



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



STATE BOARD OF ADMINISTRATION STATE STREET PRIME-MERIDIAN SYSTEM

INFORMATION TECHNOLOGY AUDIT For the Period October 2001 Through February 2002, And Selected Board Actions Taken Through May 2002

Summary

The State Street Prime-Meridian System is a proprietary software product developed and maintained by State Street Corporation. In managing the assets of the Florida Retirement System (FRS) Trust Fund and Lawton Chiles Endowment Fund, the State Board of Administration (Board) Financial Operations uses the State Street Prime-Meridian System to perform inter-bank transfers, Federal wires, and other money movement transactions. Our audit of the Board focused on evaluating management controls and selected information technology functions, determining the effectiveness of selected general controls, and determining the effectiveness of selected application controls used by the Board, all as related to the State Street Prime-Meridian System. A summary of the deficiencies follows:

- *The Board had not formally designated an information security manager to provide for a unified security program over all of the Board's information resources. Additionally, deficiencies in the security program were noted.*

- *The Board had not maintained a current formal risk analysis regarding its information technology resources, and consequently had inadequate disaster recovery procedures to ensure continuous service or minimize the impact should a major disruption occur.*

Background:

The State Board of Administration (Board) is a constitutional board comprised of the Governor as chairman, the State Treasurer, and the State Comptroller. Section 215.441, Florida Statutes, allows for the appointment of the executive director of the State Board of Administration. Section 215.44, Florida Statutes, assigns the Board's powers and duties in relation to investment of trust funds for State agencies or units of local government. Pursuant to Section 215.47(9), Florida Statutes, investments made by the Board are to maximize the financial return to the fund consistent with incumbent risk and diversification of the portfolio and shall comply with applicable Federal laws.

One of the Board's major responsibilities is investing Florida Retirement System (FRS) Trust Fund assets, which had a market value of \$94.31 billion as of January 31, 2002. The Board also has responsibility for investing the Lawton Chiles Endowment Fund which had a market value of \$1.37 billion as of January 31, 2002. The total market value of all investments managed by the Board as of January 31, 2002 was \$125 billion. The Board uses State Street Corporation's State Street Prime-Meridian System for managing the FRS Trust Fund and the Lawton Chiles Endowment Fund, which together make up 76.5% of the total investments managed by the Board.

The State Street Prime-Meridian System is a cash management system used for Federal wire transfers and asset transfers between accounts. Financial Operations within the Chief Financial Office (CFO) of the Board uses the State Street Prime-Meridian System for executing fund transfers and wires that facilitate the Board in performing its investment responsibilities assigned by Florida Statute. The Board uses information technology networks to connect to State Street Prime-Meridian System to perform these cash management functions online.

Finding No. 1:

The Board had not formally designated an information security manager to provide for a unified security program over all of the Board's information resources. Additionally, deficiencies in the security program were noted.

Management should formally assign the responsibility for assuring both the logical and physical security of the organization's information assets to an information security manager who reports to the organization's senior management. At a minimum, security

management responsibilities should be established at the organization-wide level to implement and oversee the security program for the organization.

Although the Board's Information Resource Security Plan contained a standard for the appointment in writing of an information security manager (ISM) to administer the Board's Information Resource Security program, the Board had not formally designated an information security manager. However, according to the Board, at various times in the past, the Board had informally assigned an individual certain responsibilities that would have been assigned to an ISM. During our audit we noted the following deficiencies that could be improved upon and would be the responsibility of an ISM:

- The Information Resources Security Plan (Plan) contained policies, standards, and procedures, but was incomplete, had not been updated for at least four years, was not circulated among employees, and was not always followed. The Plan addressed items such as performing a risk analysis, reviewing security logs, accessing the information resources by using personal authentication and password methodologies, and protecting the Board's information resources through use of both physical and logical security mechanisms. However, the Plan had not been updated to address changes in technology. Some policy or procedure topics not included were user access request and authorization, user access review, firewalls, Internet security, anti-virus, personal computer, screen saver usage, and Virtual Private Network (VPN).

- State Street Prime-Meridian access logs and user access reports were not monitored or reviewed on a regular basis as required by the Information Resources Security Plan.
 - The State Street Prime-Meridian System provided the capability to produce an audit log of all user actions and an activity log of user security events related to the State Street Prime-Meridian System. However, the Board did not produce and review these logs on a regular basis.
 - The User Entitlement Reports showing the users who had access to the State Street Prime-Meridian System and the levels of access were also available, but were not being reviewed on a regular basis. Our testing disclosed that three individuals with access to the State Street Prime-Meridian System had incompatible duties of approving non-repetitive wires and releasing the wires. Subsequent to our inquiries, on March 1, 2002, the releasing of wires capability was removed from two of the individuals whose job duties had changed in August 1999. Had regular reviews of the User Entitlement Reports been performed, these oversights may have been more readily identified and timely remedied. Access for the third individual who had the incompatible duties of approving and releasing wires was not removed because the individual was designated by the Board to be in a position of special

trust. However, there was no independent review of access activity performed by this individual.

- The Board did not monitor or review security settings on a periodic basis to ensure that control options continued to function as intended. Additionally, the Information Resources Security Plan did not address this procedure.
 - We found the password history control option in the network operating system was not set to prevent a user from immediately reusing the previous password. As a result of our inquiries on April 9, 2002, the Board reset the password history file option to retain the passwords used by each user. This password is used to authenticate the user requesting access to the Board's network. A password history file prevents a user from switching back and forth among their favorite passwords. Not using the password history option increases the risk that unauthorized individuals could gain knowledge of a password setting used frequently by a user.

As indicated by the deficiencies noted above, without the formal designation of an information security manager to provide for a unified security program, the risk is increased that the Board's security program for data and information technology resources will not be effectively administered and may not provide for adequate prevention or timely detection of erroneous or fraudulent activities.

Recommendation:

The Board should formally appoint an information security manager to administer the Board's security program and assign this individual the responsibilities as defined in the Information Resource Security Plan. Additionally, the Information Resource Security Plan should be periodically updated to include changes to technology or processes, circulated among the staff, and monitored by the ISM to ensure that it is being followed.

Finding No. 2:

The Board had not maintained a current formal risk analysis regarding its information technology resources, and consequently had inadequate disaster recovery procedures to ensure continuous service or minimize the impact should a major disruption occur.

Management should establish a systematic risk analysis that is performed on a recurring basis and updated with results of audits, inspections, and identified incidents. The risk analysis is a systematic process of evaluating vulnerabilities of a processing system and its data to the threats facing it in its environment. The risk analysis provides management a basis to manage their risks by assuming the risk and the potential losses or selecting cost-effective controls and safeguards to reduce the risk to an acceptable level. The risk analysis forms the basis for developing a disaster recovery plan used to provide for continuous service in the event of a major disruption.

We noted the following deficiencies:

- The Board had not maintained a current formal risk analysis as required by the Board's Information Resource Security Plan. The Florida State Board of

Administration and Florida Hurricane Catastrophe Fund Business Impact Analysis Report, prepared by Harris Disaster Recovery Associates and dated March 21, 1997, addressed risk issues for cost and losses based on down timeframes for the Board's business processes such as short-term investment balances, fund wires, investment decisions, cash float interest, and daily reconciliation. The Sysinct Enterprise Security Assessment, dated May 8, 2001, provided a vulnerability assessment of the Board's network. The Board had implemented some of the security controls included in the Information Resource Security Plan to mitigate its risk identified by the aforementioned risk analyses. However, without maintaining a current formal risk analysis, management may not have all of the information necessary to determine an acceptable level of risk.

- Contrary to the Board's establishment of a disaster recovery plan as a strategic objective in its Strategic Plan for 2002 through 2007, the Board did not have a current and complete disaster recovery plan. During our audit, the disaster recovery plan provided to us revealed that the plan:
 - had not be updated since it was created in June 26, 1997,
 - was incomplete since it contained only the first three chapters out of the five chapters listed in the table of contents. From the table of contents, chapter four detailed the recovery duties and responsibilities of teams based on functional areas. Chapter

five was an appendix containing vendor information,

- contained an outdated employee personnel skills list. Our test of 66 employees revealed that 36% were no longer employed by the Board as of February 11, 2002,
- contained no prioritized list of services or applications to be used to determine the order of restoration, and
- contained no list of resources needed to restore each service.

Recommendation:

The Board should maintain a current formal risk analysis regarding its information technology resources and use the results of the risk analysis to develop a comprehensive disaster recovery and security plan for ensuring continuous information technology services. The responsibilities for these tasks should be assigned to the Board's information security manager as outlined in the Information Resource Security Plan.

Other Matters:

The United States Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which addresses electronic data interchange, privacy, and information security standards for personal health information. HIPAA provides for civil and criminal penalties for noncompliance. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards and privacy with security regulations expected to be published in 2002. The Board does not transmit any data concerning

the health status of employees and their dependents, and has determined that the pending HIPAA regulations will have no impact on the Board.

Section 121.4501, Florida Statutes, establishes the Public Employee Optional Retirement Plan (PEORP). This optional retirement program makes available to public employees a defined contribution plan that is portable with the employee and through which the employee can specify how his or her retirement moneys are invested. In the past the State had controlled employee retirement funds and the investment of these funds through a defined benefit plan. As of June 2002, State employees will be in an open enrollment period where the option exists to convert from the existing defined benefit plan to the new PEORP. Consequently, the impact of the new retirement plan on the Board and on the defined benefit plan was unknown as of the end of the field work. However, as of April 2002, the Board estimated asset transfers to be \$4.58 billion, which is a decrease from the original January 2001 estimate of \$13.24 billion.

We will review the impact of the PEORP on the Board's management of the retirement funds, including, specifically, the State Street Prime-Meridian System, in a future audit.

Scope, Objectives, and Methodology:

The scope and objectives of this audit focused on evaluating selected information technology functions applicable to the State Street Prime-Meridian System during the period October 2001 through February 2002. Our objectives were to determine the effectiveness of selected general and application controls relating to the State Street Prime-Meridian System; to determine the Board's awareness of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and actions, if any, that had been taken

concerning this legislation; and to determine the anticipated impact of the new State retirement options on the existing State Street Prime-Meridian System.

To meet our audit objectives, we reviewed applicable Florida Statutes, administrative rules, and auditing literature; interviewed appropriate Board personnel; reviewed Board policies and procedures and other applicable documentation; obtained an understanding of management controls relating to selected information systems functions; observed control processes and procedures; and performed various other audit procedures to test selected controls related to the State Street Prime-Meridian 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 audit.



William O. Monroe, CPA
Auditor General

Board Response:

In a response letter dated June 21, 2002, the Executive Director generally concurred with our audit findings and recommendations. The Executive Director's response can be viewed in its entirety on the Auditor General Web site.

**STATE BOARD OF ADMINISTRATION
STATE STREET PRIME-MERIDIAN SYSTEM
INFORMATION TECHNOLOGY AUDIT**



We conducted our audit in accordance with applicable standards contained in Government Auditing Standards issued by the Comptroller General of the United States. This audit was conducted by Shera Bake, CISA, and supervised by Tina Greene, CPA, CISA. Please contact Jon Ingram, CPA*, CISA, Audit Manager, with any questions regarding this report. He may be reached via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.*

This report and other Auditor General reports can be obtained on our Web site (www.state.fl.us/audgen); by telephone at (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**

Post Office Box 13300
32317-3300
1801 Hermitage Boulevard-Suite 100
Tallahassee, Florida 32308
(850) 488-4406

JEB BUSH
GOVERNOR
AS CHAIRMAN

TOM GALLAGHER
STATE TREASURER
AS TREASURER

ROBERT F. MILLIGAN
STATE COMPTROLLER
AS SECRETARY

TOM HERNDON
EXECUTIVE DIRECTOR

June 21, 2002

Mr. Bill Monroe
Auditor General
111 West Madison Street
Claude Pepper Building, Room G74
Tallahassee, FL 32302

Dear Mr. Monroe:

The following responses are submitted to the audit recommendations and comments listed in your "Preliminary and Tentative Audit Findings and Recommendations" for the audit of the Florida State Board of Administration's (SBA) Prime Meridian System.

Audit Recommendation #1: The SBA should formally appoint an information security manager to administer the SBA's security program and assign this individual the responsibilities as defined in the Information Resource Security Plan. Additionally, the Information Resource Security Plan should be periodically updated to include changes to technology or processes, circulated among the staff, and monitored by the Information Security Manager to ensure that it is being followed.

Response: We are planning to update the Information Resources Security Plan which will designate the Information Security Manager by the end of fiscal year 2002/03.

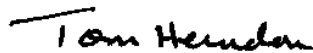
Audit Recommendation #2: The SBA should maintain a current formal risk analysis regarding its information technology resources and use the results of the risk analysis to develop a comprehensive disaster recovery and security plan for ensuring continuous information technology services. The responsibilities for these tasks should be assigned to the SBA's Information Security Manager as outlined in the Information Resource Security Plan.

Response: Business processes are being updated and at the completion of that review, risk analysis information will be updated for each process. A comprehensive Disaster

Recovery and Security Plan will be formulated using the business process and risk analysis information. As stated in the Information Resource Security Plan, responsibility for these duties will be assigned to the Information Security Manager.

Please feel free to call the Chief Financial Officer, Gwenn Thomas, at 413-1393 if you need any further assistance. As always, we appreciate your diligence and assistance.

Sincerely,

A handwritten signature in black ink that reads "Tom Herndon". The signature is written in a cursive style with a horizontal line above the first few letters.

Tom Herndon
Executive Director