AUDITOR GENERAL

WILLIAM O. MONROE, CPA

HILLSBOROUGH COUNTY DISTRICT SCHOOL BOARD

LAWSON FINANCIALS MODULE

Information Technology Audit

SUMMARY

To support its financial management needs, the Hillsborough County District School Board (District) used an enterprise resource planning (ERP) software product, Lawson Software Insight 8 Business Management System, from Lawson Software, Inc., which included modules for Financials and Procurement (Financials), and Human Resources and Payroll.

Our audit focused on selected information technology (IT) controls applicable to the Financials module of the Lawson ERP Software during the period October 2005 through February 2006. The audit included general IT controls over system modification and access to programs and data, and selected application IT controls relevant to the Lawson Financials module.

We noted that improvements were needed in District security controls surrounding the Lawson Financials module and the overall IT environment. Additional IT audit matters were disclosed as Finding No. 1 in the District's Financial and Federal Single Audit Report, No. 2006-157, dated March 2006.

BACKGROUND

In May 2001, the District selected Lawson Software, Inc.'s Insight 8 Business Management System for its ERP system consisting of the Financials module and the Human Resources and Payroll module. The Financials module was implemented by the District in December 2003, and the Human Resources and Payroll module was implemented in July 2005.

The primary user of the Lawson Financials module was the Business Division of the District. The Business Division was responsible for the financial operations of the District, such as accounts payable, student nutrition accounting, and general accounting.

The Lawson Software ERP system is a fully open, web-addressable technology. This ERP software provides General Accounting, Human Resources, Inventory, Payroll, and Purchasing business functions, among others. The Lawson software operated using the DB2 database on IBM's RX6000 servers under the Advanced Interactive Executive (AIX) operating system.

The Information and Technology Division was responsible for providing IT resources to meet the needs of the District. The Applications, Data Center, Technology Services, and Customer Service and Support, Assessment and Accountability, and the Office of Supplier Diversity were the functional areas that reported to the Chief Information and Technology Officer. The Information and Technology Division was also responsible for applying system updates from Lawson and for making District-initiated customization changes to the Lawson Software.

FINDINGS

As disclosed in the following paragraph, we noted aspects of the District's IT controls surrounding the Lawson Financials module that needed improvement. Additional matters resulting from this IT audit were disclosed as Finding No. 1 in the District's Financial and Federal Single Audit Report, audit report No. 2006-157, dated March 2006. In that finding, we noted instances of excessive system access privileges and lack of appropriate segregation of duties with regard to the Lawson Financials module. The Superintendent concurred with those findings in her response.

Finding No. 1: Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data and information technology resources. Our audit disclosed aspects of the District's security controls surrounding the Lawson Financials module and the overall IT environment that needed improvement. Specifically:

- The District had not adapted its security policies and procedures to the server environment in which the Lawson application was operated. Certain security policies and procedures existed at the District, but were primarily applicable to the mainframe environment in which the District's previous financial software was operated.
- Good security management practices include procedures for timely notifying security administrators of employee terminations. Immediate notification is necessary to facilitate the prompt cancellation of employee system access privileges. The District had not established policies and procedures for the removal of terminated employees' access privileges within the Lawson server environment. Our audit tests of 30 District employees who terminated during the 2004 and 2005 calendar years included 2 employees who had been provided access privileges to the Lawson Financials module. In both instances, these employees continued to have access privileges to Lawson Financials after their dates of termination. Until October 2005, the District did not maintain a record of the date a user's access privileges were last used within the Lawson environment. Consequently, the District could not determine, in response to our audit inquiry, whether these Lawson user accounts had been used subsequent to the employees' termination. Without adequate procedures to timely remove the access rights of terminated employees, the risk is increased of unauthorized access to District data and IT resources.
- For the District's mainframe environment security policies and procedures, there was no process for obtaining from employees a signed acknowledgment of their receipt, understanding, and acceptance of responsibility for District security requirements. The absence of such acknowledgment could limit the District in any legal recourse, should it be necessary, against individuals misusing District information technology resources.
- The District did not require each system owner to perform periodic reviews of access privileges. Access privileges were reviewed and assigned for the Lawson Financials module during the December 2003 implementation, but had not been reviewed subsequent to implementation. The absence of periodic access reviews increases the risk that inappropriate access privileges, should they exist, would not be timely detected. Inappropriate access privileges increase the likelihood of fraud or error occurring in the Financials module.
- Certain application and network security control features implemented by the District needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, the appropriate District personnel have been notified of the issues.

Recommendation: The District should establish security policies and procedures for the Lawson server environment; require applicable personnel to acknowledge in writing their receipt and understanding of, and responsibility for, security policies and procedures; require each system owner to perform periodic reviews of the appropriateness of system access privileges; and strengthen application and network security controls.

PRIOR AUDIT FINDINGS

The District had corrected, or was in the process of correcting, IT-related deficiencies noted in audit report No. 2004-018 that were within the scope of our audit. However, a portion of Finding No. 1 was previously noted in audit report No. 2004-018 and remained unresolved as of the completion of our audit field work.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected District general and application IT controls. Our scope focused on selected IT controls applicable to the Lawson Financials module during the period October 2005 through February 2006, including controls over system modification, access to programs and data, and application controls. In conducting our audit, we interviewed appropriate District personnel, observed District processes and procedures, and performed various other audit procedures to test selected IT controls.

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

MANAGEMENT RESPONSE

In a letter dated May 5, 2006, the Superintendent provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

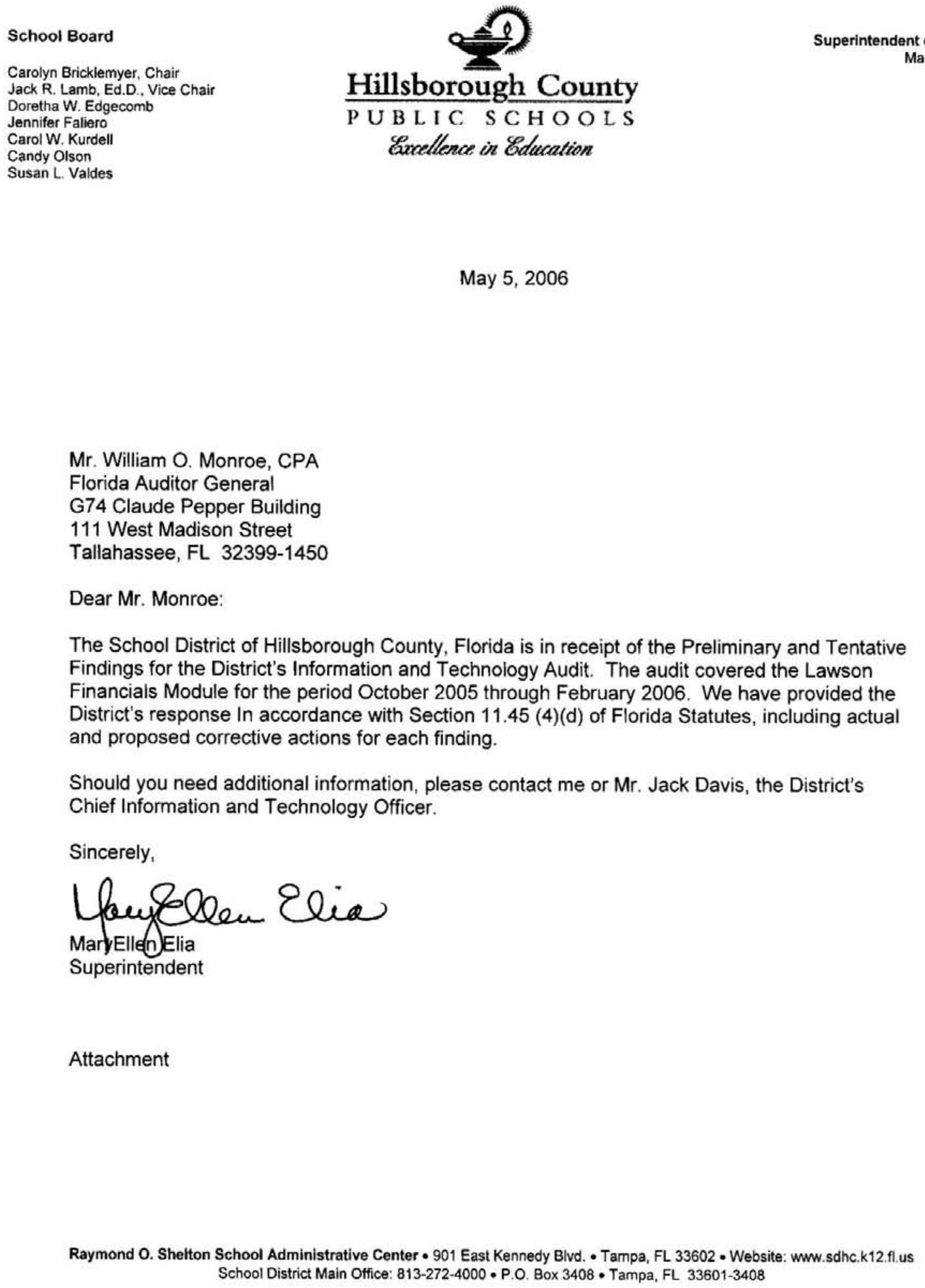
To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Robert McKee, CISA, and supervised by Tina Greene, CPA*, 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.

APPENDIX A

MANAGEMENT RESPONSE



Hillsborough County
PUBLIC SCHOOLS
Excellence in Education

Superintendent of Schools
MaryEllen Elia

May 5, 2006

Mr. William O. Monroe, CPA
Florida Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

The School District of Hillsborough County, Florida is in receipt of the Preliminary and Tentative Findings for the District's Information and Technology Audit. The audit covered the Lawson Financials Module for the period October 2005 through February 2006. We have provided the District's response In accordance with Section 11.45 (4)(d) of Florida Statutes, including actual and proposed corrective actions for each finding.

Should you need additional information, please contact me or Mr. Jack Davis, the District's Chief Information and Technology Officer.

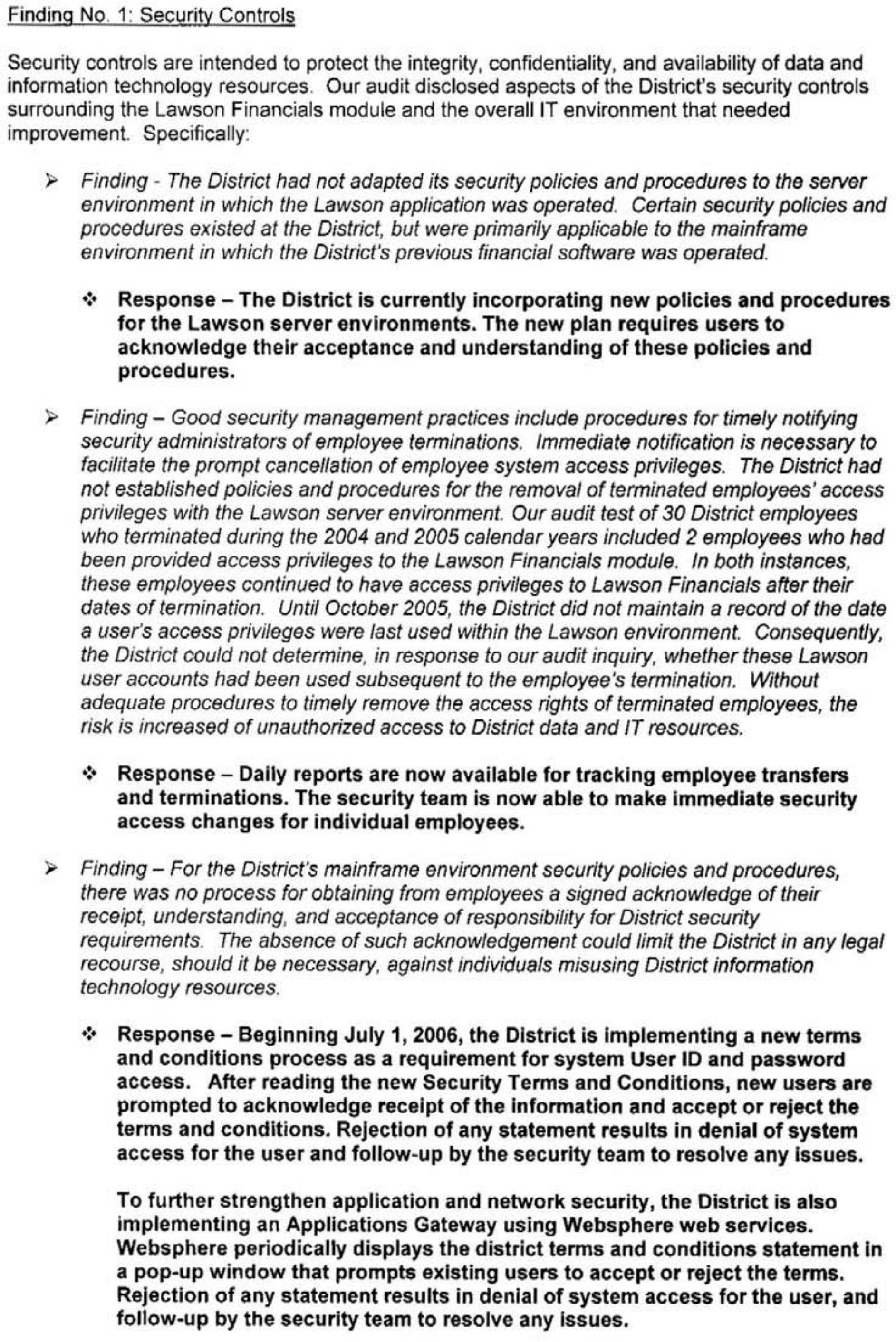
Sincerely,

MaryEllen Elia

MaryEllen Elia
Superintendent

Attachment

Raymond O. Shelton School Administrative Center • 901 East Kennedy Blvd. • Tampa, FL 33602 • Website: www.sdhc.k12.fl.us
School District Main Office: 813-272-4000 • P.O. Box 3408 • Tampa, FL 33601-3408



Finding No. 1: Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data and information technology resources. Our audit disclosed aspects of the District's security controls surrounding the Lawson Financials module and the overall IT environment that needed improvement. Specifically:

- *Finding - The District had not adapted its security policies and procedures to the server environment in which the Lawson application was operated. Certain security policies and procedures existed at the District, but were primarily applicable to the mainframe environment in which the District's previous financial software was operated.*

  - **Response – The District is currently incorporating new policies and procedures for the Lawson server environments. The new plan requires users to acknowledge their acceptance and understanding of these policies and procedures.**

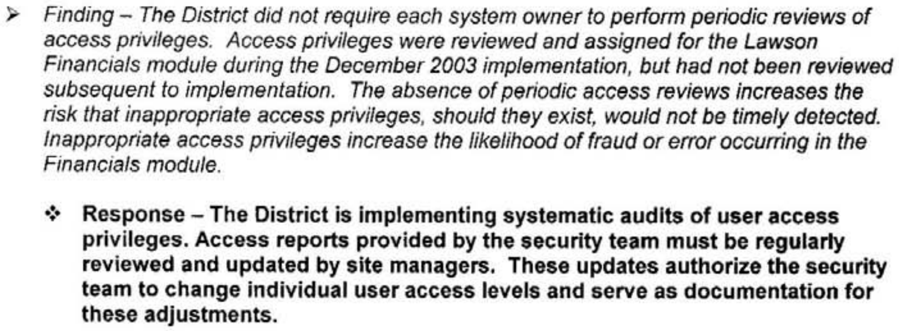
- *Finding – Good security management practices include procedures for timely notifying security administrators of employee terminations. Immediate notification is necessary to facilitate the prompt cancellation of employee system access privileges. The District had not established policies and procedures for the removal of terminated employees' access privileges with the Lawson server environment. Our audit test of 30 District employees who terminated during the 2004 and 2005 calendar years included 2 employees who had been provided access privileges to the Lawson Financials module. In both instances, these employees continued to have access privileges to Lawson Financials after their dates of termination. Until October 2005, the District did not maintain a record of the date a user's access privileges were last used within the Lawson environment. Consequently, the District could not determine, in response to our audit inquiry, whether these Lawson user accounts had been used subsequent to the employee's termination. Without adequate procedures to timely remove the access rights of terminated employees, the risk is increased of unauthorized access to District data and IT resources.*

  - **Response – Daily reports are now available for tracking employee transfers and terminations. The security team is now able to make immediate security access changes for individual employees.**

- *Finding – For the District's mainframe environment security policies and procedures, there was no process for obtaining from employees a signed acknowledge of their receipt, understanding, and acceptance of responsibility for District security requirements. The absence of such acknowledgement could limit the District in any legal recourse, should it be necessary, against individuals misusing District information technology resources.*

  - **Response – Beginning July 1, 2006, the District is implementing a new terms and conditions process as a requirement for system User ID and password access. After reading the new Security Terms and Conditions, new users are prompted to acknowledge receipt of the information and accept or reject the terms and conditions. Rejection of any statement results in denial of system access for the user and follow-up by the security team to resolve any issues.**

    To further strengthen application and network security, the District is also implementing an Applications Gateway using Websphere web services. Websphere periodically displays the district terms and conditions statement in a pop-up window that prompts existing users to accept or reject the terms. Rejection of any statement results in denial of system access for the user, and follow-up by the security team to resolve any issues.



- *Finding – The District did not require each system owner to perform periodic reviews of access privileges. Access privileges were reviewed and assigned for the Lawson Financials module during the December 2003 implementation, but had not been reviewed subsequent to implementation. The absence of periodic access reviews increases the risk that inappropriate access privileges, should they exist, would not be timely detected. Inappropriate access privileges increase the likelihood of fraud or error occurring in the Financials module.*

  - **Response – The District is implementing systematic audits of user access privileges. Access reports provided by the security team must be regularly reviewed and updated by site managers. These updates authorize the security team to change individual user access levels and serve as documentation for these adjustments.**

THIS PAGE INTENTIONALLY LEFT BLANK