AUDITOR GENERAL

DAVID W. MARTIN, CPA

HILLSBOROUGH COUNTY DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The Hillsborough County District School Board (District) utilizes enterprise resource planning (ERP) software from Lawson Software, Inc., to support various administrative functions. Our audit focused on evaluating selected general information technology (IT) controls applicable to the Lawson ERP software and the surrounding infrastructure during the period July 2007 through February 2008 and selected actions taken from July 2006. In addition, we determined the status of corrective actions taken regarding IT-related deficiencies disclosed in audit report Nos. 2006-157 and 2006-178.

The results of our audit are summarized below:

Finding No. 1: **The District's entitywide security program needed improvement.**

Finding No. 2: **We noted deficiencies in the District's management of access privileges.**

Finding No. 3: **Program change controls over the Lawson ERP software needed improvement.**

Finding No. 4: **The District had not tested its Disaster Recovery Plan at an off-site location.**

Finding No. 5: **In addition to the matters discussed in Finding Nos. 1 and 2, certain security controls related to the Lawson ERP software and the supporting infrastructure needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the District's data and IT resources.**

BACKGROUND

The Lawson ERP software (Lawson) provides application processing for the District's administrative functions, such as finance, procurement, human resources, payroll, and inventory. The management and maintenance of Lawson is the responsibility of Information Services (IS).

IS is a district-level department within the IT Division that provides an integrated set of automated processes and support to meet administrative and operational needs of the District. IS consists of two main sections, the Data Center and Applications, and provides IT application and program services to over 25,000 employees, as well as support for more than 190,000 students. The IS department is under the direction of the Chief Information and Technology Officer, who reports to a Deputy Superintendent.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: District Security Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of management's commitment to addressing security risks. The program establishes a framework and continuing cycle of activity assessing risks, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Principles that help ensure that information security policies address current risks include performing a periodic risk assessment to determine needs, implementing appropriate security controls to mitigate identified risks, and promoting security awareness.

The District's entitywide security program needed the following improvements:

- Although District personnel worked with network engineers from major vendors to implement additional safeguards, the District had not performed, since March 2004, a risk assessment identifying and documenting the IT systems and resources, vulnerabilities and exposures, policies and control measures, and management's signed acceptance of the unmitigated risks. In response to audit inquiry, District personnel indicated that a formal external assessment is planned following the March 2008 Lawson application upgrade.
- The District did not have adequate Board-approved written security policies and procedures. The District utilized undocumented procedures to control many of its security functions, such as security administration over applications, network, database, and operating systems; the use, monitoring, and minimum required security of wireless devices and personal digital assistants (PDAs); firewall management; and the use of e-mail and the Internet.
- The District had not implemented a security training program to facilitate employees' education and training on security responsibilities, including data classification and acceptable or prohibited methods for storage and transmission, Internet and e-mail usage, password protection and usage, and workstation controls. In addition, the District did not require a signed acknowledgment by employees of their responsibilities for District information security.

In response to audit inquiry, District personnel indicated that a company was hired to assist District personnel with reviewing its policies and procedures. Updated policies are scheduled to be brought to the School Board for approval in July 2008, after which procedures will be documented. Without a well-designed District security program, including a documented risk framework, controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. This increases the risk that sensitive or critical IT resources will not be sufficiently protected.

Recommendation: The District should continue its development of an entitywide security program. A risk assessment should be the starting point for identifying risks and determining the District's needs. Appropriate security policies and procedures should be implemented to mitigate the identified risks and support the confidentiality, availability, and integrity of information resources. Management should also promote security awareness through adequate training programs.

Finding No. 2:
Access Controls

Access controls are intended to protect data and IT resources from unauthorized disclosure, modification, or loss. We noted certain deficiencies in the District's access control procedures as described below:

- Authorization of access granted to Lawson was not always adequately documented on access request forms. Effective access controls include instituting policies and procedures for authorizing access to information resources, documenting such access authorizations, and then periodically monitoring the actual access capabilities through comparisons of the authorizations. Of 14 authorizations selected for testing, 5 access request forms were not specific enough for us to determine the access that had been requested. In addition, access request forms were not used to request Lawson access for personnel in Information Services. When access authorization is inadequately documented, the risk of inappropriate use of information resources is increased.
- Some terminated employees' access privileges were not timely removed. 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 terminated employees or others. Our comparison of 46 former employees who terminated employment with the District

during the period July 1, 2006, through October 15, 2007, to users with access privileges to Lawson and the operating system disclosed that, as of October 17, 2007, 10 former employees still had operating system access accounts for 27 to 215 days after the termination dates. Also, as of November 8, 2007, 2 of the 10 still had Lawson access accounts. In response to audit inquiry, District personnel indicated that procedures had been implemented to correct the instances noted above. However, no review of user accounts had been conducted by District personnel to determine if the Lawson and operating system access privileges of terminated employees were being timely deleted. Without the timely deletion of access privileges of employees who terminate employment with the District, the risk is increased that the access privileges could be misused by the former employees or others.

- ➢ The District's review of user access to IT resources was limited. The periodic review of user accounts and access privileges helps to ensure that access privileges remain appropriate. Although a review of Lawson roles and profiles had been performed by District personnel, a comprehensive periodic review of individual access privileges granted to users of Lawson had not been performed to ensure that user access continued to be appropriate. In addition, reviews of user access privileges to the operating system, database, and security software had not been performed.

- ➢ Inappropriate or unnecessary access privileges existed. The implementation of separation of duties by management eliminates the possibility for a single individual to subvert a critical process. It is important for management to ensure that employees are performing only those duties stipulated for their respective jobs and positions. Our review of Lawson and database access privileges disclosed the following:

  - Six programmers had end-user update access to Lawson that was inappropriate for their job functions. A proper separation of duties in the IT environment generally provides for the application programming function and the updating of live data to be performed independently of one another. In response to audit inquiry, District personnel indicated that, effective February 1, 2008, the programmers no longer have end-user update access.

  - Three employees had multiple Lawson user IDs that, in combination, provided excessive access for their job functions. In response to audit inquiry, District personnel indicated that the additional IDs for the three employees have now been deleted.

  - Seven Purchasing Department employees had the capability to add a vendor, approve a vendor, and perform a mass update to vendor information. Five of the seven employees also had the capability to update a vendor address. An additional two employees from other business departments had the capability to add a vendor and perform a mass update to vendor information. This access either permitted incompatible duties to be performed by the same employee or was unnecessary for their job functions. In response to audit inquiry, District personnel indicated that a new process has been approved to capture and review vendor file changes.

  - The Lawson database access privileges of one employee provided administrator rights to the database that was inappropriate for the employee's job function. On December 21, 2007, in response to audit inquiry, District personnel indicated that either the access will be revoked or a new user ID without administrator privileges will be issued.

Recommendation: The District should strengthen its access control procedures, including adequately documenting access authorizations, timely deleting access for terminated employees, reviewing the ongoing appropriateness of access privileges, and deleting inappropriate or unnecessary access privileges.

Finding No. 3: Program Change Controls

Effective controls over changes to application programs are intended to ensure that only authorized and properly functioning changes are implemented.

Program change controls include procedures to ensure that all changes are properly authorized, tested, and approved for implementation. Program change controls that are typically employed to ensure the continued integrity of application systems include providing written evidence of the program change control process, thorough testing and approving of changes by a person or group independent of the individual making the changes, controlling concurrent updates so that multiple programmers are prevented from making changes to the same program, maintaining copies of previous versions, and separating the responsibility for moving approved changes into the production environment and database responsibilities from individuals who developed the changes.

Our audit disclosed that District program change controls needed improvements in the following areas:

- Although Lawson provided a manual for application maintenance, including installing patches, the District did not have written procedures describing District practices to be used for patch management.
- There was no independent review of program changes by other IT personnel prior to user testing.
- Although changes were tracked in programmers' spreadsheets, previous versions of programs were not maintained by the District, limiting the ability to restore programs to a previous version.
- Multiple programmers were not prevented from changing the same program simultaneously.
- Some programmers, security administrator personnel, and operators had access to utility software defined in the Lawson production environment that allowed changes to the application and database. In response to audit inquiry, District personnel indicated that access to the utility software has now been removed from the programmers.

Without effective program change controls, the risk is increased that unauthorized or erroneous programs, including changes or patches, could be moved into the production environment without timely detection.

Recommendation: The District should document District patch management procedures, establish an independent review of program changes by IT staff not having the ability to change the programs, provide a mechanism for the prevention of simultaneous program changes by multiple programmers, and maintain previous versions of programs. Additionally, utility software should be regularly reviewed to ensure that a proper separation of duties exists among programmers, operators, and security administration personnel.

Finding No. 4: Disaster Recovery Plan

Disaster recovery planning is an element of IT controls established to manage the availability of valuable data and computer resources in the event of a processing disruption. The success and effectiveness of a disaster recovery plan requires, among other things, periodic testing to demonstrate the plan's validity, value, and usefulness.

Although the District had restored the Lawson production system numerous times in the test environment using backup tapes and restore procedures documented in the disaster recovery plan, the plan had not been tested at an off-site location. The absence of testing the execution of disaster recovery provisions at an off-site location limits management's assurance that critical IT services will be restored in a timely manner should an interruption in IT operations occur.

Recommendation: The District should perform a test of its disaster recovery plan each year at its off-site location to ensure a timely recovery in the event of a disaster.

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 District security controls related to Lawson and the supporting infrastructure, in addition to the matters discussed in Finding Nos. 1 and 2, that needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District data and IT resources. However, appropriate District personnel 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 the District's data and IT resources may be subject to improper disclosure, destruction, or modification.

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

PRIOR AUDIT FINDINGS

Except as previously noted in Finding Nos. 1 through 3, and 5, the District had corrected, or was in the process of correcting, the IT-related deficiencies disclosed in audit report Nos. 2006-157 and 2006-178.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected District IT controls and to determine whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed in audit report Nos. 2006-157 and 2006-178.

The scope of our audit focused on evaluating selected general IT controls applicable to the Lawson ERP software and the surrounding infrastructure during the period July 2007 through February 2008 and selected actions taken from July 2006.

This IT audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. In conducting our audit, we interviewed appropriate District personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to the Lawson ERP software and the surrounding infrastructure.

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

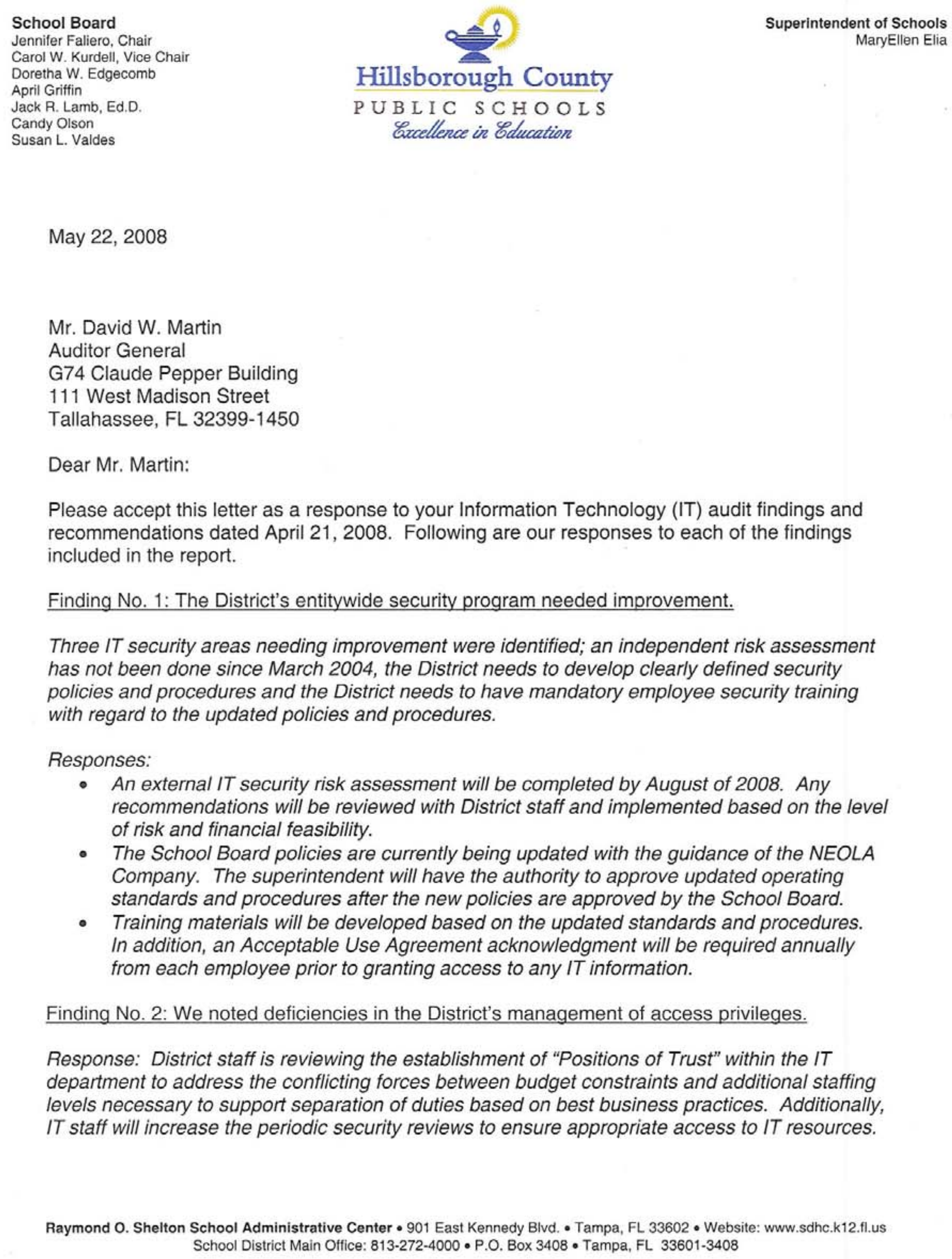
In a letter dated May 22, 2008, the Superintendent provided responses to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

This audit was conducted by Stephanie J. Hogg, CISA, and supervised by Nancy Reeder, 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.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



School Board
Jennifer Faliero, Chair
Carol W. Kurdell, Vice Chair
Doretha W. Edgecomb
April Griffin
Jack R. Lamb, Ed.D.
Candy Olson
Susan L. Valdes

Hillsborough County
PUBLIC SCHOOLS
Excellence in Education

Superintendent of Schools
MaryEllen Elia

May 22, 2008

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

Dear Mr. Martin:

Please accept this letter as a response to your Information Technology (IT) audit findings and recommendations dated April 21, 2008. Following are our responses to each of the findings included in the report.

Finding No. 1: The District's entitywide security program needed improvement.

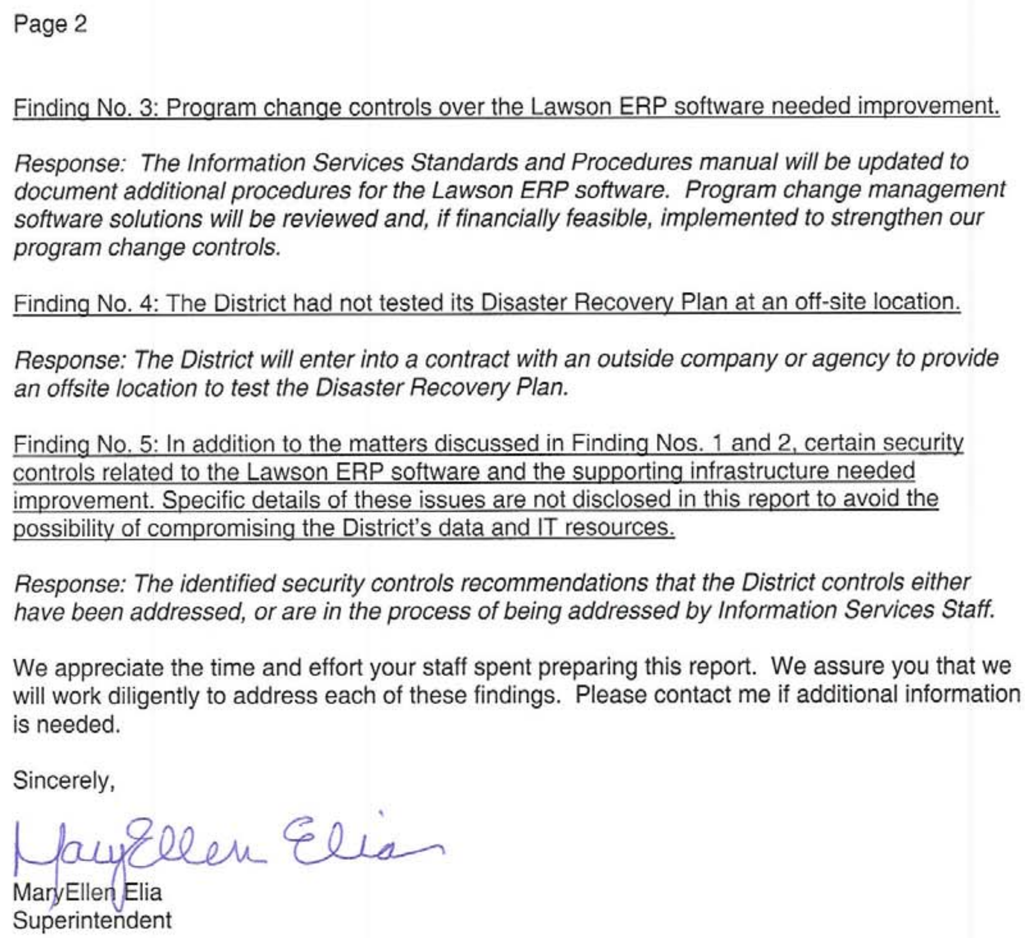
Three IT security areas needing improvement were identified; an independent risk assessment has not been done since March 2004, the District needs to develop clearly defined security policies and procedures and the District needs to have mandatory employee security training with regard to the updated policies and procedures.

Responses:

- *An external IT security risk assessment will be completed by August of 2008. Any recommendations will be reviewed with District staff and implemented based on the level of risk and financial feasibility.*
- *The School Board policies are currently being updated with the guidance of the NEOLA Company. The superintendent will have the authority to approve updated operating standards and procedures after the new policies are approved by the School Board.*
- *Training materials will be developed based on the updated standards and procedures. In addition, an Acceptable Use Agreement acknowledgment will be required annually from each employee prior to granting access to any IT information.*

Finding No. 2: We noted deficiencies in the District's management of access privileges.

Response: District staff is reviewing the establishment of "Positions of Trust" within the IT department to address the conflicting forces between budget constraints and additional staffing levels necessary to support separation of duties based on best business practices. Additionally, IT staff will increase the periodic security reviews to ensure appropriate access to IT resources.



Page 2

Finding No. 3: Program change controls over the Lawson ERP software needed improvement.

Response: The Information Services Standards and Procedures manual will be updated to document additional procedures for the Lawson ERP software. Program change management software solutions will be reviewed and, if financially feasible, implemented to strengthen our program change controls.

Finding No. 4: The District had not tested its Disaster Recovery Plan at an off-site location.

Response: The District will enter into a contract with an outside company or agency to provide an offsite location to test the Disaster Recovery Plan.

Finding No. 5: In addition to the matters discussed in Finding Nos. 1 and 2, certain security controls related to the Lawson ERP software and the supporting infrastructure needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the District's data and IT resources.

Response: The identified security controls recommendations that the District controls either have been addressed, or are in the process of being addressed by Information Services Staff.

We appreciate the time and effort your staff spent preparing this report. We assure you that we will work diligently to address each of these findings. Please contact me if additional information is needed.

Sincerely,

MaryEllen Elia

MaryEllen Elia
Superintendent