



Florida Union Free School District Internal Controls Over Selected Financial Activities

Report of Examination

Period Covered:

July 1, 2006 — March 31, 2008

2008M-170



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	2
EXECUTIVE SUMMARY	3
INTRODUCTION	5
Background	5
Objective	5
Scope and Methodology	5
Comments of District Officials and Corrective Action	6
PURCHASING	7
Recommendations	10
TAX RECEIPTS	11
Recommendation	12
INFORMATION TECHNOLOGY	13
Business Continuity	13
User Access Controls	16
Recommendations	17
APPENDIX A Response From District Officials	19
APPENDIX B OSC Comments on the District's Response	21
APPENDIX C Audit Methodology and Standards	22
APPENDIX D How to Obtain Additional Copies of the Report	25
APPENDIX E Local Regional Office Listing	26

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

November 2008

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Florida Union Free School District, entitled Internal Controls Over Selected Financial Activities. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller
Division of Local Government
and School Accountability*



State of New York Office of the State Comptroller

EXECUTIVE SUMMARY

The Florida Union Free School District (District) is governed by the Board of Education (Board) which comprises five elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are two schools in operation within the District, with approximately 850 students and 150 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$15 million, which were funded primarily with State aid and real property taxes.

Scope and Objective

The objective of our audit was to evaluate internal controls over selected financial activities for the period July 1, 2006 through March 31, 2008. Our audit addressed the following related questions:

- Are internal controls over purchasing appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over tax collection adequate to ensure timely deposit of tax receipts?
- Are internal controls over the District's information technology system appropriately designed and operating effectively to adequately safeguard District assets?

Audit Results

Internal controls need to be improved in several areas of the District's operations. Control weaknesses are primarily due to the lack of adequate policies and procedures and their implementation. As a result, the District paid professional service providers without written agreements or the necessary supporting documentation, made purchases without using competition, and lost interest revenue. In addition, District computer data and assets were exposed to the risk of loss.

For example, the District's procurement policy did not require written agreements from providers of professional services. District officials paid \$140,740 for professional services without written agreements or the necessary documentation to support the payment of providers' claims. District officials made five purchases totaling \$49,031 without obtaining three written quotes in accordance with District policy and did not use competitive bidding, as required by law, to make purchases of

computer and sports equipment which totaled \$62,911. As a result, there is an increased risk that goods and services are not procured in the most prudent and economical matter.

District taxes are collected by the Town of Warwick Receiver of Taxes for those District taxpayers residing within the Town of Warwick, which delays the deposit of funds into the District's bank account. As a result, the District lost interest revenue of \$15,387 during our audit period.

District officials also did not establish adequate policies and procedures and monitor their implementation to effectively safeguard computer data and assets. District officials did not designate an individual to be responsible for the District's IT system, nor did they adequately secure one server or its backup tape: both the server and the tape were stored in an open unlocked room. Further, when the District disposes of its old computers and servers, it removes the hard drives and stores them in the basement without sanitizing¹ the hard drives. One of the server hard drives in the basement was from the prior student management system. In addition, District officials have not developed a formal disaster recovery plan. As a result, unauthorized individuals could access and compromise the information stored in those hard drives. In addition, District personnel have no guidelines to follow to resume mission-critical functions in the event of a disaster.

Our review of the IT system also disclosed weaknesses in the controls over the District's financial information and student data applications due to the lack of policies and procedures. As a result, password and log-in security requirements were inadequate, and the default account for the financial software was not removed or password protected. In addition, user rights within the financial software were not consistent with employees' job duties, weakening the segregation of duties within the financial software application. Further, the user rights of eight former employees were not terminated timely when they left District service. Inadequate internal controls over the IT system increase the risk that unauthorized users could access the system and cause the misuse, loss, or inappropriate modification or disclosure of the District's sensitive information.

Comments of District Officials

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comments on the issues raised in the District's response letter.

¹ The purpose of data sanitization is to ensure the recovery of data is impossible. Data sanitization includes erasing data and overwriting the drive with layers of random meaningless data.

Introduction

Background

The Florida Union Free School District (District) is located in the Towns of Goshen and Warwick, in Orange County. The District is governed by the Board of Education (Board) which comprises five elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are two schools in operation within the District, with approximately 850 students and 150 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$15 million, which were funded primarily with State aid and real property taxes.

The Business Administrator is responsible for the procurement of goods and services. The Business Administrator is assisted by the District purchasing clerk, who also serves as the appointed tax collector.

Objective

The objective of our audit was to evaluate internal controls over selected financial activities. Our audit addressed the following related questions:

- Are internal controls over purchasing appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over tax collection adequate to ensure timely deposit of tax receipts?
- Are internal controls over the District's information technology system appropriately designed and operating effectively to adequately safeguard District assets?

Scope and Methodology

We examined internal controls over selected financial activities of the District for the period July 1, 2006 through March 31, 2008.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix C of this report.

**Comments of District
Officials and Corrective
Action**

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comments on the issues raised in the District's response letter.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the GML, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

Purchasing

A good system of internal controls consists of policies, practices and procedures that allow an organization to provide reasonable assurance that it is using its resources effectively and that it is complying with applicable laws and regulations. A major component of such a system is an effective procurement process that helps the District obtain necessary goods and services, as economically as possible. This includes using competitive bidding, requests for proposals (RFPs) and quotes to procure goods and services that are needed for District operations. An effective procurement process also requires written agreements with professional service organizations which provide a clearly defined and mutually agreed-upon basis for determining entitlements to payments. It is essential that District management regularly monitor procurement controls to ensure that they are working as intended.

The District does not have an effective procurement process. The District paid \$140,740 for professional services without written agreements or the necessary documentation to support payment of providers' claims. In addition, the District did not use competitive bidding when purchasing computer-related equipment, sports uniforms and equipment that cost a total of \$62,911. When aggregated by category, each purchase exceeded the threshold required for competitive bidding. We also identified five instances where District officials made individual purchases below the bidding threshold totaling \$49,031, without obtaining three written quotes as required by District policy. As a result, District officials may have lost savings opportunities by limiting their ability to choose from among alternative bids.

Professional Services— District officials are responsible for obtaining a written agreement prior to professionals rendering services. Written agreements between school districts and professional service providers provide both parties with a clear understanding of the services to be provided and the basis for compensation for those services. This system would ensure that claims submitted by professionals are itemized to clearly state who performed the service, the exact service provided and the rate charged. If additional work that is not within the parameters of the original agreement is required, District officials should request an addendum, to be approved by the Board, which sets forth the additional services to be performed, as well as, compensation for those services.

The District's procurement guidelines do not require written agreements to be obtained for professional services. We selected 10

professional service providers who received combined payments of \$328,164 from July 1, 2006 through March 31, 2008, and reviewed payments to determine whether or not written agreements existed, claims were properly itemized, and payments were in accordance with written agreements. We tested \$80,288 of those payments and noted the following deficiencies for 5 of the 10 professional service providers:

- District officials paid \$52,750 for labor-related and general legal services without a signed contract. The District has an unsigned copy of a contract dated July 2000. The District also has letters on file from the attorney for the 2006-07 and 2007-08 fiscal years proposing the fee to be paid during those years. District officials processed and paid claims submitted by the law firm without requesting itemized invoices. District officials are not able to determine the types of services rendered unless they have itemized invoices. Further, District officials cannot assess whether the proposed yearly increases are justified if they do not have the historical evidence from itemized prior-year claims.
- The District paid a certified public accountant (CPA) \$42,450 for two years of service — \$2,400 (\$1,200 per year) more than the amount agreed upon in this provider’s contract. The invoice on file stated that the additional services included assistance with the annual filing of the ST-3,² maintaining depreciation records and various consultations. However, it did not identify who provided the services or the rates charged. When services exceed the approved contractual amount, an addendum should be obtained in order to properly account for these extra costs.
- The District paid an internal auditor a total of \$4,000 for services in accordance with a written agreement; however, the services were not received timely. The District paid the \$4,000 yearly fee in advance for which the District was to receive an initial risk assessment and an updated assessment for the period July 1, 2007 through December 31, 2007. In April 2008, the internal auditor was at the District to provide the service. The function of the internal auditor is to identify risks through an annual review and updated risk assessment of the District’s internal controls. The District must receive timely information in order for it to be useful.
- The District paid a behavioral consultant \$9,187 for services without a signed agreement. The District has a letter on file,

²The ST-3 is the annual financial report filed by school districts.

which states the rate per hour to be charged for the consulting services. However, neither the consultant nor District officials signed the letter. District officials informed us the reason the agreement was not signed was that the consultant was obtained in a rushed manner. District officials are responsible for obtaining a written agreement prior to professionals rendering services. Without the benefit of a negotiated written agreement, District officials cannot be certain of the services that will be provided or the rate that will be charged. Therefore, District officials have no assurance that they obtained the best value for District taxpayers.

- The District paid \$32,352 to a speech, occupational and physical therapy consultant. We reviewed three payment vouchers totaling \$3,052 that did not contain proper itemization for services rendered. District vouchers are completed by special education service providers and signed by the head of the special education department to document that the services were provided, to identify the individual who provided the service and the student who received the service. When the provider submits an invoice for payment, the Business Office verifies that the amount of the invoice is correct by reviewing the signed vouchers. However, not all the signed vouchers were properly itemized. Without requesting itemized invoices, the District risks paying for services that were not provided.

Competitive Bidding — General Municipal Law and the District’s procurement guidelines require that purchase contracts for materials, equipment and supplies involving an estimated annual expenditure exceeding \$10,000, and public work contracts involving an expenditure of more than \$20,000, will be awarded only after responsible bids have been received in response to a public advertisement. Purchases or public work contracts from New York State contracts are exempt from bidding provisions. In determining the necessity for competitive bidding, the aggregate amount expected to be expended must be considered. Competitive bidding is required when it is known or can be reasonably expected that the aggregate amount of purchases of the same or similar commodities will exceed the dollar threshold over the course of the fiscal year. Additionally, items of the same or similar nature which are customarily handled by the same vendor should be treated as a single item for purposes of determining whether the dollar threshold will be exceeded. Further, the District’s policy requires that three written quotes be obtained for public works contracts totaling between \$7,000 and \$20,000.

We reviewed the cash disbursements list and selected 20 vendors, with total purchases of \$266,216, that typically provide computer-related

components and sports equipment to determine if the aggregate of these purchases exceeded the threshold for competitive bidding. The District purchased computer-related equipment, sports uniforms and equipment totaling \$29,144, \$17,199 and \$16,567, respectively, from 8 of the 20 vendors. These purchases should have been bid since the value of the related purchases exceeded the competitive bidding threshold. Additionally, one of the eight vendors was paid in excess of \$10,000 on multiple invoices in both the 2006-07 and 2007-08 fiscal years.

To determine if the District requested quotes in accordance with its procurement policy, we reviewed purchases from 15 vendors totaling \$221,128 that the District made during the period July 1, 2006 through March 31, 2008. We found five instances totaling \$49,031 where the District did not obtain the required three written quotes. For example, three written quotes were not obtained prior to the District expending \$10,500 for materials and services for paving one of the District's parking lots. District officials made the remaining purchases totaling \$172,097 primarily through State contracts or otherwise in accordance with the District's procurement policy.

Without strict adherence to the District's procurement policy, there is increased risk that goods and services may not be procured in the most prudent and economical manner.

Recommendations

1. District officials should enter into written agreements with all professional service providers. The agreements should clearly define the amount of compensation and scope of work to be performed. An addendum should be obtained for any work performed outside the scope of the original agreement.
2. District officials should ensure that services are provided in accordance with the agreement in place.
3. District officials should ensure that claims submitted by professionals identify the individual(s) who performed the service, are sufficiently itemized and clearly state the exact service provided and the rate charged.
4. District officials should ensure that all items are procured in accordance with competitive bidding requirements and District policy.

Tax Receipts

Financial accountability includes maximizing interest earnings whenever feasible without subjecting financial assets to unnecessary risk or cost. The Board has a fiduciary responsibility to make the most prudent use of its funds. The District collects real property taxes from property owners in the Towns of Goshen and Warwick. The District appointed one of its full-time employees to collect taxes for the Town of Goshen. For those property owners in the Town of Warwick, the Town's Receiver of Taxes collects District property taxes. We found that there was a delay between when property taxes were collected by the Town of Warwick and the date they were deposited into the District's account. This resulted in the potential loss of interest revenues to the District.

During our audit period, the Town of Warwick's Receiver of Taxes was responsible for collecting 77 percent of tax receipts owed to the District. Tax receipts are received in person or by mail and include the bulk payments from tax servicing companies. Once collected, the funds were deposited in the Town Receiver's bank account. The Town delayed disbursement of the funds collected to the District until the checks received had cleared. On a weekly basis, the District Treasurer went to the Town of Warwick to collect taxes received. The District Treasurer is provided with multiple checks corresponding to the amount of funds collected each day of the previous week and a reconciliation provided by the Receiver of Taxes.

We reviewed the amounts collected by the Town of Warwick's Receiver of Taxes and the District's deposits to determine the amount of time between the date the funds were collected and the date the District deposited the funds. A delay of seven to 10 days occurred between the times of collection and deposit by the District. For example:

Date Collected by Town of Warwick Collector	Date Deposited by the District	Number of Days Between Collection and Deposit
9/10/07	9/17/07	7
9/11/07	9/18/07	7
9/12/07	9/19/07	7
9/13/07	9/20/07	7
9/14/07	9/24/07	10
9/17/07	9/24/07	7

During the 2006-07 and 2007-08 tax collection periods, the District received an average interest rate of less than 1 percent and 1.5 percent, respectively, on the District tax account and 4.9 percent and 4.2 percent, respectively, on its investment account. It is normal District policy to routinely transfer cash to the higher yielding investment account until it is required for a specific District purpose. Applying the higher yield, we determined that the District potentially lost \$15,387 during our audit period because deposits were not made timely.

District officials were aware of the delay in processing deposits; however, they did not research alternate options or determine the financial impact to the District. Alternate options, such as having the Town of Warwick's Receiver of Taxes deposit funds directly into a District account, would eliminate the delay that is currently occurring. Improving the timeliness of deposit allows the District better management of its cash flow and can result in increased interest earnings.

Recommendation

5. District officials should evaluate potential solutions to alleviate the delay between collection and deposit of tax revenues.

Information Technology

The District relies on its information technology (IT) system to provide computer education, access the Internet, communicate by email, store student data, maintain financial records, and report to State and Federal agencies. Therefore, the IT system and the data it holds are valuable resources. If the IT system fails, the resulting problems could range from inconvenient to catastrophic. Even small disruptions can require extensive employee and consultant effort to evaluate and repair. It is therefore important that District officials assign responsibility for the District's IT system, implement password provisions, control and monitor system access, establish a formal disaster recovery or business continuity plan, and ensure that computerized assets are physically secured and that data is backed up.

District officials are responsible for adopting policies and procedures and developing controls to safeguard computerized data and assets and for ensuring that District officials and employees adhere to adopted policies and procedures. While our tests did not identify any occurrences of unauthorized activity, District officials should promptly correct the weaknesses we identified to reduce the risk that sensitive or mission-critical data may be lost or compromised, or that systems could be damaged or disrupted.

Business Continuity

Business continuity is concerned with maintaining or reestablishing the activities or level of service provided by the District in the event of a disaster or other damaging occurrence. Such an event could be a power outage, hardware failure, fire or damaging storm. Contingency planning is used to avert or minimize the damage that disasters could cause to operations. Such planning involves more than planning for a move offsite after a disaster. It also addresses how to keep critical functions operating in the event of disruptions, both large and small. District officials are responsible for assigning authority and responsibility for the security of the IT system to ensure that computerized data can be repaired or replaced if such an event occurs. Procedures must be developed to ensure computerized assets are physically secured, data is backed up and a disaster recovery plan is adopted.

Assigning Responsibilities — District officials have not designated the responsibility for assigning and monitoring computer system access of the District's IT system to one individual. The District currently uses an instructional technology specialist (IT specialist)

to perform routine maintenance on the District's IT system; however, her job description does not include responsibility for the District's entire IT system. In addition, a BOCES technician works at the District two days per week to assist the IT specialist. The function of the IT specialist is to integrate technology into classroom instruction and maintain classroom equipment, but not to maintain and assess risks over the entire network. The Board cannot ensure business continuity, as it has not designated one individual to be responsible for the District's IT system who would monitor risk and take appropriate action to mitigate identified risks.

Data Backup — Even the most reliable computers can break down. Data stored on computers and servers should be backed up (a duplicate copy made) on a routine basis to enable it to be restored in the event of a disaster. The back-up copy should be stored at an environmentally and physically secure off-site location. Periodically, the back-up copy should be used to restore the system in order to ensure that the data is both complete and useable. This will enable the restoration of the IT system and data in the event of loss.

The District contracts with BOCES to back up the Business Office server, which includes the financial information, and the student/teacher server which contains data for the use of teachers and students. The District's other critical servers are the student data servers which are supported through the Mid-Hudson Regional Information Center (MHRIC). Even though the district was unaware of it, the MHRIC backs up these servers nightly. The District's IT specialist also backs up these servers to tape; one tape is taken to a locked closet within the same building, while another tape was left sitting next to the server in an open unlocked room. The tape that is locked in the closet ensures that data is physically protected; however, a disaster, such as a fire or water leak, could damage both the computer equipment and the media containing the back-up data. The tape left sitting in an open, unlocked room presents an even greater risk. The data on these servers contains information, such as name, address, date of birth, social security number and health information retained by the District for each student. Leaving this data unprotected could lead to the unauthorized release of personal or confidential information.

Disaster Recovery — District officials are responsible for developing and documenting a disaster recovery plan. A disaster recovery plan, sometimes referred to as a business continuity plan or business process contingency plan, describes how an organization is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of the disaster will be minimized, and the risk of potentially losing important student

and financial data will be reduced. Further, the plan should set forth procedures to ensure District personnel can either maintain, or quickly resume, mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention. Disaster recovery planning should be an ongoing, dynamic process.

District officials have not developed and documented a formal disaster recovery plan. As a result, in the event of a disaster, District personnel have no guidelines or plan to follow to resume mission critical functions.

Physical Security – Proper safeguarding of assets involves restricting access to computerized assets and data to help reduce the risk of unauthorized use or loss. Limiting access to those assets, ensuring assets are located in a climate-controlled environment, and ensuring proper disposal are necessary to secure the District’s computerized assets and data.

District officials have not adequately addressed the safeguarding of their computerized assets and data. Because of inadequate climate control in the server room located at the elementary school, the room was left unlocked with the door open during the school day to avoid damage to equipment from overheating. Therefore, unauthorized personnel and students could potentially access the server room.

District officials did not ensure computer and server hard drives were sanitized³ and disposed of properly. We observed the District has over 50 computer hard drives stored in the basement. Approximately five server hard drives were removed and are currently stored in the basement, one of which was from the old student management system. Generally, this area is locked and used by custodial staff for storage of supplies. As a result, confidential student data may be at risk of loss or misuse.

Without adequate safeguarding of computerized assets, other security measures may be meaningless. Physical threats, whether internal or external, malicious or inadvertent, could lead to damaged or stolen hardware and the unauthorized release of personal or confidential information. If such events occur because of physical security breaches, addressing the damage caused can cost thousands of dollars and require countless work hours, and may lead to costly litigation for the District.

³ The purpose of data sanitization is to ensure the recovery of data is impossible. Data sanitization includes erasing data and overwriting the drive with layers of random meaningless data.

User Access Controls

Access controls provide reasonable assurance that computer resources are protected from unauthorized use and modifications. To control access, computer systems and applications need a process in place to identify and differentiate users. User accounts identify users and establish relationships between the user and a network, computer, or application. Access controls over user accounts include requiring complex passwords, limiting and controlling administrator accounts, and restricting users to the minimum access necessary for their day-to-day duties and responsibilities.

We found the District did not adequately design user access controls to protect its computer system against unauthorized access. We noted the following weaknesses associated with access controls:

Passwords/Lock-Out Policy — The use of passwords and the implementation of a lock-out policy work together to help protect computer resources from unauthorized modification. To access a network, computer, or application, users must enter their user name and password. The computer compares this information with the user account database. If a match is found, access is granted as provided for the user account. A lock-out policy automatically prevents access to the user's account after a set number of failed log-in attempts.

Complex passwords contain combinations of uppercase and lowercase letters, numbers, and punctuation, and are at least eight characters long. They should not contain words found in the dictionary; hardware or software names; repeated letters or numbers; addresses; phone numbers; or the user's name, family members' names, or pet names. Passwords should be changed every 30 to 90 days to protect confidentiality.

We identified weaknesses in the District's controls over password security. Given the sensitive nature of this issue, we have communicated these weaknesses to District officials in a separate, confidential letter. As a result of the weaknesses, the District is at an increased risk of loss or unauthorized modification of its sensitive information.

Financial System User Accounts — We also found weaknesses in user access controls for the financial system. The District's financial software consists of modules that segregate various financial recording and reporting processes. Access privileges within the financial software can be programmed to restrict individuals' access to transactions within the scope of their responsibilities. However, our review disclosed that Business Office employees had unlimited access rights to all modules. Also, the claims auditor was given unlimited access rights, where, based on her job function, read only rights are sufficient. In an effort to determine if the default administrative account had been removed

or password protected, we attempted to login using the default values for this software and were able to gain full administrative access to the program. As a result of the inadequate access controls, there is a significant risk that improper transactions could be initiated and be concealed. When we informed District officials, they immediately made changes to correct the weaknesses.

Authorization and Notification of Changes to User Access Rights – Effective access controls require that authorized users’ specific needs, and any modifications, are approved by a senior manager and directly communicated in writing to the IT specialist or individual in an equivalent position. It is especially important that an employee’s termination or revocation of access rights be communicated immediately. A formal process for transmitting these authorizations, including standardized access request forms, reduces the risk of errors and misunderstandings. Although notification may be provided by the building principals or by others, policies should be in place that clearly assigns responsibility for such notifications.

District officials have not developed policies and procedures for authorizing, making, and documenting changes to user accounts. There are no formal procedures to notify the IT specialist when employees were hired or terminated, or to ensure that user accounts were promptly deactivated when employees leave District service. We reviewed user access rights granted to the Business Office server, student/teacher servers and the student management server to determine if there were former employees with system access. We found eight instances where an employee who left the District still had access to the system. Of the eight, five were on the student/teacher servers and three were on the student management server from 11 to 25 months after they had been removed from District employment. By not disabling user accounts when employees leave District service, District computers can be vulnerable to unauthorized use which places data at risk of loss or alteration.

Additionally, we found two accounts with administrative rights used by the MHRIC on each of the District’s two student management servers. While it is necessary for MHRIC personnel to access these servers, individual accounts should be created. Furthermore, the student/teacher server has 16 generic IDs and the student management server has three generic user IDs. The use of generic accounts increases the difficulty of monitoring and controlling access and does not provide accountability for user access and activities taking place on the network.

Recommendations

6. District officials should establish clear authority and responsibility for IT system security.

7. District officials should establish written procedures to ensure that all information stored on the IT system is properly backed up and that backup files are secured in a safe, off-site location.
8. District officials should develop a formal disaster recovery plan to address the possible loss of computer equipment and data in the event of a disaster.
9. District officials should ensure access to computerized assets is restricted, assets are located in climate-controlled areas and hardware is properly sanitized or destroyed upon disposal.
10. District officials should improve controls over password security and login attempts.
11. District officials should establish formal policies or procedures to authorize user accounts, outline how user permissions will be established to ensure employee access is restricted in accordance with their job duties, require changes to accounts to be documented and ensure prompt termination of user accounts.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.

Florida Union Free School District

S.S. SEWARD MEMORIAL BUILDING
51 NORTH MAIN STREET
P.O. DRAWER 757
FLORIDA, NEW YORK 10921-0757

TELEPHONE: 845-651-3095
FACSIMILE: 845-651-6801

DOUGLAS W. BURNSIDE
Superintendent of Schools

October 28, 2008

[REDACTED]

Division of Local Government and
School Accountability
Office of the State Comptroller
110 State Street
Albany, NY 12236

Dear [REDACTED]

We are in receipt of the preliminary draft findings of your recent examination of the Florida Union Free School District.

Conceptually, we do not dispute any of the findings. There are a few minor points of fact that should be addressed before the final report is issued:

1. On pages 4 and 6 of the Executive Summary, it says that our Board of Education is "comprised of seven elected members." It should say "five."
2. On page 15 of the Executive Summary, second paragraph, line 5, the following phrase is inaccurate and should be deleted: "Even though the district was unaware of..."

See
Note 1
Page 21

See
Note 2
Page 21

These discrepancies were shared with [REDACTED] and [REDACTED] when they made their field visits to our District. Both examiners were highly professional, courteous, and cordial. We feel that we will benefit greatly from their thorough examination, as reflected in the preliminary findings. We expect to improve our operations and maximize our revenues based on our responses to the audit. These responses will be forthcoming in our CAP reports, that we are in the process of developing presently.

If there are any questions or concerns, please contact me at 845-651-3095, extension 1.

Sincerely,



Douglas W. Burnside
Superintendent of Schools

DWB/ha

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

We have amended our report based upon the information submitted.

Note 2

When we initially inquired about the backup of information on District servers, the District's IT specialist needed to contact the Mid-Hudson Regional Information Center (MHRIC) for a definitive answer. As a result, we believe that our statement in the report that District officials were "unaware" that the MHRIC performed a nightly backup of the servers is accurate.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard District assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, and payroll and personal services and information technology.

During the initial assessment, we interviewed appropriate District officials, performed limited tests of transactions and reviewed pertinent documents, such as District policies and procedures manuals, Board minutes, and financial records and reports. In addition, we obtained information directly from the computerized financial databases and then analyzed it electronically using computer-assisted techniques. This approach provided us with additional information about the District's financial transactions as recorded in its databases. Further, we reviewed the District's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed, and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided upon the reported objectives and scope by selecting for audit those areas most at risk. We selected procurement, tax receipts and information technology for further audit testing.

In order to accomplish the objectives of this audit, our procedures included the following:

- We interviewed employees in the District's Business Office and other relevant employees to obtain an understanding of the internal controls in place at the District with regard to purchasing practices. We conducted tests of transactions related to competitive bids and professional services.
- We reviewed the cash disbursement list and selected ten professional service providers for testing and reviewed contracts where available. We also reviewed the cash disbursement list and selected three invoices for each provider.
- We reviewed the cash disbursement list and judgmentally selected 15 vendors whose total disbursements exceeded the threshold required for competitive bidding. We selected multiple claims for each vendor for review. In instances where a bid was required, we reviewed the bid. When a State contract was used, we verified that it was a valid State contract and the vendor was authorized under that contract.
- We reviewed the cash disbursement list and selected vendors who provide computer-related components and sports equipment. We reviewed all invoices for each of the selected vendors to determine items purchased. We grouped similar or like items to determine if the aggregate purchase exceeded the threshold required for competitive bidding.

- We interviewed employees in the District's Business Office and interviewed the Town of Warwick Tax Receiver to obtain an understanding of the process in place for billing, collecting, depositing and remitting tax revenues to the district.
- We obtained reports from Ttheown of Warwick Tax Receiver detailing the amount of taxes collected daily to determine when taxes were actually collected, and traced those amounts to the District's bank records to determine the amount of time between actual collection and deposit to District bank accounts.
- We reviewed District bank statements to determine the interest rate available to the District during the period audited. We used this rate to determine the amount of interest revenue forgone due to the lag time between collection and deposit.
- We obtained reports from the Town of Warwick Tax Receiver to determine the amount of taxes received during the penalty period. We recalculated the penalty using the rate the District would be entitled to receive.
- We interviewed the Superintendent, Business Assistant and instructional technology specialist to gain an understanding of policies and procedures in place related to the physical and logical security of the District's information technology infrastructure.
- We reviewed the instructional technology specialist's job description to determine her responsibilities and interviewed the Superintendent regarding her job description.
- We performed an inspection of the District's infrastructure and inspected the server room, wiring closets and storage areas.
- We reviewed the list of current user IDs on the student/teacher server and the student management server and compared it to employee records to determine if all active user IDs were for current employees. For those former employees still active on the system, we obtained the last date of employment with the District to determine the amount of time active after separation from the District.
- We reviewed access rights granted to District Business Office personnel for the financial software to determine if rights were granted in accordance with job duties.
- Reviewed a list of employee accounts on the financial software to determine if all users were valid employees. We also performed a test login using the default the account to determine if account was removed or password changed.
- We interviewed employees regarding lock out provisions on computers. We observed while one employee attempted to log in to the Business Office server to determine if the system would lock after a predetermined number of failed login attempts. The same test was performed for the student/teacher server and student management server.
- We reviewed network policies set up on the student/teacher server and student management server to determine if password changes were forced and complexity requirements set.

We conducted our performance audit in accordance with generally accepted government auditing standards (GAGAS). 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.

APPENDIX D

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
<http://www.osc.state.ny.us/localgov/>

APPENDIX E
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Steven J. Hancox, Deputy Comptroller
John C. Traylor, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BUFFALO REGIONAL OFFICE

Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie,
Genesee, Niagara, Orleans, Wyoming counties

ROCHESTER REGIONAL OFFICE

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe,
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates
counties

SYRACUSE REGIONAL OFFICE

Eugene A. Camp, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison,
Oneida, Onondaga, Oswego, St. Lawrence counties

BINGHAMTON REGIONAL OFFICE

Patrick Carbone, Chief Examiner
Office of the State Comptroller
State Office Building, Room 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Otsego, Schoharie, Sullivan, Tioga, Tompkins
counties

GLENS FALLS REGIONAL OFFICE

Karl Smoczynski, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Clinton, Essex, Franklin, Fulton, Hamilton,
Montgomery, Rensselaer, Saratoga, Warren, Washington
counties

ALBANY REGIONAL OFFICE

Kenneth Madej, Chief Examiner
Office of the State Comptroller
22 Computer Drive West
Albany, New York 12205-1695
(518) 438-0093 Fax (518) 438-0367
Email: Muni-Albany@osc.state.ny.us

Serving: Albany, Columbia, Dutchess, Greene,
Schenectady, Ulster counties

HAUPPAUGE REGIONAL OFFICE

Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE

Christopher Ellis, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Orange, Putnam, Rockland, Westchester
counties