to avoid the possibility of compromising SBA data and IT resources. However, we have notified appropriate SBA staff of the specific issues. Some of these issues were communicated to SBA management in connection with our report No. 2008-170. Without adequate security controls in the areas of user authentication and firewall patch management, the confidentiality, integrity, and availability of data and IT resources may be compromised.

Recommendation: SBA should improve security controls related to user authentication and firewall patch management to ensure the confidentiality, integrity, and availability of data and IT resources.

PRIOR AUDIT FOLLOW-UP

SBA had taken corrective actions for four of the six findings included in our report No. 2008-170 that were applicable to the scope of this audit. SBA had partially corrected the remaining two prior audit findings.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from September 2012 through January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2008-170.

The scope of our audit focused on evaluating selected SBA IT controls applicable to Eagle STAR and PeopleSoft Financials during the period July 2012 through January 2013, and selected SBA actions through March 20, 2013. The audit included selected general IT controls over systems modification; logical access to programs, data, and data files; and physical access. The audit also included selected application and user controls relevant to Eagle STAR and PeopleSoft Financials including the interface between Florida PRIME and Eagle STAR.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed SBA personnel.
- Obtained an understanding of the Eagle STAR, PeopleSoft Financials, and Florida PRIME systems, including the computing platform for each system and related software, purpose and goals, and the basic data and business process flows through each system.

- Obtained an understanding of key application controls, including input, processing, output, and user controls.
- Observed and evaluated the effectiveness of key user account administration processes and procedures.
- Obtained an understanding of general IT controls related to Eagle STAR, PeopleSoft Financials, and Florida PRIME.
- Observed and evaluated key processes and procedures related to logical access controls over Eagle STAR and PeopleSoft Financials IT resources.
- Observed and evaluated key processes and procedures related to network and barrier controls.
- Observed and evaluated key processes and procedures related to physical access controls protecting SBA resources.
- Evaluated the appropriateness of controls relevant to the interface between Florida PRIME and Eagle STAR.
- Evaluated the appropriateness of access privileges and the effectiveness of controls over separation of duties of SBA staff with access to Eagle STAR, PeopleSoft Financials, the database environment, the network, and production programs.
- Tested the effectiveness of procedures for deactivating the network, Eagle STAR, and PeopleSoft Financials access privileges of former employees. Specifically, we tested all five SBA employees who terminated employment between July 1, 2012, and October 11, 2012, to determine if their access privileges had been timely deactivated.
- Tested the effectiveness of the system modification process to ensure that program modifications are suitably authorized, tested, and implemented. Specifically, we tested all 11 program change requests that had been completed between July 1, 2012, and November 30, 2012, for Eagle STAR and PeopleSoft Financials.
- Inspected network, Eagle STAR, and PeopleSoft Financials password settings to evaluate whether the settings were appropriately configured to adequately protect SBA resources.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

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 IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated May 10, 2013, the Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

STATE BOARD OF ADMINISTRATION
OF FLORIDA

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

POST OFFICE BOX 13300
32317-3300

RICK SCOTT
GOVERNOR
AS CHAIRMAN

JEFF ATWATER
CHIEF FINANCIAL OFFICER

PAM BONDI
ATTORNEY GENERAL

ASH WILLIAMS
EXECUTIVE DIRECTOR & CIO

May 10, 2013

Mr. David W. Martin, CPA
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 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 Operational Audit of the State Board of Administration Selected Financial Systems are discussed below.

Finding No. 1:
Access Privileges

Recommendation: SBA should limit user access privileges to only what is necessary for the performance of assigned job duties. Additionally, SBA should ensure that periodic reviews of access privileges to the Eagle STAR PriceBatch template are performed and that all supervisor access privileges in PeopleSoft Financials are independently reviewed.

Response: The SBA agrees and has already taken corrective action to limit access privileges. The access privileges will also be reviewed periodically.

Finding No. 2:
User Identification

Recommendation: SBA should assign unique user IDs to all individual users, including all administrators who are authorized to perform database and server administration functions.

Response: The SBA agrees and has already taken corrective action.

Finding No. 3:
Other Security Controls

Recommendation: SBA should improve security controls related to user authentication and firewall patch management to ensure the confidentiality, integrity, and availability of data and IT resources.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin, CPA
May 10, 2013
Page 2

Response: The SBA agrees and has already taken corrective action.

We appreciate the diligence, professionalism, and efforts of the Office of the Auditor General.

Sincerely,

Ashbel C. Williams
Executive Director & CIO