

**SEMINOLE COUNTY
DISTRICT SCHOOL BOARD**

Operational Audit

For the Fiscal Year Ended
June 30, 2008



BOARD MEMBERS AND SUPERINTENDENT

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

	<i><u>District No.</u></i>
<i>Diane Bauer, Chairman from 11-20-07, Vice-Chairman to 11-19-07</i>	<i>1</i>
<i>Sandra Robinson</i>	<i>2</i>
<i>Dede Schaffner, Vice-Chairman from 11-20-07</i>	<i>3</i>
<i>Barry Gainer, Chairman to 11-19-07</i>	<i>4</i>
<i>Jeanne Morris</i>	<i>5</i>

Bill Vogel, Ed. D., Superintendent

The audit team leader was Tina Z. Myers and the audit was supervised by Keith A. Wolfe, CPA. For the information technology portion of this audit, the audit team leader was Heidi Burns, CPA, CISA, and the supervisor was Nancy Reeder, CPA, CISA. Please address inquiries regarding this report to Gregory L. Centers, CPA, Audit Manager, by 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.

SEMINOLE COUNTY

District School Board

SUMMARY

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

Finding No. 1: The District granted excessive or unnecessary access privileges within PeopleSoft and the supporting information technology (IT) environment.

Finding No. 2: The District did not timely conduct a review and evaluation of the collection of social security numbers or provide a written statement to individuals stating the purpose for collection of the numbers, contrary to Section 119.071(5)(a), Florida Statutes.

Finding No. 3: The District used ad valorem tax proceeds, totaling \$74,053, for nonauthorized purposes such as the purchase of band uniforms and software licenses. Subsequent to our inquiry, the District appropriately reimbursed these expenditures from other moneys.

Finding No. 4: The District lacked written policies and procedures for certain IT security and configuration management functions.

Finding No. 5: The District's security controls related to user account management, logging, and user authentication needed improvement.

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 Seminole County. The governing body of the Seminole County District School Board is composed of five elected members. The appointed Superintendent of Schools is the executive officer of the School Board.

During the audit period, the District operated 61 elementary, middle, high, and specialized schools; sponsored 3 charter schools; and reported 65,017 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 Privileges

Access controls are intended to protect data and IT resources from unauthorized disclosure, modification, or loss. A clear division of roles and responsibilities between IT development staff and functional end users and within the established overall IT function is a key element of internal control to preclude the possibility of a single individual subverting a critical process. For example, the functions of application end user, application development and maintenance, and technical (systems software) support are typically separated. Additionally, as resources permit, it is generally advisable to limit technical support access privileges to the software products for which they are responsible.

Certain individuals had been granted access capabilities that were greater than what was needed for the performance of their job duties. In response to audit inquiry, District management indicated that certain user access privileges had

been removed or modified. Nevertheless, instances of excessive access privileges remained unaddressed by the District. Specifically:

- The Database Administrators (DBAs), a System and Business Analyst, and a PeopleSoft contractor were allowed Financial Management (Finance) and Human Resources Management (HR) application rights through the ALLPNLS and ALLPANLS, respectively, permission lists assigned to them. These permission lists grant powerful security authorizations by providing superuser level access to most functional and technical related menus and pages within PeopleSoft. In addition, these individuals, along with two additional PeopleSoft contractors, had access to pages that allowed for the creation of payments, journal suspense corrections, marking journals for unposting, and approval of vouchers via additional permission lists assigned.
- Access to correction mode was granted to most Finance and HR users in the performance of their job duties. Correction mode, which is intended to be granted under limited and monitored circumstances, allows the alteration, insertion, or deletion of data rows without logging the changes. Consequently, data integrity and management reporting from the system may be adversely affected through the unauthorized or erroneous use of correction mode access.
- Access privileges to perform role and user security maintenance was granted to individuals other than those defined as having security administrator responsibilities or other responsibilities requiring the access. Specifically, Information Services department (IS) employees, including the Project Manager, a Developer, the DBAs, and two Analysts had security administrator rights for Finance. The IS Project Manager, PeopleSoft contractor, Operations Supervisor, and an Analyst, along with various Human Resources department employees had security administrator rights for HR assigned through the MAINTAIN_SECURITY menu and, for some of the employees, through the ADMIN permission list. In response to audit inquiry, District management indicated that they have now reviewed and modified access rights in Finance for the IS Project Manager and Developer but that access was necessary for one of the Analysts based on responsibilities for creating high-level queries. District management also stated that, in HR, access has now been modified for the IS Project Manager, Operations Supervisor, Deputy Superintendent, and Executive Director but that access was necessary for the Personnel/Lead Payroll Specialist and the Human Resources Administrator based on responsibilities during payroll processing.
- PeopleSoft Finance and HR application access capabilities, established through the use of permission lists, did not in some instances correspond to what was documented by the District.
- The District's primary DBA had superuser level privileges within the PeopleSoft application in addition to the superuser accounts assigned as a system administrator for the operating system component of PeopleSoft and as the DBA. Effective access controls typically separate the functions of accessing data through an application, system administration, and database administration. Additionally, certain IS employees had been granted user accounts on the operating system supporting the PeopleSoft database outside of their assigned responsibilities. In response to audit inquiry, District management indicated that these operating system accounts have now been removed.

Inadequate separation of duties may result in improper system changes, erroneous transactions processed, or damage to data and IT resources. The above-listed instances of excessive access privileges significantly increased the risk of individuals performing unauthorized system activities without timely detection.

Recommendation: The District should continue to critically evaluate employee access privileges to ensure that privileges enforce a separation of end-user functions and technical staff functions and to determine whether superuser level access can be redefined so that capabilities are restricted to only those necessary to perform assigned functions. In addition, the District should review user permissions specific to correction mode to further restrict its use to limited and monitored circumstances. Further, management should critically evaluate and define the responsibilities of the DBA with regard to the application and supporting operating system and database platforms and ensure that access privileges do not exceed what is necessary to perform DBA duties.

Finding No. 2: 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 District has stated in writing the purpose for its collection and unless it is specifically authorized by law to do so or 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, this 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 review whether its collection of SSNs is in compliance with the above requirements; immediately discontinue the collection of SSNs for purposes that are not in compliance; and 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 this date, the District was 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.

District personnel indicated that SSNs are obtained for various purposes such as for employee insurance, withholding taxes, background checks, and citizenship verification. District personnel further stated that, as of March 18, 2008, the District had initiated efforts to comply with the requirements above by reviewing the reasons to obtain SSNs, discontinuing unnecessary collection of such numbers, and addressing these procedures in the employee handbook, student code of conduct and volunteer manuals. However, the District had not adopted a written statement stating the purpose for the collection of SSNs, and had not filed the required reports and certifications with the Governor and Legislature by January 31, 2008. Subsequently, the Board adopted a policy which identified various purposes for collecting the SSNs at the August 2008 Board meeting. 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 119.71(5), Florida Statutes, and properly monitor its collection and use of social security numbers.

Finding No. 3: Ad Valorem Taxation

The District was authorized, pursuant to Section 1011.71(2), Florida Statutes, to levy ad valorem taxes for capital outlay purposes within specified millage rates. Additionally, Section 1011.71(2), Florida Statutes, provides that revenue generated by the capital outlay millage levy should be used for only certain purposes such as the costs of new construction and remodeling projects; maintenance, renovation, and repair of existing school plants; the purchase of school buses and the purchase of new and replacement equipment.

Pursuant to Section 1011.71(2), Florida Statutes, the District levied the ad valorem taxes for capital outlay purposes, budgeted the capital outlay taxes for specific projects, and accounted for the tax levy in its Local Capital Improvement Fund (LCIF). LCIF expenditures totaled approximately \$37.7 million for the 2007-08 fiscal year. Our review of 25 LCIF expenditures, totaling approximately \$7.7 million, disclosed three expenditures, totaling \$74,053 for purposes not specifically included in law as allowable uses of the capital outlay millage levy proceeds. These expenditures were for software licenses used in foreign language classes and for band uniforms and headsets. Subsequent to our inquiry, the District appropriately reimbursed the LCIF from other resources for these questioned costs, totaling \$74,053.

Recommendation: The District should continue its efforts to ensure that proceeds generated from ad valorem tax proceeds are used for authorized purposes.

Follow-Up to Management Response:

Management indicates in their response that band uniforms and headsets would fall under the definition of equipment because they have a useful life greater than one year, and therefore would be an acceptable use of capital outlay tax proceeds. While assets may have lives of more than one year, the allowability of expenditures from capital outlay tax proceeds is not based on an asset's life, but on the provisions of Section 1011.71, Florida Statutes. Additionally, management indicates the Auditor General did not take exception with the District classifying these purchases as equipment. However, when we brought this issue to management's attention in April 2008, the District corrected the classification by reimbursing the LCIF, and charging the expenditures to noncapitalized equipment in the General Fund.

Management further indicates that the General Counsel of the Florida Department of Education (FDOE) issued an opinion stating that software purchases were an allowable expenditure of capital outlay millage proceeds. However, that opinion is directed at the allowability of incurring one-year obligations by a school district, and not the propriety of using capital outlay millage proceeds to purchase computer software. Further, in October 2008, FDOE responded to another school district regarding its purchase of computer software noting that "the issue is not the accounting treatment of the funds used to purchase the software; but rather it is the legal issue that the expenditure of capital improvement funds for computer software is not authorized in Section 1011.71, Florida Statutes." Therefore, our position remains that proceeds generated from ad valorem tax proceeds should only be used for those purposes specifically outlined in Section 1011.71, Florida Statutes. To obtain further clarity on this subject, the District may consider consultation with the Florida Department of Education.

Finding No. 4: Information Technology – Written Policies and Procedures

Each IT function needs complete, well-documented policies and procedures to describe the scope of the function and its activities. Sound policies and procedures provide benchmarks against which compliance can be measured and contribute to an effective control environment.

Our audit disclosed that, although informal procedures existed and were executed in the daily course of the Information Services Department's support of PeopleSoft, the District lacked written policies and procedures for the following IT security and configuration management functions:

- Administration of vendor-supplied user identification codes (IDs).
- Specification of the level of access required by those service and application "user" accounts that enable system processes or system configuration modification.
- Definition of user roles and permissions in accordance with assigned responsibilities.
- Periodic review of users' access privileges for appropriateness.
- Responsibilities for network administration.

- Responsibilities for system administration.
- Responsibilities for database administration.
- Responsibilities for security administration.
- Application programs and system software change management procedures.
- Maintenance of workstation administration rights by end users.

Without written policies and procedures, the risk is increased that IT security and configuration management controls may not be followed consistently and in a manner pursuant to management's expectations.

Recommendation: The District should establish written policies and procedures to document management's expectations for the performance of the above-listed IT security and configuration management functions.

Finding No. 5: Information Technology – Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain District security controls in the areas of user account management, logging, and user authentication that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising District data and IT resources. However, we have notified appropriate District staff 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 improve security controls in the areas of user account management, logging, and user authentication to ensure the continued confidentiality, integrity, and availability of District data and IT resources.

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions related to the findings included in our report No. 2006-174.

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. 2006-174. 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
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.
Fraud policy and related procedures.	Examined written policies and procedures, and examined supporting documentation relating to the District's fraud policy and related procedures.
Strategic plan.	Reviewed supporting documentation to determine whether the District's strategic plan contained essential elements, such as long and short term goals.
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.
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.
Results of school internal account audits.	Reviewed school internal account audit reports to determine whether recurring control deficiency or noncompliance issues were noted which may effect school operations.
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.
Security Administrator duties.	Interviewed Security Administrator and observed selected functions to determine whether the District established specific duties and responsibilities for the position.
Disaster recovery plan.	Reviewed plan to determine whether it contained step-by-step procedures for recovery, and provided for periodic testing.
Information systems user ID and passwords.	Reviewed adequacy of policies and procedures on use and safeguarding of user IDs and passwords.
Procedures for adopting and amending the budget.	Examined supporting documentation to determine whether budgets and amendments to budgets were prepared and adopted in accordance with applicable Florida Statutes, and State Board of Education Rules.
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.

**EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY**

Scope (Topic)	Methodology
Stale-dated checks (abandoned property).	Interviewed personnel and reviewed records to determine whether stale-dated checks were timely identified, reported and remitted to the State, pursuant to Section 17.26, Florida Statutes.
Investment practices.	Reviewed authorized investments listed in the certificate of participation (COP) agreements, and District records to determine whether investments were proper.
Restrictions on use of nonvoted capital outlay tax proceeds.	Selected a sample of 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.
Capital construction projects.	Selected a sample of construction projects to determine whether separate project ledgers were properly maintained to account for costs of the respective projects. Also, examined supporting documentation for one completed project to determine whether expenditures were consistent with contract terms.
Amount and type of liability insurance carried by architects.	Tested major construction projects in progress during the audit period to determine the type and amount of liability insurance carried by architects.
Procedures for timely ensuring 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.
Tangible personal property annual inventory procedures.	Examined supporting documentation to determine whether the District timely conducted a physical inventory of tangible personal property.
Facility safety procedures.	Examined documentation to determine whether floor plans were timely provided to local law enforcement agencies and fire departments, as required by Section 1013.13, Florida Statutes.
Fee revenues for after school programs.	Examined supporting documentation to determine whether fee audits, comparing enrollment records with fee collections, were properly conducted for after school programs.
E-rate program.	Interviewed personnel and reviewed records to determine whether the District timely applied for and received moneys due from the E-rate program.
Food service operations.	Interviewed personnel and reviewed records to determine whether the District considered the cost/benefit of food service operations at the Educational Services Center administrative facility.
Operating fund transfers.	Examined supporting documentation to determine whether moneys transferred from one fund to another were properly used.

**EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY**

Scope (Topic)	Methodology
Employee timesheets.	Examined supporting documentation to determine whether time records were properly reviewed and approved by supervisory personnel.
Employee terminal leave pay.	Selected a sample of terminal leave payments to determine whether amounts paid were consistent with District policies and Florida Statutes.
Procedures and policies for overtime pay.	Selected a sample of overtime payments to determine whether amounts paid were properly supported and allowable pursuant to District policies.
Self-insurance programs.	Reviewed accounting records of the worker’s compensation and prescription drug programs to determine whether the District adequately funded these programs.
Procedures relating to purchasing cards.	Reviewed a sample of purchase card expenditures to determine the effectiveness of the District’s purchasing card procedures and reviewed controls over the issuance and cancellation of card privileges.
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.
Requirements for fingerprinting and background checks for personnel that had direct contact with students.	Selected a sample of 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 included in our sample.
Procedures for control over diplomas.	Interviewed school personnel to determine the adequacy of procedures to order and safeguard diplomas.
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.
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 and contractor access to selected functions within PeopleSoft to determine if an appropriate separation of duties existed. Tested selected network, operating system, and database management system accounts for proper security, administration, and assignment of these accounts in support of the PeopleSoft applications.

**EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY**

Scope (Topic)	Methodology
Procedures for IT authentication controls.	Examined supporting documentation to determine whether authentication controls were configured and enforced in accordance with IT best practices.
Procedures for logging.	Reviewed supporting documentation to determine the adequacy and appropriateness of the District's implemented logging policies for PeopleSoft and its supporting environment.

THIS PAGE INTENTIONALLY LEFT BLANK.

**EXHIBIT B
MANAGEMENT'S RESPONSE**



SEMINOLE COUNTY
PUBLIC SCHOOLS

BILL VOGEL, Ed.D.
Superintendent

Educational Support Center
400 E. Lake Mary Boulevard
Sanford, Florida 32773-7127

November 7, 2008

David W. Martin, CPA
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Monroe Street
Tallahassee, FL 32399-1450

Included below is my response to your list of preliminary and tentative audit findings for the operating audit of the Seminole County School Board for the fiscal year ended June 30, 2008.

Finding No. 1: Information Technology – Access Privileges

- (permission lists) The district is taking this recommendation under advisement, and will review the permission lists and make changes as appropriate.
- (access to correction mode) The district believes the appropriate access authority is in place. A review will be conducted regarding individuals and their access, and changes deemed necessary will be made.
- (access privileges) The district is taking this under advisement and will review the appropriate roles to be assigned to users in question.
- (access vs documentation) The district is taking this recommendation under advisement and will review the personnel lists and documentation. Changes will be implemented as deemed necessary.
- (access controls) The district acknowledges this finding but does not have sufficient resources to separate duties as recommended.

Finding No. 2: Collection of Social Security Numbers

The district takes this responsibility seriously, to monitor the collection of sensitive information. We will continue to police the forms and processes to ensure collection is only when required. The district will continue efforts to comply with the statutes.

Finding No. 3: Ad Valorem Taxation

As noted in the finding by the Auditor General, the District has reimbursed the Local Capital Improvement Fund (LCIF) for the items in dispute. However, we are not in agreement with this finding. The Auditor General's finding involves two separate issues. The first issue involves band uniforms (including head dresses). The second issue involves the purchase of software licenses used in a foreign language class.

Regarding the first issue, the band uniforms are considered by general accepted accounting principles to be capital assets, because the life of the noted items exceeds more than a single period. *Governmental Accounting Standard Board, Statement 34, Paragraph 19* defines capital assets as the following:

“As used in this Statement, the term capital assets include land, improvements to land, easements, buildings, building improvements, vehicles, machinery, equipment, works of art and historical treasures, infrastructure, and all other tangible or intangible assets that are used in operations and that have initial useful lives extending beyond a single reporting period....”

Visit Our Web Site
www.scps.k12.fl.us

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Page 2 of 2
November 7, 2008
Preliminary and Tentative Audit Findings for Seminole County District School Board

Under the definition listed above, the band uniforms would fall under equipment, since their useful life extends beyond a single reporting period. This is supported in the Red Book issued by the Florida Department of Education and by the fact that the Auditor General staff did not object when the above noted reimbursements of the band uniforms were charged to equipment in the General (Operating) Fund.

Under Section 1011.71(2), of the Florida Statutes, "... each school board may levy not more than 1.75 mills against the taxable value for school purposes for district schools ...". The purchase, lease-purchase, or lease of new and replacement equipment is authorized by Section 1011.71(2)(d). Since the band uniforms are considered to be equipment and are school related, they are authorized under Section 1011.71(2), Florida Statutes.

Regarding the second issue, software is not specifically addressed in Section 1011.71(2), Florida Statutes. The software purchase was based on an opinion issued by our counsel that was later confirmed by an opinion issued by the General Counsel for Florida Department of Education. These opinions stated that software although not specifically addressed are allowable under Section 1011.71(2)(d), Florida Statutes.

Finding No 4: Information Technology – Written Policies and Procedures

The district is taking this recommendation under advisement and will implement policies and write procedures as needed.

Finding No 5: Information Technology – Security Controls

The district is taking these recommendations under advisement and will take corrective action as appropriate.

Sincerely,



Bill Vogel, Ed.D.
Superintendent