



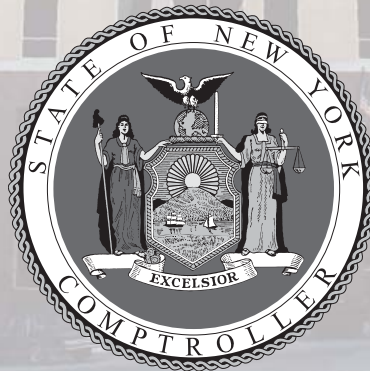
West Islip Union Free School District Internal Controls Over Selected Financial Activities

Report of Examination

Period Covered:

July 1, 2006 — November 30, 2007

2008M-180



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
CONFLICTS OF INTEREST	7
Recommendations	9
EMPLOYEE FRINGE BENEFITS	10
Recommendations	10
INFORMATION TECHNOLOGY	11
Recommendations	15
APPENDIX A Response From District Officials	17
APPENDIX B OSC Comments on the District’s Response	22
APPENDIX C Audit Methodology and Standards	23
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

December 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 West Islip 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 West Islip Union Free School District (District) is governed by the Board of Education (Board) which comprises seven 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.

The Board adopted a revised code of ethics for all District personnel in 2001 and again revised it in 2006 and 2007. The District's payroll clerk uses a computerized financial system to process payroll transactions through the Business Office. For the year ending June 30, 2007, gross payroll disbursements totaled \$81 million.

Scope and Objective

The objective of our audit was to determine if internal controls over selected financial operations were appropriately designed and operating effectively for the period July 1, 2006 to November 30, 2007. Our audit addressed the following related questions:

- Did District officials appropriately monitor compliance with the Board's adopted code of ethics that prohibits conflicts of interests?
- Are internal controls over employee fringe benefits appropriately designed and operating effectively to adequately safeguard District assets?
- Did the District design adequate controls over information technology to protect electronic data?

Audit Results

We found that District management did not develop adequate policies and procedures or ensure that existing policies and procedures were followed to safeguard District assets. As a result, we found instances where officials did not comply with its code of ethics, and also found inadequate controls over employee fringe benefits and information technology.

We found that District officials failed to design procedures to facilitate compliance with the District's code of ethics, which resulted in the Board President and a Board Member having interests that were not publicly disclosed.

The District's internal controls over employee fringe benefits were not appropriately designed or operating effectively to safeguard District assets. We found that the District paid the Assistant Superintendent for Business a total of \$6,276 for waiving the right to participate in the District's medical insurance plan. However, her employment contract did not contain a provision for this benefit. As a result, the District may have incurred unnecessary expenses.

We found that District officials have not developed comprehensive policies and procedures to protect critical electronic data. We found that the District established a computer use policy but does not require all employees to comply with it. In addition, the District had no formal policies and procedures to add and delete employees from the system and did not disable two former employees' access. The District allowed two employees full system user maintenance rights, although their job responsibilities did not require full maintenance rights. The District also granted a payroll clerk full access to all payroll functions although her duties did not require full access rights. The District has not established policies and procedures addressing remote access, and has not implemented procedures to generate and review audit logs. Furthermore, because of a lack of formal policies and procedures, 15 vendors in the District's master vendor list were assigned multiple identification numbers, and the District had not conducted a test or restoration of backup data. Finally, the District has not developed a formal disaster recovery plan. As a result of all of these control weaknesses, critical electronic data is subject to an increased risk of loss or misuse.

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. Appendix B contains our comments on issues raised in the District's response. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to take corrective action.

Introduction

Background

The West Islip Union Free School District (District) is located in the Town of Islip, Suffolk County. The District is governed by the Board of Education (Board) which comprises seven 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 nine schools in operation within the District, with approximately 5,870 students and 1,230 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$92.7 million, which were funded primarily with State aid, real property taxes, and grants.

The Board adopted a revised code of ethics for all District personnel in 2001 and again revised it in 2006 and 2007. The District's payroll clerk uses a computerized financial system to process payroll transactions through the Business Office. For the year ending June 30, 2007, gross payroll disbursements totaled \$81 million.

Objective

The objective of our audit was to determine if internal controls over selected financial operations were appropriately designed and operating effectively. Our audit addressed the following related questions:

- Did District officials appropriately monitor compliance with the Board's adopted code of ethics that prohibits conflicts of interest?
- Are internal controls over employee fringe benefits appropriately designed and operating effectively to adequately safeguard District assets?
- Did the District design adequate controls over information technology to protect electronic data?

Scope and Methodology

We examined the District's internal controls over selected financial activities of the West Islip Union Free School District for the period July 1, 2006 to November 30, 2007.

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. Appendix B contains our comments on issues raised in the District's response. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to take corrective action.

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.

Conflicts of Interest

The General Municipal Law (GML, Article 18) limits the ability of municipal officers and employees to enter into contracts in which both their personal financial interests and their public powers and duties conflict. Unless a statutory exception applies, the GML prohibits municipal officers and employees from having an “interest” in contracts with the municipality for which they serve when they also have the power or duty – either individually or as a board member – to negotiate, prepare, authorize, or approve the contract; to authorize or approve payment under the contract; to audit bills or claims under the contract; or to appoint an officer or employee with any of those powers or duties. Municipal officers and employees have an interest in a contract when they receive a direct or indirect monetary or material benefit as a result of a contract. Municipal officers and employees are also deemed to have an interest in the contracts of their spouse, minor children and dependents (except employment contracts); a firm partnership or association of which they are a member or employee; and a corporation of which they are an officer, director or employee, or directly or indirectly own or control any stock. As a rule, interests in actual or proposed contracts on the part of a municipal officer or employee, or his or her spouse, must be publicly disclosed in writing to the municipal officer or employee’s immediate supervisor and to the governing board of the municipality.

The GML also requires that the governing body of every school district in the State adopt a local code of ethics to guide the District’s officers and employees. A code of ethics can help enhance the control environment of an organization by setting forth the standards of conduct expected of officers and employees and reinforcing applicable statutory provisions. Under the GML, the chief executive officer of each school district is required to cause a copy of the code of ethics to be distributed to every officer and employee of the district. Failure to distribute the code, or failure of an officer or employee to receive the code, however, has no effect on the duty of compliance with the code.

The Board adopted a revised code of ethics for all District personnel in 2001 and again revised it in 2006 and 2007. This code sets forth certain standards of conduct including with respect to private employment in conflict with official duties, and certain disclosures of interests. Among other things, the code generally requires that District officers and employees who participate in a discussion or render an opinion to the Board publicly disclose “on the official record the nature and extent of any direct or indirect financial or private interest ... in the

determination of such matter.” The term “interest” for this purpose is deemed under the code to include “the affairs of the officer’s or employee’s spouse, minor children and dependents ...” In addition, the code directs the Superintendent to distribute a copy of the code of ethics to every officer and employee of the School District.

The District has not established proper procedures to monitor the distribution of the code of ethics. The Assistant Superintendent for Curriculum and Instruction emailed a copy of the code to District officers and employees in September 2007; however, the Board revised the code in November 2007 to require the completion of an annual “conflict of interest form” by all central and building administrators. This revised version included the directive for the Superintendent to distribute a copy to every officer and employee within two weeks of adoption, but District officials could not confirm that the Superintendent complied with this directive. At the exit conference, the Superintendent provided us with a copy of an email that was intended to distribute the revised code of ethics. However, the email was sent to only five District officials and not the same District officers and employees who received the September 2007 email.

Two District officials did not publicly disclose interests that resulted in total payments of \$23,310. The District’s code of ethics appears to require disclosure by District officers and employees whose spouses have or will have an interest in a contract with the District.

- In one instance, a Board Member’s spouse was appointed as a paraprofessional for the District. The Board Member abstained from voting for both the temporary and permanent appointments of his spouse, but the relationship was not publicly disclosed for the official record. In addition, the Board Member did not announce why he abstained from voting on his spouse’s appointment. During the 16 month audit period, the Board Member’s spouse was paid gross wages of \$11,460.
- In a second, similar instance, the Board President’s spouse was employed by the District as a substitute clerical staffer. The Board President abstained from voting on his spouse’s appointment, but did not disclose his relationship, and did not announce why he abstained from voting on his spouse’s appointment. Further, the Board President later voted on a wage increase for substitute clerical staff, without publicly disclosing the relationship for the official record. During the 16 month audit period, the Board President’s spouse was paid gross wages of \$10,850.

The District’s lack of procedures related to the code of ethics and required disclosures creates a weakness in internal controls, which

can create an appearance of impropriety or increases the risk that prohibited transactions, which may result in an improper enrichment of the individual at taxpayers' expense, may occur.

Recommendations

1. The Superintendent, in consultation with the Assistant Superintendent for Business, should establish procedures which include specific steps to ensure that District officers and employees are made aware of and comply with the requirements of both the District's code of ethics and Article 18 of the GML, and that each officer and employee receives a copy of the latest version of the code of ethics in a timely manner.
2. Board members should publicly disclose employment relationships of their spouses such as those discussed above, for the official record as required by the code of ethics and the GML.

Employee Fringe Benefits

The Board must clearly define and authorize all employees' compensation and benefits payments to ensure employees receive payments that they are entitled to. The Board may choose to establish District-wide policies or pass annual resolutions concerning the compensation and benefits to be provided to individuals who are not covered by employment contracts or collective bargaining agreements.

The collective bargaining agreements representing most District employees allow them to be reimbursed for waiving their right to participate in the District's health insurance plan. For management employees, such as the Assistant Superintendent for Business, who are excluded from coverage under the District's collective bargaining agreements, the Board passes annual resolutions that set salaries and address additional fringe benefits to be received.

The District did not properly review disbursements to employees for fringe benefits to ensure that payments were made in accordance with employment contracts. During the period February 1, 2007 through January 25, 2008, the District made payments totaling \$390,092 to 110 employees who waived their right to participate in the District's health insurance plan. We examined eight of these reimbursements totaling \$51,434 to various employees and found that the Assistant Superintendent for Business received a \$6,276 payment for waiving her right to participate in the District's medical insurance plan. However, her contract did not contain a provision for this reimbursement.

Because internal controls to review fringe benefit payments were not in place, the District improperly paid the Assistant Superintendent for Business \$6,276 that she was not entitled to.

Recommendations

3. The District should ensure that procedures for processing fringe benefit payments are in place to prevent errors or improper payments.
4. The District should review compensation provided to employees and pursue the repayment of any unauthorized or unintended amounts.

Information Technology

The District's widespread use of information technology presents a number of internal control risks that must be addressed. These risks include unauthorized access to data, unauthorized changes to data in master files, and potential loss of data. The District can mitigate these risks through a combination of automated and manual controls including policies and procedures adopted by the Board, and limiting user access to protect data from loss by intentional or unintentional manipulation. The internal control system should include a disaster recovery plan and systematic backup procedures to restore lost or damaged data as quickly as possible.

We examined controls over the District's computerized financial operations and found that District officials have not developed comprehensive policies and procedures to protect critical financial data. We found that the District established a computer use policy but does not require all employees to comply with it. In addition, the District had no formal policies and procedures to add and delete employees from the system and did not disable two former employees' access. The District allowed two employees full system user maintenance rights, and granted a payroll clerk full access to all payroll functions. The District has not established policies and procedures addressing remote access, and has not implemented procedures to generate and review audit logs. Furthermore, because of a lack of formal policies and procedures, 15 vendors in the District's master vendor list were assigned multiple identification numbers, and the District had not conducted a test or restoration of backup data. Finally, the District has not developed a formal disaster recovery plan. As a result, critical financial data is subject to an increased risk of loss or misuse.

Computer Use Policy — Computer use policies define appropriate user behavior and the tools and procedures necessary to protect information systems. Such policies include procedures governing the acceptable use of computers, internet access, electronic mail and portable devices, as well as procedures for information protection, virus protection and password security. Penalties for the violation of these policies should be clearly defined. To be effective, District management must ensure that the computer use policy is distributed to all district employees.

In March 2001, the Board adopted the "Staff Use of Computerized Information Resource" policy. This policy outlines the staff's responsibilities regarding computer use, email and internet. This policy

requires all employees to acknowledge in writing that they received a copy of the policy and agree to abide by its terms. However, District management only required teachers to sign the acknowledgement; they did not require the rest of District staff to sign the acknowledgement. We interviewed employees in the Business Office, and they informed us that they were not required to sign the acknowledgement and were not aware of the policy.

The District's failure to require all employees to comply with the District's computer use policy increases the risk that confidential and sensitive information and hardware and software systems may be lost or damaged by inappropriate use.

User Access Accounts — User accounts identify specific users within a particular network, computer and/or application. These accounts are created by the system administrator and contain information such as passwords and access rights to files, applications, directories and other computer resources. The District has no policies or procedures in place to add or delete an employee's, teacher's or student's access to the District's network. The Director of Information Systems informed us that, usually, the human resource department informs the IT department of a change to user access, and the IT Department makes the requested change. However, we found the District has no written documentation to support this procedure. Also, the District does not have procedures to disable the accounts of inactive employees, and user accounts are not deactivated timely. We identified two former District employees who still had active user accounts within the financial software. These user accounts remained active three months to more than two years after leaving District service. After we brought this issue to District officials' attention, they disabled the accounts. We reviewed the audit logs and confirmed that these accounts had not been used after the employees left service. The failure to establish and implement policies and procedures to limit user access increases the risk that unauthorized users could inappropriately gain access to the District's computer systems and change, destroy or manipulate computerized data and assets.

User Permissions — Controls for user permissions are designed to limit system users' ability to access software and data based on their job duties. Administrative user rights give users complete access to create, delete, and modify files, folders, and settings within specific software. The District's financial software has the ability to restrict individuals' access to transactions within the scope of their job responsibilities. We found that two District officials had full system user maintenance rights, allowing them to change user permissions and add or delete users. However, neither District official needed full user maintenance rights to perform their job duties. In addition,

we found that a payroll clerk had full access to all payroll functions as well as incompatible rights within the human resource functions. These incompatible functions allow the clerk access to adjust pay rates and hours worked in addition to processing the payroll. During the planning phase, we tested three employees' pay rates and found no exceptions. The District's failure to restrict individuals' access to areas of the accounting software which are incompatible with their job duties contributes to the risk that unauthorized transactions can be initiated and not be detected or corrected.

Remote Access — Remote access (i.e., ability to access the network from the internet or other external source) must be controlled, monitored and tracked so that only authorized individuals may enter or retrieve data. Policies and procedures should address how remote access is granted, as well as how it will be monitored, tracked and controlled. The District has not established policies and procedures addressing remote access. As part of the system maintenance, the financial software's manufacturer has remote access to the District's network to upload and install software updates and patches.¹ The manufacturer connects to the network remotely via a VPN² connection through a port channel which is left open at all times, allowing the manufacturer unlimited access to the District's server. Additionally, the District does not monitor remote access to the network. The system's capability for generating remote access logs is turned off; therefore, no logs are generated or monitored. Internal controls are greatly weakened when remote access is not monitored, tracked and controlled. As a result, financial data could be manipulated and could allow for errors and irregularities to occur and go undetected.

Audit Logs — A computerized financial management system provides a means of determining, on a constant basis, who is accessing the system and what transactions are being processed. Audit logs (commonly referred to as audit trails) maintain a record of activity by system or application and by user. In conjunction with appropriate tools and procedures, audit logs can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The District's financial software application is capable of providing the District with logs indicating who enters the system, from where and when, and what changes occurred. However, the District has not implemented procedures to generate and review the audit logs. Without reviews of the audit logs, the District does not have adequate

¹ A patch is a device that filters and forwards information between components in the network.

² A virtual private network (VPN) is a private network constructed across a public network such as the Internet.

assurance that changes to data or programs are appropriate and authorized. As a result, there is an increased risk that errors and irregularities can occur and go undetected.

Duplicate Vendor Identification Numbers — The vendor master file in a computerized financial system contains a list of vendors who District employees are permitted to purchase goods from. Any changes to the vendor master file must be deemed necessary and properly authorized. To reduce the risk of duplicate or improper payments, it is important to provide each vendor with a unique vendor number. In addition, the District must remove vendors from the active vendor master file who are no longer used by the District. The District's procedure for adding a vendor does not include a cross check to determine if the new vendor is already in the system. Additionally, there is no procedure to change a vendor to 'inactive' in the master vendor list when a vendor is no longer going to be used by the District or was entered incorrectly. We determined that the District's master vendor list contained 5,411 'active' vendors, 2,358 of which received payments during the audit period. We identified 187 possible duplicate vendors in the master vendor list. We selected a judgmental sample of 20 vendors who were paid a total of \$840,302. We determined that 15 of the 20 vendors, who were paid a total of \$764,952, were assigned multiple identification numbers in the District's master vendor list. Although we did not find that the District made duplicate or improper payments to these vendors, District officials' failure to determine that a vendor already exists in the master vendor list increases the risk of duplicate payments, errors and/or irregularities occurring and not being detected or corrected. In addition, allowing vendors to remain in the vendor master file as 'active' when they are no longer going to be used, or were entered incorrectly, increases the risk of improper payments.

System Backup — The District's ability to restore computer data relies on the integrity of its backup data. To ensure its validity, the data backup must be stored at an off-site location and tested and restored on a routine basis. District officials have not conducted a test or restoration of backup data to test the validity of the backup. The failure to periodically test and restore the backup data leaves the District with no assurance that the data is complete and useable and could lead to loss of critical data.

Disaster Recovery — A disaster recovery plan (DRP), sometimes referred to as a business continuity plan, specifies how an organization should deal with potential disasters. A disaster could be a power outage, hardware failure, fire, or storm. Contingency planning is used to avert or minimize the potential damage that a

disaster or other disruption could cause to operations. It also addresses how to keep critical functions operating in the event of disruptions, both large and small. The District has not established formal policies or procedures to address potential disasters. In November 2007, the Board adopted a policy directing District officials to design and develop a DRP; however, currently one does not exist. In the event of computer failure, District personnel have no guidelines or plan to prevent loss of equipment and data or to recover data that has been lost or damaged. The failure to adopt a DRP increases the risk of potential loss of data or the ability to maintain or quickly resume mission-critical functions in the event of a disaster.

Recommendations

5. The District should establish procedures to ensure that all District employees receive and sign the Staff Use of Computerized Information Resource policy before they are granted network access.
6. The District should establish policies and procedures that address:
 - Requiring all District employees to sign acknowledgment of their receipt of the Computer Use Policy
 - Adding and deleting user access accounts, as well as deactivating user accounts as soon as employees leave District service
 - Limiting the ability of system users to access software and data based on the relevance of their job duties
 - Monitoring of the remote access logs and periodically determining whether the benefits of remote access outweigh the security risks
 - Regular monitoring of the IT system, including periodic review of the audit logs
 - Ensuring that backup data is tested and restored on a routine basis and periodically verifying that backup data can be used if necessary
 - Creating a comprehensive disaster recovery plan that details specific guidelines for the protection of private and essential data against damage, loss or destruction.
7. The District should amend the procedure for adding new vendors to the master file to include verification that vendor information

is accurate, complete, and not being duplicated. The procedure should include a limit on the amount of time a vendor can remain “active” but not used. District officials should periodically review the vendor database to ensure that vendors are not duplicated and to ensure consistency and appropriateness of the vendor master file.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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



West Islip School District
100 Sherman Avenue
West Islip, NY 11795
631-893-3000

Dr. Beth Virginia Blau
Superintendent of Schools

November 24, 2008

Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, New York 11788-5533

Dear Mr. Leonard,

In response to the audit report presented to the district by the Office of the State Comptroller, the district has prepared the following response. The State Comptroller's audit team conducted their review of the West Islip UFSD between December 2007 and May 2008. The draft report was sent to the district on October 23, 2008. Throughout the audit the State Comptroller's team was courteous and professional in their interactions with the school district staff.

The West Islip Schools' administrative staff and Board of Education have been diligently making improvements in our record keeping, accountability, and fiscal transparency. The success of our efforts is evident in the audit findings. As described in Appendix B of the audit report, the audit team conducted an initial assessment of our financial records. The result of the assessment was that our internal controls were effective except in three areas.

The District will be reviewing these three areas to improve our internal controls. The suggestions provided in the report, and the suggestions provided by the audit team, will be very helpful in the review process. Following are comments to clarify the District's current practices with regard to the three areas which require improvement.

Conflicts of Interest:

1. Revised Code of Ethics

Revised Code of Ethics was distributed to staff on 11/21/07.

See
Note 1
Page 22

2. Conflict of Interest Form

Policy requires form be distributed to Administrative staff annually. The form was distributed and completed at an administrative meeting on 2/13/08.

See
Note 2
Page 22

3. District Official disclosure

It has not been the District’s procedure to include comments in the minutes of the School Board meetings. The District will amend this procedure for items that pertain to Policy, such as a School Board member’s reason for abstaining from a personnel vote. As the report notes, the School Board members did abstain from voting on matters that they had a personal interest in, and explained the reasons; however, the explanation was not included in the minutes.

Employee Fringe Benefits:

1. Properly review disbursements to employees

Disbursements are properly reviewed. Employment contracts and Board approved agreements are reviewed. Health insurance enrollment records are reviewed. And the calculations of the payments are reviewed. We reviewed the findings in the audit report and found that payments were made properly.

See
Note 3
Page 22

Information Technology:

1. Computer use policy

The audit report stated that it was determined that all users have not been made to sign the Computer Use Policy. The situation will be rectified and all employees and non-employees who serve in the school district will be required to sign a copy of the policy and it will be stored in their files. In addition, the IT department is implementing a process whereby the user has to accept the Internet and Computer Usage policy everyday when signing on to the Internet. By not accepting the online policy the users will forfeit access to the appropriate resources. The statement “We found that the District established a computer use policy but does not require all employees to comply with it” should not be taken out of context. The District does require all employees to comply with it, yet not all employees have a signed copy of the policy on file.

2. User Access Accounts

The user accounts are created by the System Administrators and are disabled upon request from the Personnel department with a form which indicates the last day of employment. This would indicate that the correct IT function to handle the process is being performed. We agree that this procedure should be documented wherever required. We will be implementing a procedure that will require a password change every 45 days for network access.

With response to the two users being found active within the financial system, when an employee leaves who has access to the accounting software, his or her accounting software rights are maintained so that the access rights can be copied for the new employee. The audit team provided the recommendation that the access rights be temporarily disabled until the new employee is hired. We will implement this procedure.

3. User Permissions

Our checks and balances in Accounting are such that the internal controls are strong and risk is not an issue. As was stated by the audit team during our exit interview, this area was a low risk area but was chosen for review because it is an element of our information technology. A computer technician has been designated, by the Board of Education, as the System Administrator for our accounting software. The Computer Technician was deliberately selected by the Board of Education because he has no business function responsibilities, thereby ensuring segregation of duties. The System Administrator does not use the accounting software system for any record keeping or data management. His responsibility is to add and delete employees' access to the software. Instructions are provided to him via a form. The form is either generated by the Assistant Superintendent for Business or the Assistant Superintendent for Curriculum and Instruction and counter signed by the other. The form is signed by the Computer Technician when the change is made and sent to the Internal Claims Auditor. We will do a full review of all the employees' access rights to the accounting software, to conform their access to their job duties.

See
Note 4
Page 22

The function of adding and updating employee's salaries has been handled by the Payroll Clerks, because the Personnel Department was operating with different software. The Personnel Department began this school year 2008/2009 using the same software as the Business Office. The District is in the process of reviewing and implementing procedures to more effectively control the Payroll Clerks' tasks.

4. Remote Access

The only users having remote access to the system are the IT and Network administrators, the accounting software vendor and the school information system vendor. There are no logging servers designated to log any remote access due to the fact that we have very limited remote users. The vendor's access to the server is logged directly on the server. Per the recommendations of the audit team we will implement restricted access for the software vendors.

5. Audit Logs

The audit logs are extremely voluminous. The District, in conjunction with our Internal Auditors, has reviewed our internal controls and have determined that we have effective separation of duties and effective controls. To add more control, we will review procedures to examine audit logs.

6. Duplicate Vendor Identification Numbers

The District makes every effort to prevent duplicate vendor numbers. Our current procedure is that vendor numbers are only assigned by the Purchasing Agent, to minimize duplication. When duplications are found by the Accounts Payable clerks during their

processing of disbursements, they notify the Purchasing Agent. As was noted in the report no improper payments were found.

7. System Back up

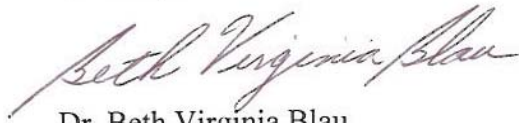
During the interview process it was stated that the IT Department performs a nightly backup of all the data and the data is stored offsite in a fireproof vault at the High School. It was also stated that the tapes are checked for restores, not as per a schedule, but randomly. We will review these procedures.

8. Disaster Recovery

The District recognizes that it needs to evaluate the implementation of a Disaster Recovery Plan.

In conclusion the District understands that an audit of procedures is a process. We view this audit as a tool to assist us in our endeavor to enhance the accountability of our financial operations. We will be reviewing the recommendations from the Comptroller's audit team and will forward our Corrective Action Plan as required.

Sincerely,



Dr. Beth Virginia Blau

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

We have revised our report to clarify this matter. Information provided to us at the exit conference shows that the District's revised code of ethics was distributed to a very limited number of District staff in November 2007.

Note 2

The District distributed this form to administrative staff after we brought it to their attention during our fieldwork.

Note 3

As indicated in our report, the Assistant Superintendent for Business received a \$6,276 payment for waiving her right to participate in the District's medical insurance plan; however, her contract did not contain a provision for this reimbursement. Therefore, we continue to question whether she was entitled to this payment.

Note 4

Our audit report states that a payroll clerk had full access to all payroll functions as well as incompatible rights within the human resource functions. These incompatible functions would allow the clerk access to adjust pay rates and hours worked in addition to processing the payroll. As a result, the District's failure to restrict individuals' access to areas of the accounting software which are incompatible with their job duties increases the risk that unauthorized transactions can be initiated and not be detected or corrected.

At the exit conference, District officials agreed that the payroll clerk was performing incompatible duties and stated they would be correcting this issue during the 2008-09 school year. During our exit conference, we explained to District officials that while our initial assessment of risk did not identify segregation of duties as a high risk issue, our subsequent review of IT issues identified this weakness.

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.

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 conflicts of interest, employee fringe benefits and information technology for further audit testing.

During this audit, we examined records and reports of the District for the July 1, 2006 to November 30, 2007. To accomplish the objectives of the audit and obtain valid evidence, our procedures included the following steps:

- We interviewed appropriate District officials to obtain an understanding of the organization, the District's accounting system and to identify key personnel.
- We obtained copies of District policies and procedures and evaluated the adequacy of these policies.
- We interviewed District staff to obtain an understanding of procedures in place to ensure compliance with the Board-adopted policies.
- We reviewed the minutes of the proceedings of the Board of Education.
- We reviewed the District's financial system for control weaknesses to determine if controls over the system were lacking or circumvented.
- We interviewed the Information Technology Director and Assistant Superintendent concerning network passwords, user accounts, physical access to the system, backups of data and disaster recovery plans.

- We physically inspected the location of system equipment.
- We reviewed user rights and permissions documentation and judgmentally chose users to determine if their user rights were appropriate.
- We interviewed employees in the District’s IT Department and the Business Office concerning the administrative rights to the District’s financial system.
- We examined the collective bargaining agreements and personal employment contracts to determine if the District had properly designed and implemented controls over disbursements for health insurance buy out payments.
- We tested health insurance reimbursements to verify that employees who were receiving reimbursements were not also receiving health insurance through the District, and that payments made were in compliance with employment contracts.
- We examined the following records to determine the effectiveness of internal controls pertaining to the cash receipts and disbursements function and to identify any associated effect of deficiencies found in those controls:
 - o Cash receipt log
 - o Deposit slips
 - o Bank statements
 - o Transaction history reports
 - o Claims packets
 - o Cancelled checks
 - o Cash control accounts
 - o Bank reconciliations
- For internal controls over conflicts of interest, we examined procedures to identify and prevent potential conflicts of interest, and examined Board minutes for associated public disclosures of interest.
- We obtained representations from Board members, District officials, and their spouses that disclosed their outside employment and business interests for the 2006-07 fiscal year. We compared these disclosures to cash disbursement records, claim vouchers, payroll journals and other records to determine if the District had financial transactions with any business interests that might constitute a prohibited conflict of interest.
- We reviewed the District’s vendor master file and judgmentally selected vendors that appeared to be duplicated. We interviewed the District’s purchasing agent for explanations for the apparent duplication.

We conducted our 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