REPORT NO. 2011-173
APRIL 2011

DEPARTMENT OF FINANCIAL SERVICES

SELECTED DIVISION OF TREASURY APPLICATIONS

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

CHIEF FINANCIAL OFFICER

Pursuant to Article IV, Sections 4.(c) and 5.(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Alex Sink served as Chief Financial Officer during the period of our audit.

The audit team leader was Shawn McCormick, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@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.

DEPARTMENT OF FINANCIAL SERVICES

Selected Division of Treasury Applications

SUMMARY

The Chief Financial Officer (CFO) serves as the chief fiscal officer of the State and is responsible to settle and approve accounts against the State and keep State funds and securities. The CFO heads the Department of Financial Services (Department) that has a wide range of constitutional and statutory responsibilities. Within the Department, the Division of Treasury performs functions generally associated with private financial institutions, such as deposit security, funds management, and deferred compensation. To perform the Division of Treasury's functions, the Department maintains various Division of Treasury (Treasury) information technology (IT) applications.

Our audit focused on evaluating selected IT controls applicable to the following Treasury applications: Bank Accounts, Chargebacks, Receipts, and Verifies. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2009-004, including findings related to the Department's Investment Accounting application.

The results of our audit are summarized below:

Finding No. 1: Some password controls surrounding the Treasury applications needed improvement. One issue relating to password expiration intervals was also disclosed in our report No. 2009-004.

Finding No. 2: The access privileges of some Department staff with regard to production programs and data were not appropriate for their job duties. Similar issues were disclosed in our report No. 2009-004.

Finding No. 3: Program change controls needed improvement in the areas of monitoring program changes in the production environment and the movement of source programs into the production environment. One issue relating to monitoring program changes in the production environment was also disclosed in our report No. 2009-004.

Finding No. 4: The Department did not have written procedures for some Treasury application security administration functions.

Finding No. 5: Some Department security controls in the areas of user authentication and system logging needed improvement. Similar issues regarding system logging were also disclosed in our report No. 2009-004.

BACKGROUND

The CFO has various statutory responsibilities for State funds that include paying warrants and other orders for the disbursement of State funds, accounting for State funds and securities, and depositing and investing funds. The Division of Treasury is responsible for ensuring that State moneys, employee deferred compensation contributions, State and local governments' public funds on deposit in Florida banks and savings associations, and cash and other assets held for safekeeping by the CFO are adequately accounted for, invested, and protected.

Within the Division of Treasury, the Bureau of Funds Management is responsible for posting State receipts and disbursements, performing cash management services, and investing available funds. To perform these duties, several Treasury applications have been developed and maintained by the Division of Information Systems, Bureau of Enterprise Applications, Division of Treasury programming staff and Bureau of Operations and Customer Services, Mainframe Systems programming staff.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Password Controls

Access controls are dependent, in part, on the ability to authenticate the identity of system users, such as through the use of personal passwords. The effectiveness of passwords as an authentication tool depends on the ability to maintain password confidentiality. Typical controls protecting the confidentiality of user passwords include password length and requirements for passwords to be changed on regular intervals.

User access privileges to the selected Treasury applications are controlled using the Treasury Authorization System's menu functions, such as the Configuration and Change Password functions. Our review of the Treasury Authorization System's password configuration settings noted the following issues:

- Contrary to Department of Financial Services Administrative Policies and Procedures No. 4-03, Information Technology Security Policy, the Treasury Authorization System password parameter configuration allowed Treasury application users to create six character passwords instead of the setting required in policy. In response to audit inquiry, Department staff modified the application password configuration setting to comply with policy.
- Users were presented the "change password screen" for entering a required new password. However, users were able to click on the "Close" button that closed the change password screen but not the application, thus bypassing the intended password change process. As a result, users were able to retain their old passwords for extended periods of time. In response to audit inquiry, Department staff modified the program code to close both the "change password screen" and the application, thereby preventing users from bypassing the requirement to enter a new password.

Our review of password controls on the Web and database servers that hosted the selected Treasury applications disclosed that the Department had implemented adequate default system values over password expiration. However, on the database server, the password expiration interval was set to allow passwords to remain unchanged on the user profiles of a programmer and a consultant. This was contrary to Department of Financial Services Administrative Policies and Procedures No. 4-03, Information Technology Security Policy. A similar issue regarding password expiration intervals was noted in our report No. 2009-004. In response to audit inquiry, Department staff adjusted the expiration interval on the two user profiles so that the passwords would expire in accordance with Department policy. Subsequently, Department staff disabled the consultant's user profile.

Without adequate password controls, the risk is increased that unauthorized access and misuse of Department data and IT resources could occur through the use of compromised passwords.

Recommendation: The Department should ensure that adequate password controls are maintained in accordance with established policy to reduce the risk of compromise to passwords and unauthorized disclosure, modification, or destruction of data and IT resources.

Finding No. 2: Appropriateness of Access Privileges

Properly configured IT access privileges restrict employees and consultants to only those system functions necessary to perform their assigned job duties, enforce an appropriate separation of incompatible duties, and minimize the risk of unauthorized system actions. For example, access privileges are typically configured to restrict application programmers from having access to production program libraries and data.

Our review of selected Treasury production data objects (i.e. data tables, programs, and files) disclosed instances of inappropriate update access privileges (permissions) to Treasury production data outside of the application controls. A similar finding was noted in our report No. 2009-004. Specifically, a test profile used by the programming staff had been granted inappropriate update permissions to 20 of the 21 production data objects as a result of the profile being a member of two server groups. These conditions increased the risk of unauthorized modification or destruction of Treasury data. In response to audit inquiry, Department staff removed the test profile from the two server groups on November 5, 2010.

Our review of access permissions for the selected Treasury applications' production program code disclosed instances of inappropriate update permissions. These conditions increased the risk of unauthorized modifications to production programs that could compromise the integrity of Treasury application controls and functionality. Similar findings were noted in our report No. 2009-004. Specifically:

- Seven users, including five programmers, one consultant programmer, and one end user from the Bureau of Funds Management, belonged to a directory group who had permissions that included the ability to update Treasury production program code. In response to audit inquiry, Department staff removed the directory group's update permissions on October 11, 2010; and subsequently on October 12, 2010, removed the end user from the group as well.
- Sixteen user profiles and 31 system profiles had unnecessary update permissions to the production batch program code because of inappropriate settings within the directory that contained the code. In response to audit inquiry, Department staff adjusted the directory settings to remove the update permissions on October 26, 2010.

Recommendation: The Department should ensure that update access permissions continue to remain commensurate with assigned job duties.

Finding No. 3: Program Change Controls

Effective controls over the modification of application programs help ensure that only authorized programs and authorized modifications are implemented. Source programs (the code created by application programmers) are compiled into object (executable) programs that are machine readable and used during data processing. To ensure an appropriate separation of duties, a group or persons independent of the programmers should control the movement of programs into production.

As similarly noted in our report No. 2009-004, the Department had no mechanism in place to automatically detect and log Treasury application program changes moved into the production environment. The absence of an automatic system-generated log increases the risk that unauthorized or erroneous modifications will be moved into the production environment and not be timely detected.

In addition, the Treasury source programs were compiled into production code by the programmers and placed in a staging area where the programs were then moved to a controlled production library by the database administrators or system administrators. However, the source programs were not moved to a controlled production library by an independent group or person, contrary to an appropriate separation of duties. Without a controlled production source code library (in which the programmers have no update ability), the Department's ability to ensure the integrity of the installed versions of the programs was limited.

Recommendation: The Department should provide for an automatic system-generated log of changes to production Treasury application programs. Until a logging mechanism can be acquired, the Department

should implement alternative monitoring and review processes over program changes in the Treasury production environment to ensure that unauthorized or erroneous modifications, should they occur, are timely detected. In addition, the Department should implement procedures to ensure the integrity of the Treasury source programs by having an independent group or person move the source programs to a separately controlled production library.

Finding No. 4: Application Security Administration Procedures

Effective access controls include documenting management expectations with regard to security administration in the form of written procedures that provide tactical guidance on the day-to-day operations of creating, assigning, monitoring, updating, and revoking access privileges. Detailed, written instructions should exist and be followed to guide personnel in performing their duties.

Our review of the Department's application security administration procedures disclosed that the Department had developed written procedures that provided security administrators guidance on enabling and disabling user access privileges to the Treasury applications using the Authorization menu screen within the Treasury Application Tool (Authorization System). However, written procedures for the use of other Authorization menu functions such as Add User, Add/Modify System, Configuration, or Change Password did not exist.

The lack of complete written procedures for all Authorization menu functions increases the risk that security administrators may not maintain security controls through the Authorization menu consistently and in a manner pursuant to management expectations.

Recommendation: The Department should enhance its procedures to provide written guidance on all security administration functions of the Authorization System.

Finding No. 5: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls that needed improvement in the areas of user authentication and system logging. Similar issues regarding system logging were noted in our report No. 2009-004. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to user authentication and system logging, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should improve security controls related to user authentication and system logging to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2009-004.

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 August 2010 through December 2010 in accordance with applicable 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 applicable to the selected Treasury applications 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; the safeguarding of IT resources; the effectiveness and efficiency of IT operations and to determine whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2009-004.

The scope of our audit focused on evaluating selected general and application IT controls and selected user controls applicable to the Division of Treasury Bank Accounts, Chargebacks, Receipts, and Verifies applications, including selected general IT controls over systems modification and logical access to programs and data.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the selected Treasury applications, including the purpose and goals of the applications, and the basic data and business processing flows through the applications.
- Observed and tested the effectiveness of selected application controls, including input, processing, output, and user controls in ensuring the reliability and integrity of the Bank Accounts, Chargebacks, Receipts, and Verifies applications' data.
- Tested the proper functioning of 25 significant input edits within the Chargebacks application.
- Observed and tested the effectiveness of the controls surrounding the interfaces between the Bank Accounts, Chargebacks, Receipts, and Verifies applications and other applications and entities.
- Examined, on a sample basis, five FLAIR Batch Verification and Online Verification reports that had been processed on various days of the week between August 30, 2010, and October 26, 2010, to determine whether data in FLAIR verified transaction files correctly transferred to the Receipts application.
- Examined, on a sample basis, five EFT Returned Items reports that had been processed between August 30, 2010, and October 13, 2010, to determine whether amounts for EFT returned items loaded into the Verifies application reconciled to amounts for Debit Memos produced from the Receipts application.
- Examined, on a sample basis, five Chargebacks Reconciliation reports that included 466 returned checks (Chargeback items) that had been processed on various days of the week between August 30, 2010, and October 19, 2010, to determine whether amounts for Chargeback items loaded into the Chargebacks application reconciled to amounts for Debit Memos produced from the Receipts application.
- Examined, on a sample basis, six Chargebacks reports that included 591 records (Chargeback items) that had been processed on various days of the week between September 1, 2010, and October 14, 2010, to determine

the effectiveness of controls surrounding the transfer of data between the Bank of America and the Chargebacks application.

- Evaluated the appropriateness of user application access privileges to selected Treasury functions to determine whether the access privileges granted to users of the Bank Accounts, Chargebacks, Receipts, and Verifies applications were appropriate. Specifically, we tested all 17 users who were granted access privileges to the Bank Accounts, Chargebacks, Receipts, and Verifies applications to determine whether the users' access privileges were appropriate based on their job duties.
- Obtained an understanding of logical access paths to the Bank Accounts, Chargebacks, Receipts, and Verifies applications and tested whether logical access controls ensured that access privileges were appropriately authorized. Specifically, we tested all employees who had changes in access privileges to the selected Treasury applications between August 1, 2010, and September 30, 2010, to determine whether access privileges were appropriately authorized.
- Evaluated the appropriateness of selected logical access controls for the Web and database servers that hosted the selected Treasury applications to determine whether access privileges to the selected applications' program code and data was appropriately restricted. Specifically, we tested 55 accounts and 624 data objects to determine whether access privileges to production program code, job control language, and data objects were appropriate.
- Observed and tested the effectiveness of selected general controls over the authorization, documentation, testing, approval, and implementation of application program changes. Specifically, we sampled 10 completed Requests for Changes for program and data changes moved into production between January 1, 2010, and September 7, 2010, to determine whether application change control procedures were in place and operating effectively.
- Evaluated the effectiveness of password parameters for the selected Treasury applications and the related Web and database servers.

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 April 5, 2011, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

April 5, 2011

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

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed responses are provided for the preliminary and tentative audit findings included in the Auditor General's Information Technology Operational Audit of the Department of Financial Services, Selected Division of Treasury Applications.

If you have any questions or would like to discuss the matter further, please contact Alan Sands, Audit Director, at (850) 413-4962.

Sincerely,

Jeff Atwater

JA:Sc

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 FAX (850) 413-2950

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Financial Services
Selected Division of Treasury Applications
Information Technology Operational Audit
Preliminary and Tentative Findings
Audit Response

Finding No. 1: Password Controls

Some password controls surrounding the Treasury applications needed improvement. One issue relating to password expiration intervals was also disclosed in our report No. 2009-004.

Recommendation: The Department should ensure that adequate password controls are maintained in accordance with established policy to reduce the risk of compromise to passwords and unauthorized disclosure, modification, or destruction of data and IT resources.

Response: The Department concurs.

In response to the audit inquiry related to the override of two user profiles, Department staff disabled the user profiles and adjusted the expiration interval on the identified user profiles so that the passwords would expire in accordance with Department policy.

In response to the audit inquiry related to password length parameters, DIS will remove Treasury's ability for that control to be changed to less than the Department standard.

In response to the audit inquiry related to the "change password screen," all applications will be reviewed and modified to ensure that closing the Change Password screen will quit the application if a user tries to circumvent the requirement to change their password.

Finding No. 2: Appropriateness of Access Privileges

The access privileges of some Department staff with regard to production programs and data were not appropriate for their job duties. Similar issues were disclosed in our report No. 2009-004.

Recommendation: The Department should ensure that update access permissions continue to remain commensurate with assigned job duties.

Response: The Department concurs. In response to the audit inquiry, Department staff removed the test profile from the two server groups on November 5, 2010. The Department will ensure that access permissions are commensurate with assigned job duties. The Department will explore refining the Personnel Action Request (PAR) process to include the Information Technology Application Access and Resource Request Form (Form 1820).

Finding No. 3: Program Change Controls

Program change controls needed improvement in the areas of monitoring program changes in the production environment and the movement of source programs into the production environment. One issue relating to monitoring program changes in the production environment was also disclosed in our report No. 2009-004.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation: The Department should provide for an automatic system-generated log of changes to production Treasury application programs. Until a logging mechanism can be acquired, the Department should implement alternative monitoring and review processes over program changes in the Treasury production environment to ensure that unauthorized or erroneous modifications, should they occur, are timely detected. In addition, the Department should implement procedures to ensure the integrity of the Treasury source programs by having an independent group or person move the source programs to a separately controlled production library.

Response: The Department concurs. In the absence of an automated monitoring tool, procedures will be developed to have an independent party move source programs to a controlled production library. Comparisons will be made between production libraries and the controlled production source code libraries to ensure that erroneous production changes will be detected in a timely manner.

Finding No. 4: Application Security Administration Procedures

The Department did not have written procedures for some Treasury application security administration functions.

Recommendation: The Department should enhance its procedures to provide written guidance on all security administration functions of the Authorization System.

Response: The Department concurs. Written procedures will be developed to address all security administration functions of the Authorization System.

Finding No. 5: Other Security Controls

Some Department security controls in the areas of user authentication and system logging needed improvement. Similar issues regarding system logging were also disclosed in our report No. 2009-004.

Recommendation: The Department should improve security controls related to user authentication and system logging to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response: The Department concurs with the recommendation and will pursue security control remediation.