REPORT NO. 2009-029
OCTOBER 2008

ESCAMBIA COUNTY

DISTRICT SCHOOL BOARD

Operational Audit

For the Fiscal Year Ended
June 30, 2008

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

BOARD MEMBERS AND SUPERINTENDENT

District School Board members and the Superintendent who served during the 2007-08 fiscal year are listed below:

	District No.
Jeffrey W. Bergosh	***1***
Gerald W. Boone	***2***
Claudia S. Curry	***3***
Patricia Hightower, Chair	***4***
Peter R. Gindl, Sr., Vice-Chair	***5***

Jim Paul, Superintendent

The audit team leader was Edward H. Brewton, CPA, and the audit was supervised by James W. Kiedinger, Jr., CPA. For the information technology portion of this audit, the audit team leader was Stephanie J. Hogg, CISA, and supervised by Nancy Reeder, CPA, CISA. Please address inquiries regarding this report to Gregory L. Centers, CPA, Audit Manager, via e-mail at gregcenters@aud.state.fl.us or by telephone at (850) 487-9039.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

ESCAMBIA COUNTY

District School Board

SUMMARY

Our operational audit for the fiscal year ended June 30, 2008, disclosed the following:

Finding No. 1: The District's management of information technology (IT) access privileges needed improvement.

Finding No. 2: Enhancements could be made to timely terminate the IT access privileges of former employees.

Finding No. 3: The District's IT program change controls needed improvement.

Finding No. 4: The District's security controls within the application and supporting IT environment needed improvement.

Finding No. 5: Improvements could be made in District procedures for timely obtaining background screenings and fingerprints for District and contractual personnel that have direct contact with students.

Finding No. 6: Internal controls over child care fee collections could be strengthened.

Finding No. 7: The District did not provide employees a written statement to specify the purpose for collection of social security numbers (SSNs) for certain documents or timely certify compliance with the new SSN requirements to the Legislature, contrary to Section 119.071(5)(a), Florida Statutes.

Finding No. 8: Enhancements could be made to ensure the adequacy of insurance coverage for charter schools sponsored by the District and design professionals.

Finding No. 9: Instances were noted in which employees did not timely submit their time sheets for work performed beyond their regular assigned duties or certify the work performed on the time sheets.

Finding No. 10: The District had not implemented a formal ongoing security awareness training program to protect IT resources.

BACKGROUND

The District is part of the State system of public education under the general direction of the Florida Department of Education. Geographic boundaries of the District correspond with those of Escambia County. The governing body of the Escambia County District School Board is composed of five elected members. The elected Superintendent of Schools is the executive officer of the School Board. During the audit period, the District operated 66 elementary, middle, high, and specialized schools; sponsored 8 charter schools; and reported 41,078 unweighted full-time equivalent students.

The results of our audit of the District's financial statements and Federal awards for the fiscal year ended June 30, 2008, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Information Technology – Access Controls

The District attempts to assign job responsibilities in the various finance- and human resource-related job areas in a way that promotes good internal control. For example, payroll department employees who have responsibilities

relating to processing payroll checks should not have human resource department responsibilities that allow them to set up a new employee or change an employee's rate of pay. Employees with such responsibilities could create a fictitious employee, change rate of pay, and process payroll checks. Since these employees perform most of these job responsibilities through access to IT applications, it is important that these employees not have access privileges that are incompatible with their job responsibilities.

We reviewed the access privileges to IT applications for selected finance and human resource (HR) employees and identified several employees who had inappropriate or unnecessary access privileges as described below:

- Twenty-one employees from various finance-related departments had the capability to add or change vendor information. An additional employee had the capability to perform invoice matching, make a direct payment to a vendor, add a new vendor, and change existing vendor information.
- Eleven employees in the payroll and staff development departments had the ability to add or update general employee and job base pay information via HR screens.
- Four employees in various departments or schools had the ability to change and submit payroll processing jobs.
- One school employee had the ability to add or update existing general employee and job base pay information, time exceptions, pay adjustments, substitute pay, and account and other compensation information. This employee also had the ability to change and submit payroll processing jobs.

These access privileges either permitted the employees to perform incompatible duties or the access privileges were not necessary for their job functions, increasing the risk of malicious or unintentional disclosure, modification, or destruction of data and IT resources.

The District does not periodically perform a comprehensive review of user access to the finance and HR applications. Although IT personnel make annual inquiries of department heads requesting them to verify that users' access privileges are still appropriate for their job responsibilities, the inquiry focuses on authorizing transactions and does not address all access privileges. The District assigned access privileges based on position, so when a new employee fills an existing position, the new employee receives the same access privileges as the former employee. The District did not review access privileges before issuing them to the new employees. Subsequent to our inquiry, District management indicated that they will review and remove unnecessary access privileges.

IT personnel provide daily activity reports that list the previous day's application activity to department directors. This procedure would serve as a compensating control if the department directors did not have incompatible access privileges and if they reviewed the daily activity reports to verify that all activity was appropriate and authorized. We interviewed three department directors to determine the extent of their review of the daily activity reports. We noted that one department director reviewed the reports when time permitted and another department director did not retain the reports to document such review of the reports. Although a procedure providing for appropriate review of the daily activity reports may compensate for the incompatible access privileges of some users, the District could not evidence that department directors were performing this procedure timely and regularly.

Recommendation: The District should annually perform a comprehensive review of user access privileges to ensure that they are compatible with employee job responsibilities. Additionally, the District should enhance its procedures to ensure that department directors review daily activity reports to ensure timely detection of unauthorized or erroneous transactions and retain evidence of those reviews.

Finding No. 2: Information Technology – Terminated Employee Access

Proper information technology (IT) access controls include provisions to timely remove employee access privileges when employment terminations occur. Prompt action is necessary to ensure that a former employee does not retain IT access privileges that would allow misappropriation or abuse of District assets.

Each week, the District generates a report that shows names of personnel who transferred or terminated employment during the week. IT Data Support personnel use this report to identify employees who should have their access privileges removed. However, our review of the 52 employees with access privileges who terminated employment with the District during the 2007-08 fiscal year disclosed 17 former employees whose access privileges to certain IT resources, such as human resource and student records, were not promptly discontinued upon termination. According to District records, the District did not remove access privileges for the 17 employees from 11 to 340 days after their employment termination dates. IT Department personnel indicated that the access privileges of the former employees were not timely terminated due to e-mail transmission problems and higher priority projects. Subsequent to our inquiry in July 2008, IT Department personnel indicated that access rights for these former employees were removed. IT Department personnel also indicated that District security software automatically inactivates the access of employees who do not use their privileges within 30 days. However, access privileges should be closed immediately upon termination to minimize the risk that the privileges could be misused by the former employee or others.

Although our tests did not disclose any instances of errors or misappropriations as a result of the control deficiencies noted above, the District is exposed to a greater risk of loss when it does not timely terminate the IT access privileges of former employees.

Recommendation: The District should continue its efforts to enhance controls over the timely deletion of IT access privileges for terminated employees to minimize the risk of compromising District resources.

Finding No. 3: Information Technology – 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 separating the responsibility for moving approved changes into the production environment from employees who developed the changes.

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

- Although application change requests were usually documented via e-mails, there was no form used to document the programmer's name; the name of the programmer or analyst who tested the change; user acceptance, if applicable; management approval for the implementation of the change; and the employee who implemented the change. The lack of a complete record of the work and approval flow associated with program changes may limit management's ability to monitor the program change process and detect departures from appropriate program change controls, should they occur.
- The movement of program changes to production was performed by employees who had the capability of making the program change or developing a new program. During testing, we noted that the five employees from Application Support had the capability to move program changes into production. Although District management recognized and documented their acceptance of this access, allowing the same employee to create

or modify a program and move the program to production exposes the District to a greater risk that these employees could implement unauthorized or erroneous programs without timely detection.

- No test environment was used when testing program changes to the finance application. Although finance production program libraries and data were backed up before testing major update changes to the finance application, program changes were performed in the production environment and then tested against production data. Since testing was performed in the production environment, six programmers or analysts had end-user update access to the financial application. A proper separation of duties in the IT environment generally provides for application programming and updating of production data to be performed independently of one another. Although District management recognized and documented acceptance of analysts and programmers having this access**,** programming and testing in the production environment increased the risk of corrupting production program libraries and having to restore programs to a previous version. The risk is also increased of a loss of productivity for employees who would need to reenter lost information if the District was unable to restore the previous version.
- District management had not established written policies and procedures governing the change control process for applications and data. Absent written policies and procedures, the risk is increased that management's expectations regarding program change controls will not be clearly understood or consistently followed by programming personnel.

Recommendation: The District should document who changed, tested, approved, and moved programs to production and ensure that an appropriate separation of duties exists regarding the testing and movement of programs to production. The District should also create a test environment for the programming and testing of program changes to the finance application and then restrict programmers and analysts from having end-user access privileges. In addition, the District should establish written policies and procedures to govern the program change control process.

Finding No. 4: Information Technology – Security Controls

The District should improve certain security controls related to its network and applications. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the District's data and IT resources. However, we have notified appropriate District management of the specific issues. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that District data and IT resources may be subject to improper disclosure, modification, or destruction.

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

Finding No. 5: Background Screening and Fingerprinting Requirements

Improvements could be made in District procedures for timely obtaining background screenings and fingerprints for District and contractual personnel that have direct contact with students. Section 1012.56(9), Florida Statutes (currently Section 1012.56(10), Florida Statutes), required that instructional personnel renewing their teaching certificates undergo a background screening, including a requirement that such employees file a complete set of fingerprints. These screening and fingerprint requirements, pursuant to Section 1012.465, Florida Statutes, also apply to noninstructional personnel every five years following employment and contractors that have access to school grounds while students are present. In a memorandum dated June 25, 2004, the Florida Department of Education (FDOE) recommended that districts conduct background screenings for certified instructional employees every five years, at the time of renewal of their teaching certificates, and that background screenings be obtained for

approximately 20 percent of the noninstructional employees each year, beginning with the 2004-05 fiscal year, in order to complete background screenings for all employees over the five-year period ending July 1, 2009.

Personnel. The District elected to perform the background screenings of District personnel by location and plans to have the screenings completed by the July 1, 2009, deadline. However, at June 30, 2008, the District had only performed screenings of approximately 47 percent (approximately 2,800) of its personnel, or 33 percent less than the 80 percent benchmark recommended by FDOE. A similar finding was noted in our report No. 2006-181.

Contractors. The District established procedures for identifying contractors and their employees that were subject to the background screenings and generally obtained the screenings or evidence of the screenings for applicable individuals. However, our review of 18 contractors disclosed that the District did not obtain evidence of the required background checks for an unidentified number of employees working for 3 of the contractors, as follows:

- Employees of a security company that provided traffic guard services at schools.
- Employees of a nursing services company that provided nursing services in the schools.
- Employees of an educational mentoring service not-for-profit organization that provided mentoring and educational services for students at their location after school. The contract provided that the employees would have the required background screenings.

District employees did not verify background screenings for the first two companies because they thought the licensing requirements for employees working for those companies were more extensive than the required background screenings. They also did not require evidence of background screenings for the employees of the educational mentoring services organization because they overlooked the contractual requirement and decided that because the services were not performed on school grounds, the law did not apply. However, given that the contractors had direct contact with students and were not under the direct supervision of a District employee, the District would be subject to these provisions.

Without timely completion of the required fingerprinting and background screenings of District and contractual personnel, there is an increased risk that individuals with unsuitable backgrounds may be allowed access to students.

Recommendation: The District should ensure that it timely obtains the required background screenings for its employees and contractors. In those instances where contractors perform their own background screenings, the District should obtain evidence of the required screenings or perform the screenings.

Finding No. 6: Child Care Program Collection Procedures

Collection procedures of District-operated child care programs could be improved. During the 2007-08 fiscal year, the District offered after-school child care programs at 33 schools, 7 of which were operated by District personnel. Total child care fee collections at the District-operated sites were approximately $428,600 during the 2007-08 fiscal year. At District-operated sites, the child care workers generally transferred fee collections to the school bookkeepers, who deposited them in the school's internal accounts. Subsequently, the school bookkeepers remitted the collections to the District office for deposit into District budgetary accounts.

Our review of child care fee collection procedures at Bellview and Ensley Elementary schools, two of the District-operated sites, with collections totaling $61,603 and $38,788, respectively, disclosed certain control deficiencies, as follows:

- District personnel did not independently verify that fees were appropriately assessed, collected, and deposited in the school internal funds or District budgetary accounts. Without such, there is an increased risk that errors or misappropriations could occur and not be detected timely.
- Prior to deposit by the school bookkeeper, child care employees at Bellview Elementary placed collections in unlocked cash bags that were not stored in a secure location. Since more than one employee had access to the cash bags, the District may not be able to fix responsibility if collections were missing.

We noted similar findings in our report No. 2006-181.

Recommendation: The District should strengthen internal controls over child care fee collections. Such procedures should ensure the fees are properly assessed, collected, and deposited.

Finding No. 7: Collection of Social Security Numbers

The Legislature has acknowledged in Section 119.071(5)(a), Florida Statutes, the necessity of collecting social security numbers (SSNs) for certain purposes because of their acceptance over time as a unique numeric identifier for identity verification and other legitimate purposes. The Legislature has also recognized that SSNs can be used to acquire sensitive personal information, the release of which could result in fraud against individuals or cause other financial or personal harm. Therefore, public entities are required to provide extra care in maintaining such information to ensure its confidential status.

Effective October 1, 2007, Section 119.071(5)(a), Florida Statutes, as amended by Chapter 2007-251, Laws of Florida, provides that the District may not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless it is specifically authorized by law to do so or it is imperative for the performance of the District's duties and responsibilities as prescribed by law. Additionally, this section requires that as the District collects an individual's SSN, it must provide the individual with a copy of the written statement indicating the purpose for collecting the number. Further, the section provides that SSNs collected by the District may not be used by the District for any purpose other than the purpose provided in the written statement. This section also requires that the District certify to the President of the Senate and the Speaker of the House of Representatives its compliance with these requirements no later than January 31, 2008. Further, by that date, the District was also required to file a report with the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives listing the identity of all commercial entities that have requested SSNs during the preceding calendar year and the specific purposes stated by each commercial entity regarding its need for SSNs. If no disclosure requests were made, the District was required to so indicate.

The District attempted to comply with these requirements, in part, by providing a written statement to new employees when they were hired that indicated, in very general terms, that the District specifically collects SSNs where authorized by law for such purposes and where it is imperative for the performance of the District's duties and responsibilities. However, the District did not provide employees a written statement to specify the specific purpose for collection of SSNs for other documents such as employment applications, extra pay time sheets, Florida Retirement System new employee certification forms, direct deposit authorization forms, and medical history questionnaires, contrary to Section 119.071(5)(a), Florida Statutes.

Further, contrary to the above law, the District did not certify to the Legislature that it complied with Section 119.071(5)(a), Florida Statutes, or report to the Governor and Legislature the identity of all commercial entities that requested SSNs during the preceding calendar year. At the close of our audit fieldwork in August 2008, approximately seven months after the due date, District personnel indicated they were in the process of completing the certification

to the Legislature. Effective controls to properly monitor the need for and use of SSNs and ensure compliance with statutory requirements reduce the risk that SSNs may be used for unauthorized purposes.

Recommendation: The District should continue its efforts to comply with Section 119.071(5)(a), Florida Statutes, and properly monitor its collection and use of social security numbers.

Finding No. 8: Insurance

Enhancements could be made to ensure the adequacy of insurance coverage for charter schools sponsored by the District and design professionals, as discussed below.

Charter School Insurance. During the 2007-08 fiscal year, the District sponsored eight charter schools which were required to provide evidence to the District of certain insurance, such as liability and property coverage. Our review disclosed that liability insurance certificates indicated that the policies could be canceled with prior written notification to the District ranging from 10 to 30 days before the cancellation date, contrary to the charter school agreements which required a 60-day prior cancellation notice. Additionally, the policies for four of the charter schools provided for total aggregate liability coverage of $1 million, which is less than the $2 million required by the charter school agreements. We further noted that District records did not evidence property insurance coverage for seven of the eight charter schools.

Design Professional Insurance. Our review of the liability insurance policies of design professionals for eight construction projects disclosed that each of the professionals carried liability insurance which was on a one-year claims-made basis. A claims-made policy provides coverage only during the period in which a claim is made rather than the period in which the event occurs that gives rise to the claim. Claims-made liability policies may not provide the District with sufficient protection if, for example, a design flaw were discovered subsequent to the construction period and the responsible design professional no longer carries such insurance, carries an insufficient amount of insurance, or is no longer in business. Further, District records did not evidence a cost/benefit analysis of using claims-made insurance rather than other coverage to possibly lower the District's risk of loss due to design flaws.

Similar findings were noted in our report No. 2006-181. Without adequate procedures to monitor the insurance coverage of charter schools and design professionals, there is an increased risk that such coverage may not be adequate, subjecting the District to potential losses.

Recommendation: The District should enhance procedures to ensure that its charter schools maintain insurance as required in the charter school agreements, and that adequate insurance protection is obtained for the design of District construction projects.

Finding No. 9: Time Sheets - Extra Pay Compensation

Instances were noted in which employees did not timely submit their time sheets for work performed beyond their regular assigned duties or certify the work performed on the time sheets. Noninstructional employees who perform assignments beyond their regular assigned duties receive extra pay at their regular pay rate or, for time worked in excess of 40 hours per week, at one and one-half times their regular rate. Instructional employees who perform such work receive part-time pay at rates based on their years of teaching experience. During the 2007-08 fiscal year, the District paid approximately $1,486,000 in extra pay for purposes other than attending workshops.

District administrative procedures provide that time sheets for extra pay should not be accumulated for multiple pay periods but should be properly submitted as soon as the work is completed. However, our review of extra-pay time sheets during the 2007-08 fiscal year disclosed 17 extra-pay time sheets that were not submitted to the payroll department timely. These time sheets included extra pay hours for 76 District employees and resulted in the District's payroll department processing these payments from 44 to 168 days after the services were performed. Of these instances, 12 extra-pay time sheets included time worked in multiple pay periods. We also noted 4 extra-pay time sheets which were not signed by employees to certify the extra time worked. In these circumstances, the District has a greater risk that errors or fraud may occur.

Similar findings were noted in our report Nos. 03-184 and 2006-181.

Recommendation: The District should establish procedures to ensure that employees timely submit extra-pay time sheets and sign the time sheets to certify the time worked.

Finding No. 10: Information Technology - Security Awareness

The District had not implemented a formal ongoing security awareness training program to apprise new employees of, or reemphasize to current employees, the importance of preserving the confidentiality, integrity, and availability of data and IT resources entrusted to them. Included in the data maintained by the District's IT systems are significant nonpublic records (for example, student record information and other records that contain sensitive information). Although the District required employees to sign an annual acknowledgment that they have read and understood the applicable policies, such as the *Guidelines for Acceptable Use of District Information Systems* and copyright laws, the District did not have a formal security awareness 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 response to our inquiry, District management indicated that certain security-related topics are covered, when appropriate, at various IT and school-based personnel meetings. However, implementing a formal security awareness training program would allow for an ongoing, structured approach to promoting security awareness in a uniform manner throughout the District.

The District's failure to implement a formal ongoing security awareness training program increases the risk that the District's IT resources could be intentionally or unintentionally compromised by employees while performing their assigned duties.

Recommendation: To minimize misuse of IT resources, the District should promote security awareness through adequate training programs to ensure that its employees are aware of the importance of information handled and their responsibilities for maintaining its confidentiality, integrity, and availability.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the District had taken corrective actions for findings included in our report No. 2006-181.

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 operational audit 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 operational audit were to: (1) obtain an understanding and make overall judgments as to whether District internal controls promoted and encouraged compliance with applicable laws, rules, regulations, contracts, and grant agreements; the economic and efficient operation of the District; the reliability of records and reports; and the safeguarding of assets; (2) evaluate management's performance in these areas; and (3) determine whether the District had taken corrective actions for findings included in our report No. 2006-181. Also, pursuant to Section 11.45(7)(h), Florida Statutes, our audit may identify statutory and fiscal changes to be recommended to the Legislature.

The scope of this operational audit is described in Exhibit A. Our audit included examinations of various records and transactions (as well as events and conditions) occurring during the 2007-08 fiscal year.

Our audit methodology included obtaining an understanding of the internal controls by interviewing District personnel and, as appropriate, performing a walk-through of relevant internal controls through observation and examination of supporting documentation and records. Additional audit procedures applied to determine that internal controls were working as designed, and to determine the District's compliance with the above-noted audit objectives, are described in Exhibit A. Specific information describing the work conducted to address the audit objectives is also included in the individual findings.

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 operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

Management's response is included as Exhibit B.

THIS PAGE INTENTIONALLY LEFT BLANK.

EXHIBIT A
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Information Technology (IT) policies and procedures.	Inspected the District's written IT policies and procedures to determine whether they address certain important IT control functions.
Program change management procedures.	Reviewed documentation to determine the District's change management methodology for requesting, approving, and implementing application program changes. Tested employee access to application production libraries and datasets to determine if an appropriate separation of duties existed in relation to the change management function.
Procedures for granting access to IT resources.	Reviewed documentation to determine the District's process for requesting, approving, implementing, reviewing, and removing system access to IT resources. Tested employee access to selected functions within different applications to determine if an appropriate separation of duties existed in relation to employees' job functions. Tested selected security software groups and system privileges granted to employees to determine if an appropriate separation of duties existed in relation to employees' job functions.
Procedures for IT authentication controls.	Examined supporting documentation to determine whether authentication controls were configured and enforced in accordance with IT best practices.
Security awareness and training program regarding the confidentiality of information.	Examined supporting documentation relating to the District's information technology security awareness and training program.
Procedures to timely prohibit terminated employees' access to electronic data files.	Tested employees with access privileges who terminated during the audit period, and examined supporting documentation evidencing when the District terminated access privileges.
Procedures for monitoring charter schools pursuant to Section 1002.33(5)(b), Florida Statutes..	Interviewed District personnel and examined supporting documentation to determine if the District effectively monitored selected operations and performance measures of its charter schools, including evidence of required insurance.
Fraud policy and related procedures.	Examined written policies and procedures, and examined supporting documentation relating to the District's fraud policy and related procedures.
Sunshine Law requirements for Board meetings (i.e., proper notice of meetings, ready access to public, maintain minutes).	Read Board minutes and, for selected Board meetings, examined supporting documentation evidencing compliance with Sunshine Law requirements.
Financial condition.	Applied analytical procedures to determine whether General Fund unreserved fund balance at June 30, 2008, was less than 2.5 percent of General Fund revenues.
Restrictions on use of nonvoted capital outlay tax proceeds.	Applied analytical procedures, tested payments made from nonvoted capital outlay proceeds and examined supporting documentation to determine whether the District complied with requirements related to the use of nonvoted capital outlay proceeds.

EXHIBIT A (Continued)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Restrictions on use of Workforce Development funds.	Applied analytical procedures to determine whether the District used funds for authorized purposes (i.e., not used to support K-12 programs or District K-12 administrative costs).
Adult general education program enrollment reporting.	Selected a sample of adult education students and examined supporting documentation to determine whether the District reported instructional and contact hours in accordance with FDOE requirements.
Social security number requirements of Section 119.071(5)(a), Florida Statutes.	Examined supporting documentation to determine whether the District had provided individuals with a written statement as to the purpose of collecting social security numbers, certified compliance pursuant to Section 119.071(5)(a)4.b., Florida Statutes, and filed the required report specified by Section 119.071(5)(a)9.a., Florida Statutes, no later than January 31, 2008.
School advisory council requirements.	Examined supporting documentation to determine whether the District had established an advisory council for each school and complied with Section 1001.452, Florida Statutes.
Procedures for issuing diplomas.	Selected a sample of diploma recipients and examined supporting documentation evidencing that the recipients were eligible to graduate.
Procedures to ensure timely performance of bank reconciliations.	Reviewed bank reconciliations and other supporting documentation to determine whether the District timely performed bank reconciliations.
Procedures to timely mark and number newly acquired tangible personal property.	Examined records detailing tangible personal property acquisitions to determine whether the District timely marked and numbered them.
Cash collection procedures at District-operated after school programs.	Reviewed collection procedures at selected locations and tested daily cash collections to determine the effectiveness of the District's collection procedures.
Requirements for fingerprinting and background checks for personnel that had direct contact with students.	Reviewed District and contractual personnel who had direct contact with students and examined supporting documentation to determine whether the District had obtained required fingerprint and background checks for the individuals reviewed.
Performance based pay plan requirements for instructional personnel.	Reviewed pay plan documentation and performance records of instructional personnel who received performance pay increases to determine whether the District complied with performance based pay plan requirements.
Procedures for monitoring of employee extra-pay claims.	Reviewed extra-pay claim procedures and tested extra-pay claims to determine effectiveness of the District's monitoring of employee extra-pay claims.
Five-year facilities work plan.	Reviewed the current five-year facilities work plan and determined whether the District maintained records that supported the amounts reported on the plan.

EXHIBIT A (Continued)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Amount and type of liability insurance carried by design professionals.	Tested major construction projects in progress during the audit period to determine the type and amount of liability insurance carried by the architects and engineers.
Procedures for monitoring cellular telephone usage and compliance with related IRS reporting requirements.	Determined whether the District either provided for compliance with IRS substantiation requirements for cellular telephone usage or, for the most recent calendar year, reported the value of cellular telephone services provided to employees as income for those employees.
Procedures for timely ensuring that expense claims were processed before grant deadlines.	Identified grants that refunded money to grantors and examined supporting documentation to determine reasons for the refunds and whether the requests for refunds had been made timely.
Procedures to ensure that deficiencies noted in annually required safety inspections were timely resolved.	Reviewed a sample of safety inspection reports and examined supporting documentation to determine current status of any deficiencies identified in the reports and whether the District timely resolved such deficiencies.

THIS PAGE INTENTIONALLY LEFT BLANK.

EXHIBIT B
MANAGEMENT'S RESPONSE

THE SCHOOL DISTRICT OF ESCAMBIA COUNTY

215 WEST GARDEN STREET
PENSACOLA, FL 32502
PHONE 850/432-6121, FAX 850/469-6379
http://www.escambia.k12.fl.us
JIM PAUL, SUPERINTENDENT

October 15, 2008

Mr. David W. Martin, CPA
Auditor General
7282 Plantation Road, Suite 401
Pensacola, FL 32504

Re: Preliminary and Tentative Audit Findings and Recommendations of the Operational Audit of the Escambia County District School Board for the Fiscal Year Ended June 30, 2008

Dear Mr. Martin:

Enclosed is our response to the preliminary and tentative audit findings of the operational audit for the fiscal year ended June 30, 2008.

We appreciate the opportunity to respond to the findings. After reviewing the response, please advise me if you require any further clarification or action on our part.

In the meantime, we shall look forward to receiving the final audit when it becomes available.

Sincerely,

Jim Paul
Superintendent

JP:BSL:dlh

c: Board Members

Affirmative Action/Equal Opportunity Employer

EXHIBIT B (Continued)
MANAGEMENT'S RESPONSE

Escambia County School District
Preliminary and Tentative Audit Findings & Recommendations
Fiscal Year Ended June 30, 2008

Finding No. 1: Information Technology – Access Controls

The District's management of information technology (IT) access privileges needed improvement.

The IT department fully recognizes the necessity of an annual review of user access privileges and consistent compliance with established procedures for review of daily activity reports in the human resource and finance systems. The IT, human resource, and finance departments will take immediate collaborative steps to develop Standard Operating Procedures (SOPs) that will ensure employees' access privileges are compatible with job responsibilities and that evidence of unauthorized or erroneous transactions is retained and examined. In fact IT, human resource, and finance personnel already consistently observe a set of institutionalized procedures for assigning employee access privileges and dissemination of daily activity reports. These institutionalized procedures rely on role-based assignment of employee access privileges and hard copy distribution of activity reports. These procedures have proven to be effective for Escambia, although they are not as formally codified or as frequently reviewed as prescribed by industry standard governance guidelines contained in the Information Technology Infrastructure Library (ITIL) and the Control Objectives for Information and Related Technology (COBIT). This effectiveness is in large part due to the numerous opportunities for supervisory and peer oversight among the relatively small group of administrative and professional staff assigned to IT, human resource, and finance duties. These oversight opportunities are facilitated by: the redundant skills, cross training, and work ethic that exists among these employees; the close physical proximity of their workstations and work locations; and the comprehensiveness of the supervisory responsibilities and diligence of the subject department directors. These institutionalized practices and work site circumstances will serve as the starting point for initial discussion and subsequent development of the above-mentioned SOPs to address access control and activity report review procedures in a manner that is consistent with audit recommendations and with ITIL and COBIT governance.

Finding No. 2: Information Technology – Terminated Employee Access

Enhancements could be made to timely terminate the IT access privileges of former employees.

The IT department fully recognizes the necessity of enhancing the current District procedures for timely deletion of exiting employees' access privileges in order to minimize the risk of misappropriation or abuse of District assets. Current institutionalized procedures observed by district employees rely on the monthly School Board agenda listing retirees, terminations, and resignations to initiate a timely deletion of employee access privileges to District systems. A backup to the School Board agenda procedure utilizes an automated deletion of employee access rights when and if 30 days elapses without the occurrence of an employee login to any District system. Although these institutionalized procedures have been effective in preventing misappropriation and abuse to this point, they are not compliant with industry standard governance guidelines contained in ITIL and COBIT. IT and other germane district departments will use the above described procedures as a starting point for initial discussion and subsequent development of SOPs addressing timely deletion of exiting employees' access privileges that are compliant with audit recommendations and with ITIL and COBIT governance.

EXHIBIT B (Continued)
MANAGEMENT'S RESPONSE

Escambia County School District
Preliminary and Tentative Audit Findings & Recommendations
Fiscal Year Ended June 30, 2008

Finding No. 3: Information Technology –Program Change Controls

The District's IT program change controls needed improvement.

The IT department fully recognizes the importance of the development and maintenance of written policies and procedures to govern the program change control process including: consistent documentation regarding who changed, tested, approved, and moved programs to production; appropriate separation of duties regarding testing and movement of programs to production; provision of an environment for testing of program changes to the finance application; and restriction of programmers from end-user access privileges. Change control is currently being addressed through email and email archiving of change requests and change verification among germane IT, human resource, and finance department personnel. To this point that process has been effective due in large part to an institutionalized understanding among IT, human resource, and finance employees that this email exchange is necessary to reduce the risk of corruption of production program libraries and the subsequent loss of productivity involved in restoration of previous program versions or re-entry of lost information. As in the case of the timely termination of employee access privileges, opportunities for supervisory and peer oversight regarding program change control is further facilitated by: the redundant skills, cross training, and work ethic that exists among these employees; the close physical proximity of their workstations and work locations; and the comprehensiveness of the supervisory responsibilities and diligence of the subject department directors. These institutionalized practices and work site circumstances will serve as the starting point for initial discussion and subsequent development and maintenance of written policies and procedures to govern the program change control process in a manner that is consistent with audit recommendations and with ITIL and COBIT governance.

Finding No. 4: Information Technology – Security Controls

The District's security controls within the application and supporting IT environment needed improvement.

The District is working on procedures to improve security controls within the application and supporting IT environment.

Finding No. 5: Background Screening and Fingerprinting Requirements

Improvements could be made in District procedures for timely obtaining background screenings and fingerprints for District and contractual personnel that have direct contact with students.

The District has made significant progress in the re-fingerprinting of current employees since the last operational audit was conducted. Currently, we have fingerprinted 3,120 employees which represents 52% of our personnel. Our projections show that we anticipate re-fingerprinting the remaining 2,880 employees during the 2008-09 school year in order to achieve the state mandate.

We recognize that we are behind according to the state benchmark of 80% but we are closing the gap. While the District started out slow in implementing the re-fingerprint program, our progress year-to-date has been significant. We fully intend to complete this program by the deadline requirement of June 30, 2009.

EXHIBIT B (Continued)
MANAGEMENT'S RESPONSE

Escambia County School District
Preliminary and Tentative Audit Findings & Recommendations
Fiscal Year Ended June 30, 2008

Contractors

Since October of 2005, the District has conducted background checks on over 7,000 individuals. These individuals include vendors, contractors, mentors, student teachers, etc. These applicants represent approximately 50 volunteer/mentor agencies and hundreds of contractors and vendors. Of those 7,000 applicants, approximately 9% have been denied access to District campuses due to disqualifying offenses included in their criminal history. Based on anecdotal information from numerous applicants, it would seem that this District is more stringent than most others when implementing and enforcing the Lunsford Act.

The Protection Services Division has provided ongoing communication regarding the credentialing requirements and process to both District staff and those agencies and businesses doing business with the District. Training specific to the requirements of the Lunsford Act has been provided multiple times to school administrators. In addition, Protection Services staff utilizes every opportunity available to continue to educate and clarify these requirements with agencies and businesses with which they have contact.

Following are responses to the three specific examples noted in the audit report:

- *Security Company* (Securitas) – These three individuals are licensed by the state of Florida and undergo a rigorous background check similar to, if not more than, that required by the Lunsford Act. We are currently working with Securitas to ensure we obtain the proper documentation regarding the background checks conducted by this contractor so that it will be on file with the District.
- *Nursing Services* – There was one individual providing this service who had not had a background check conducted. As stated in the report, the department utilizing this individual assumed that she did not require a background check due to the fact she was licensed as a nurse with the state. This discrepancy was resolved when bought to the attention of Protection Services staff and the individual has had a background check completed and a security credential has been issued.
- *Mentoring Service* – There has been some misinterpretation on the part of curriculum and instruction staff in regard to how the Lunsford Act applies to individuals providing mentoring services to students. At this point, it appears that those misconceptions have been cleared up and that all mentors providing such services to the District have been, or are in the process of, being cleared.

The audit report also contains a recommendation that the District "*should ensure that it timely obtains the required background screenings for its employees and contractors*".

As stated above, the District has conducted background checks on several thousand individuals providing services to the students and staff of this community. It should be pointed out that while this District is aggressive and deliberate in its attempt to fully comply with the Lunsford Act, it does face challenges in doing so.

However, it is also important to recognize that both school and District staff have a responsibility to ensure that everyone on our campuses has the proper security credentials. These staff members must accept their responsibility as the first line of defense in ensuring our students are safe and secure. To that end, the District must continue to communicate this responsibility and hold appropriate individuals accountable for accomplishing this important task.

EXHIBIT B (Continued)
MANAGEMENT'S RESPONSE

Escambia County School District
Preliminary and Tentative Audit Findings & Recommendations
Fiscal Year Ended June 30, 2008

Finding No. 6: Child Care Program Collection Procedures

Internal controls over child care fee collections could be strengthened.

To further strengthen internal controls over child care fee collections the following will be implemented. The School Age Child Care (SACC) Coordinator will receive monthly Account Snapshots from secretaries/bookkeepers. The attendance documentation form will be revised to include a formula that will calculate monies owed so this information will be located in one form—this will provide additional documentation that can be validated against other forms of documentation such as receipt books. A test will be implemented which involves selecting a random sampling of students, and tracking the monies collected from the receipt book, to the monies collected form, to the Account Snapshot, to the amount remitted to the district revenue department. These tests will be documented by the SACC Coordinator.

Safes that are bolted to the floor have been installed at Bellview and Ensley Elementary Schools specifically to ensure that monies collected are sorted in a secure location. The SACC Coordinator has reviewed the policy on properly securing monies collected with all the SACC Directors.

Finding No. 7: Collection of Social Security Numbers

The District did not provide employees a written statement to specify the purpose for collection of social security numbers (SSNs) for certain documents or timely certify compliance with the new SSN requirements to the Legislature, contrary to Section 119.071(5)(a), Florida Statutes (2007).

The District established procedures in anticipation of complying with Section 119.071(5)(a), Florida Statutes. All prospective and current employees were provided with a general statement concerning the collection of Social Security Numbers.

The statement reads:

> The Escambia County School District, in compliance with Florida Statutes, is required to inform individuals the purpose for collection of Social Security Numbers. The District specifically collects Social Security Numbers where it is authorized by law for such purpose and where it is imperative for the performance of the District's duties and responsibilities.

The District is working to develop a more specific statement to inform prospective and current employees as to the reason for the collection of the Social Security Number. This statement, once developed, will be provided to individuals via the website, online application, and personally when the full Social Security Number is required.

Where it is possible, the District has limited the collection of Social Security Numbers to the last 4 digits of the Social Security Number as the identifier. The Escambia County School District is taking a proactive approach in establishing a separate employee identification number for active employees from that of a Social Security Number.

The findings are correct concerning the report that must be submitted to the Governor and Legislature identifying all commercial entities that requested Social Security Numbers during the preceding calendar year. The District has prepared the proper correspondence for reporting in the future.

EXHIBIT B (Continued)
MANAGEMENT'S RESPONSE

Escambia County School District
Preliminary and Tentative Audit Findings & Recommendations
Fiscal Year Ended June 30, 2008

Finding No. 8: Insurance

Enhancements could be made to ensure the adequacy of insurance coverage for charter schools sponsored by the District and design professionals.

The Risk Management Department has been working with the Department of Alternative Education to bring all Charter School insurance in compliance with their contract. Risk Management has conducted insurance training with Alternative Education in order to assist in facilitating full compliance with contract language and drafted a letter that was sent to all Charter School Programs that identified deficiencies and requested verification of full compliance with contract provisions.

The requirement for Professional Insurance was added by Board policy due in part to comments provided in report No. 2006-181. No claims have been filed against any design professionals during the time that the insurance requirement has been in place. The Director of Risk Management and the Director of Facilities Planning will discuss the advantages and disadvantages of each type of policy. We will then make a determination of the type of coverage that will be most advantageous from a liability standpoint. Once a determination is made, we will be able to add language that addresses the specific period of coverage for the design professionals coverage.

Finding No. 9: Time Sheets - Extra Pay Compensation

Instances were noted in which employees did not timely submit their time sheets for work performed beyond their regular assigned duties or certify the work performed on the time sheets.

The importance of timely submittal of work performed beyond regular assigned duties will be re-emphasized through a memorandum regarding proper procedures. In addition, departments and schools will be contacted via email when time sheets are received for extra pay that has not been submitted promptly. Time sheets will be more closely monitored to ensure that all extra pay time sheets are signed by employees to certify the extra time worked.

Finding No. 10: Information Technology - Security Awareness

The District had not implemented a formal ongoing security awareness-training program to protect information technology resources.

The IT department fully recognizes the necessity of implementing appropriate security awareness training programs to ensure that employees are aware of the importance of the data they handle and their responsibilities for maintaining the confidentiality, integrity, and availability of that data. District departments already consistently observe a range of institutionalized procedures that are intended to address security-training issues. The Guidelines for Acceptable Use of District Information Systems document contains District guidelines for accessing and using various data types. All employees must sign that document each year and by doing so acknowledge their awareness and agreement with its contents. The employee's signature is also explained as a condition of continued employment with the District. There are also several forums in which IT employees and school based employees are intermittently advised of the importance of

EXHIBIT B (Continued)
MANAGEMENT'S RESPONSE

Escambia County School District
Preliminary and Tentative Audit Findings & Recommendations
Fiscal Year Ended June 30, 2008

adherence to security policies and security-related responsibilities, briefed on security-related policies and procedures, and/or trained in procedures to fulfill their security responsibilities. These IT and school-based personnel meetings include School Data Clerk Meetings, School Technology Coordinator meetings, District Network Services personnel meetings, District Technology Support personnel meetings, IT Area Meetings, and District Technology Advisory Committee meetings (not a comprehensive list). Although this approach to security-awareness training has been effective, it is not as formally codified or as frequently reviewed as prescribed by industry standard governance guidelines contained in ITIL and COBIT. This approach to security awareness training will serve as the starting point for initial discussion and subsequent development and maintenance of written policies and procedures to ensure that employees are aware of the importance of the data they handle and their responsibilities for maintaining the confidentiality, integrity, and availability of that data. These policies and procedures will be written in a manner that is consistent with audit recommendations and with ITIL and COBIT governance.