OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Highland Falls-Fort Montgomery Central School District

Internal Controls Over Selected Financial Activities

Report of Examination

Period Covered:

July 1, 2006 — November 16, 2007

2008M-91

Thomas P. DiNapoli

Table of Contents

Page

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

August 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 Highland Falls-Fort Montgomery Central 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

EXECUTIVE SUMMARY

The Highland Falls-Fort Montgomery Central 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.

Scope and Objective

The objective of our audit was to examine the internal controls over selected financial activities for the period July 1, 2006 through November 16, 2007. Our audit addressed the following related questions:

- Are internal controls over personnel policies and procedures appropriately designed and operating effectively to ensure the District's compliance with applicable laws and regulations and to safeguard assets?

- Are internal controls over payroll appropriately designed and operating effectively to adequately safeguard District assets?

- Are internal controls over purchasing appropriately designed and operating effectively to adequately safeguard District assets?

- Are access controls over the District's information technology system appropriately designed and operating effectively to adequately safeguard District's data?

Audit Results

Our audit disclosed internal control weaknesses in the areas of personnel and payroll, purchasing, and information technology. These weaknesses, which included the lack of policies and procedures and poor documentation of activities, potentially placed the welfare of District students at risk; increased the chance that unqualified or ineligible individuals would hold employment with the District; and exposed District's assets and data to the risk of error and loss.

The District's internal controls over its personnel processes need to be improved. The District did not obtain fingerprint-supported background checks for 27 of 58 District employees that we reviewed and four contractors who are in direct contact with students. Therefore, there was an increased risk to

the welfare of District students. In addition, District officials did not obtain Employment Eligibility Verification Forms, required by Federal Law for nine of the 16 employees we reviewed. As a result, the District may be liable for civil penalties. District officials also could not locate the personnel files of two employees, and therefore, the District could not be certain that these employees possessed the necessary educational requirements or had necessary criminal background clearances to hold employment.

The District's controls over payroll processing also need to be improved. We found that District officials hired 13 summer employees without any Board authorization and three others were hired prior to the Board approval. In addition, there is a lack of segregation of duties in processing payrolls, and the District Clerk, who is responsible for certifying payroll, only performs a cursory review of the payroll. Inadequate internal controls over payroll processing increase the chances that errors, as well as fraud, could occur and not be detected in a timely manner

We also found that purchasing controls were not adequate. The purchasing agent was also responsible for processing cash disbursements. These incompatible duties increase the risk that inappropriate purchases could be processed, paid and remain undetected and uncorrected. Our review of payments revealed no exceptions. In addition, District officials did not seek competition when procuring legal, appraisal, architectural, telephone and boiler repair services, totaling approximately $161,361. Without competition and clearly defined and authorized contracts, the District does not have assurance that these services were obtained at the best price.

Finally, District officials have not established sufficient controls over key components of the District's Information Technology (IT) System. The Business Official has not developed and implemented effective access control to the financial software. User rights of Business Office employees, transportation employees, and the District Clerk were not consistent with their duties, weakening the segregation of duties within the financial software application. In addition, the user rights of five former employees were not terminated in a timely manner when the employees left District service. Because of these inadequate internal controls, the District is at an increased risk that unauthorized users could access the system and misuse, lose, or inappropriately modify or disclose 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. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

Introduction

Background

The Highland Falls-Fort Montgomery Central School District (District) is located in the Town of Highland Falls, Orange 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 four schools in operation within the District, with approximately 1,190 students and 235 employees. The District's budgeted expenditures for the 2006-07 fiscal year were approximately $21 million, which were funded primarily with State aid, real property taxes, and grants.

The District clerk is responsible for certifying payroll and managing personnel files, including the obtainment and filing of completed and signed employment eligibility verification forms and fingerprint-supported criminal background checks of employees and contractors who are in direct contact with students. The payroll clerk prepares and distributes payroll.

The District obtains information technology (IT) hardware and software support from the Mid-Hudson Regional Information Center (MHRIC). The District paid MHRIC approximately $427,000 for its services from July 1, 2006 to November 16, 2007. The Director of Technology is responsible for managing the District's IT system. His duties include coordinating services provided by MHRIC; overseeing the District's computer system; and assigning, deleting and changing user access rights to the student information software application.

Objective

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

- Are internal controls over personnel policies and procedures appropriately designed and operating effectively to ensure the District's compliance with applicable laws and regulations and to safeguard assets?

- Are internal controls over payroll appropriately designed and operating effectively to adequately safeguard District assets?

- Are internal controls over purchasing appropriately designed and operating effectively to adequately safeguard District assets?

- Are access controls over the District's IT system designed appropriately and operating effectively to adequately safeguard District's data?

Scope and Methodology

We examined the internal controls over selected financial activities of the District for the period July 1, 2006 to November 16, 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 B 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. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, the Board must approve a corrective action plan that addresses the findings in this report, forward the plan to our office within 90 days, forward a copy of the plan to the Commissioner of Education, and make the plan available for public review in the District Clerk's office. For guidance in preparing the plan of action, the Board should refer to applicable sections in the publication issued by the Office of the State Comptroller entitled *Local Government Management Guide*.

Personnel Policies

Management develops personnel policies to ensure that employees and prospective employees are treated in a manner consistent with existing laws and regulations. Personnel policies and the procedures to implement them protect both the employee and the employer and, by extension, the students within the District. Personnel policies may include specific guidelines for required security clearances and should outline the specific forms that new hires are required to complete. The personnel policy should also prescribe a method to keep track of all the personal information that District officials gather during the hiring process and then maintain during the individual's time of employment with the District. We found the Board had not developed personnel policies and procedures and had not complied with State and Federal laws. As a result, the safety of the students within the District could have been compromised, the District is at risk of incurring civil penalties, and District officials cannot be certain that every employee possesses the necessary educational background.

Fingerprint Clearances

To protect the safety and well-being of students, the Law requires that all employees and independent contractors who have direct contact or are reasonably expected to provide services that involve direct contact with students under the age of 21 must have criminal background checks including fingerprinting. These fingerprint-supported background criminal history checks are required to be filed with the New York State Education Department's Office of School Personnel Review and Accountability (OSPRA). If an individual is arrested subsequent to providing fingerprints to OSPRA, The District will be notified by OSPRA of the name of the arresting agency, the date of arrest, and the court jurisdiction. In order for OSPRA to be able to contact the school district, fingerprint clearances must be obtained in the individual district's name.

The District does not have policies and procedures in place to ensure that background checks are performed and filed with OSPRA for employees and independent contractors who have direct contact with students. We reviewed personnel files of 58 of the 235 current District employees. We also reviewed vendor files for the four consultants who had regular access to students. We found no documentation showing that fingerprint-supported background criminal history checks had been performed or valid clearances had been obtained for 27 of the 58 employees and the four consultants. The personnel clerk could not locate personnel files for two of the 58 employees; therefore, District officials were unable to determine if they had obtained background checks for these employees. In addition, the fingerprint clearances

found on file for three employees were obtained under another district's name. Therefore, in the event that one of these employees is arrested after fingerprint clearance was obtained, OSPRA will not be able to contact the District and inform them of the arrest. As a result of the failure to obtain necessary background checks, there was an increased risk to the welfare of District students.

After we brought the lack of background checks and fingerprinting to their attention, District officials stated they would obtain the necessary clearances.

Employment Eligibility Verification (I-9) Form

The Federal Immigration Reform and Control Act of 1986 (IRCA) requires that U.S. employers verify the employment eligibility status of newly-hired employees. IRCA made it unlawful for employers to knowingly hire or continue to employ unauthorized workers. As a result, all employers are required to have Eligibility Verification (I-9) forms on file for all newly-hired employees to verify their employment eligibility status.

We selected 16 of 235 employees' personnel files for review and we found that the District did not have (I-9) forms on file for nine of the 16 employees. District officials could not provide a reason for the lack of nine I-9 forms on file and said that they were currently working to rectify this situation.

Employers who fail to properly complete, retain, and/or make available for inspection I-9 forms as required by law may face civil monetary penalties of not less than $100 and not more than $1,000 for each employee for whom the Form I-9 was not properly completed, retained, and/or made available. As a result, the District could potentially be liable for a civil penalty for non-compliance.

Personnel Files

To keep track of safety and financial concerns related to District employment, it is important for the District to maintain personnel files that contain all necessary data for each employee. These files should contain emergency contact and address information, payroll withholding information, professional certifications, fingerprint-supported background criminal history checks, and I-9 forms. If there are no personnel files or if the files lack the necessary documentation, the District will not be prepared for emergencies; does not have adequate assurance that its employees are eligible for employment, are compensated at the proper rate, and are qualified; and may face various monetary penalties.

District officials could not locate personnel files for two of the 58 employees selected for fingerprint testing and did not know what happened to the files. Therefore, the District cannot be certain that

these employees possess the necessary educational background and have received clearance to work with the District's students through a criminal background check. In addition, the District does not have the employees' contact information in the event of an emergency.

Recommendations

1. District officials should comply with Education Law requiring a fingerprint-driven background check of all prospective employees and contractors.

2. District official should develop procedures to ensure that the personnel clerk obtains an Eligibility Verification (I-9) form for all new employees.

3. The District Clerk should ensure that complete personnel files are maintained for all District employees.

Payroll

Internal controls over payroll should include written policies and procedures that describe employee responsibilities in preparing and disbursing payroll and should require written Board authorization for personnel changes, salaries, wages and fringe benefits. Board policies, collective bargaining agreements and/or individual employee contracts must stipulate each employee's entitlement to the accrual, use and payment of leave time, including compensatory time. A good system of internal controls over payroll would also include effective managerial oversight and a proper segregation of duties. Where practicable, duties should be separated so that one employee does not control all phases of the payroll process. In a small operation, where complete segregation of duties is not possible, compensating controls such as active supervision and payroll payout audits become important components of an effective internal control system. Failure to establish and adhere to a sound system of internal controls increases the risk that fraud, abuse or errors may occur and go undetected and uncorrected.

The District's internal controls over payroll were inadequate. Personnel changes were made without Board authorization, and there was a lack of segregation of duties over payroll with little or no supervisory review. The District does not perform payroll payout audits, nor does it track and monitor compensatory time.

Board Authorization

Education Law requires Board approval of all staff appointments. In addition, any change to an employee's pay or benefits that is not part of a signed collective bargaining agreement requires Board authorization, which must be documented in the Board minutes. The District's Human Resources Department should then prepare documentation authorizing the Payroll Department to execute the respective changes. Without such authorization, payroll personnel should not execute any changes to the payroll. Furthermore, any special services for which employees are to be paid additional compensation should be considered a change to payroll and require the same level of authorization as the hiring of new employees.

We selected 29 of the District's 235 employees to determine if the Board authorized their salaries and payments were made according to their contracts. We found no documentation to show that the Board authorized the appointments of 13 summer employees hired as custodians who received a total of $27,945. In addition, three employees were hired by the District prior to the Board resolution authorizing them to work for the District. These employees were

paid, and payroll changes were made without Board authorization. The Buildings and Grounds Superintendent stated that the former Superintendent authorized him to hire the employees without Board approval.

When individuals are allowed to work without the Board's approval or are allowed to work prior to Board approval, the District is at risk of employing individuals that may not be qualified for their respective positions. Additionally, when individuals assume the responsibilities of a position prior to an official appointment, there is a risk to the individual that the Board may not subsequently approve his or her hire.

Segregation of Duties

Good internal controls require payroll duties to be segregated and computer access granted based upon job responsibility to ensure that no employee controls all phases of the payroll cycle and that the work performed by one individual is verified in the normal course of another employee's regular duties. If this is not feasible, District officials should consider implementing mitigating controls such as having someone independent of the payroll process perform a review of completed payroll records. At a minimum, the review should include random checks to verify that payrolls are based on actual hours or days worked and verify that the Board authorized the hourly rates or annual salaries used, a comparison of net payrolls to payroll journals, and an assessment of payrolls for reasonableness.

The District's internal controls over payroll transactions were inadequate. District officials did not develop adequate written policies for payroll processing or for certifying the payroll and there was a lack of segregation of duties over payroll processing. The payroll clerk was responsible for adding new employees into the computerized payroll system, inputting and updating salaries, inputting bi-weekly payroll information, and distributing the payroll checks. The only mitigating control present is the certification of the payroll by the District Clerk. However, we determined that the District Clerk performs a cursory review of the payroll. She also does not review payroll changes to make sure that they are entered per Board authorization and does not review overtime or hourly payments to make sure they are authorized. She does not receive payroll reports to make sure that payments are proper. Because the District Clerk did not perform an adequate review of the payroll, the certification process does not significantly reduce the risk associated with the inadequate segregation of duties. As a result, unauthorized payroll transactions could be initiated and processed without a timely detection and correction.

We selected 19 of the 214 payroll changes made during July, September, and November of 2007 to determine if they were made according

to Board authorization. Our testing did not reveal any exceptions. However, when internal controls over payroll are not appropriately designed and/or are not operating effectively, it increases the chances that errors, as well as fraud, could occur and not be detected in a timely manner.

Payroll Payout Audit

Random and periodic payroll payout audits help reduce the risk of fraud and abuse of District funds. An employee not connected with the payroll process should periodically perform a payroll payout audit. A payroll payout audit entails personally handing out each paycheck or remittance advice (for direct deposits) to the appropriate individual. The employee signs for the paycheck or remittance advice when he or she receives it, and provides identification when necessary to verify his or her identity. This process validates the existence of all employees receiving pay.

The District does not perform payroll payout audits to ensure that payroll disbursements are made to only bona fide employees. Given the lack of segregation of payroll duties, the lack of a payroll payout audit increases the risk that inappropriate payroll transactions could be initiated and not be detected.

Compensatory Time

Compensatory time off is paid leave which is earned and accrued by an employee in lieu of immediate cash payment for overtime work. An employee who has accrued compensatory time off is paid for the unused compensatory time upon termination of employment. School districts can place limits on the accrual or payment of compensatory time provided a policy is created and clearly communicated to employees in advance. For example, districts may require employees to take accumulated compensatory time within a specified time frame or require that a certain amount of accrued hours above a specified limit be paid in cash. Good internal controls require that the District adopt policies and procedures that address the amount of compensatory time an employee can earn, how it can be used and how it will be authorized, documented, and monitored.

The District does not have comprehensive policies and procedures for compensatory time and has not placed any limits on the amount of compensatory time that can be accrued. If employees with significant compensatory balances decide to leave the District's services, the financial impact could be significant. For example, as of February 2008, 23 District employees had accrued 259.25 hours of compensatory time totaling approximately $46,000. Because compensatory time represents a District cost that is not funded through the budget, and the District is currently operating on a contingency budget, it is vital that the District develop and implement adequate policies and procedures to monitor compensatory balances.

Recommendations

4. The Board should properly authorize and document all employment approvals.

5. District officials should establish policies and procedures for payroll processing describing employee responsibilities and assigning duties so that incompatible functions are segregated. If segregation of duties is not possible, District officials should establish mitigating controls such as enhanced monitoring of payroll transactions.

6. The payroll certifying agent should review final payrolls to verify that they are based on actual hours or days worked, or authorized leave time; verify that the hourly rates or annual salaries used were authorized; compare net payroll checks to the payroll journal and review the payrolls for reasonableness.

7. District officials should review payroll exception reports prior to the certification of the payroll.

8. District officials should periodically perform a payroll payout to ensure that payment is made to only District employees.

9. The Board should adopt policies dealing with compensatory time that address the amount of compensatory time employees are allowed to accrue, when it can be used, who can authorize it and how it will be monitored.

Purchasing

An effective system of controls over purchasing and good management practices require, whenever applicable, the use of competition such as bids, requests for proposals (RFPs) and quotes to procure goods and services. Good controls also include the segregation of duties to ensure that no one individual controls most or all phases of a transaction, such as requesting, authorizing, receiving, processing for payment and issuing checks; and that the work of one employee is independently verified in the course of another employee's regular duties. If it is not practical to segregate duties, District management is responsible for establishing compensating controls such as independent reviews by supervisory personnel.

The District has not established adequate internal controls over purchasing to ensure that District assets are properly safeguarded. District officials have not segregated the duties of the purchasing agent, who also is the District Treasurer. In addition, District officials did not always advertise for bids when required or solicit competitive proposals when purchasing professional services.

Segregation of Duties

Proper internal controls normally rely on the separation of various duties so that one person does not control a transaction from beginning to end, such as from authorizing a purchase through issuing a check for payment. If duties cannot be properly separated, other compensating controls must be put into place to reduce the risk that errors or irregularities could occur and not be detected and corrected. Such compensating controls would consist of reviews of activities and transactions by supervisory personnel, such as the Superintendent or Board members.

The District's purchasing agent's job duties are not adequately segregated. The purchasing agent authorizes purchase orders and also processes cash disbursements. In addition, the purchasing agent is also the Treasurer and is authorized to sign District checks with no oversight. An employee with these conflicting duties could request and authorize inappropriate purchases, receive goods, process the payments for the purchases, and issue checks to vendors without detection.

Because of this internal control weakness, we reviewed the vendor history accounts, and any disbursements that were made directly to the purchasing agent. We reviewed 33 payments made to the purchasing agent totaling $7,291 during our audit period and found no exceptions. Although our audit testing did not disclose errors or

irregularities, the performance of these incompatible duties increases the risk that inappropriate purchases could be initiated and remain undetected and uncorrected.

Professional Services

The District's policy requires that alternate proposals or quotations for goods and services shall be secured by use of written requests for proposals (RFPs), written quotations, verbal quotations or any other method of procurement when competitive bidding is not required. The District did not solicit RFPs or any other form of competition when procuring certain professional services during the 2006-07 fiscal year.

We reviewed 10 payments made in fiscal year 2006-07 to professional services providers totaling $237,295. In seven of these cases, payments totaling approximately $161,361 were made without the use of RFPs or other form of competition. These included legal services, appraisal services, architectural services, telephone services, heating controls and boiler repair services.

In addition, we noted that five of these contracts totaling $101,870 were signed by the Buildings and Grounds Superintendent, without any Board resolutions authorizing these contracts. Also, the District did not enter into formal contracts with two legal service providers and a property appraisal services provider. The three professional service providers were paid a total of $81,542.

The Buildings and Grounds Superintendent told us that he was not aware that the District should be soliciting RFPs or obtaining other forms of competition, such as quotations, when procuring professional services. Also, he was not aware that he could not sign District contracts. The failure to procure professional services in a manner that assures the prudent and economical use of public moneys could result in the District paying more for these services than necessary. The absence of a contract that stipulates the rights and responsibilities of all parties could impair the District's ability to monitor the intended purpose of the work performed and to ensure that related payments are reasonable and appropriate.

Competitive Bids

The purpose of obtaining bids is to encourage competition for the purchase of supplies, equipment, and services which will be paid for with public funds. The appropriate use of competition provides taxpayers with the greatest assurance that goods and services are procured in the most prudent and economical manner. The Board developed a procurement policy to help ensure that the District purchases materials, supplies and equipment at the best prices, in compliance with all applicable Board and legal requirements. Both the District's policy and General Municipal Law (GML) require

purchases of goods in excess of $10,000 ($20,000 for public works) to be competitively bid.

We reviewed the District's vendor history report for our audit period and judgmentally selected a sample of seven vendors who received payments in excess of $10,000 to determine if the purchasing agent adhered to the District's procurement policy and solicited bids when purchasing these goods. The District paid these seven vendors $212,104. The purchasing agent did not seek competitive bids for one of the seven purchases. This vendor was paid a total of $28,300 for asphalt and paving services. In addition, the District did not enter into a formal contract with the vendor and the Board did not pass a Board resolution authorizing this purchase. As a result, there is no assurance that the District is obtaining goods and services in a prudent and economical manner, and the District could pay more than necessary.

Recommendations

10. District officials should properly segregate the purchasing agent's duties. If proper segregation is not possible, officials should implement compensating controls, such as enhanced review of the purchasing agent's work.

11. District officials should procure professional services in accordance with General Municipal Law and the Board's adopted policy.

12. District officials should obtain competitive bids for purchases over $10,000 as required by General Municipal Law and District policy.

Information Technology

The District's IT system is a valuable and essential part of the District's operations, used to provide computer education, access the Internet, communicate by electronic mail (email), store student data, and maintain financial records. The potential consequences of a failure of the IT system range from inconvenient to severe; even small disruptions in processing can require extensive time and effort to evaluate and repair. Accordingly, District officials are responsible for establishing internal controls over the IT system to ensure that District assets are protected against waste, loss, and misuse. Such controls should address:

- User Access Rights — Restriction and monitoring of users' access to the IT system through secure passwords, system "lock-out" protection, appropriate restriction of access rights based on employees' job responsibilities, and policies and procedures for establishing and modifying user accounts.

- Change Notification — A system that creates a report whenever any changes are made to user access rights.

- Disaster Recovery — A formal disaster prevention and recovery plan, including contingency procedures, to minimize disruption and/or resume critical operations in the event of a system failure.

- Risk Management — An ongoing risk management process to identify, measure, monitor, and address potential risk from contractual arrangements with outside vendors, and classification of the District's data according to the level of risk.

The District spent approximately $427,000 during the 2006-07 fiscal year for IT-related services provided by MHRIC. Specifically, the District contracted with the MHRIC to provide security for all networks and software applications, perform data backups and warehousing, and provide disaster recovery services. Given the MHRIC's involvement in and access to the District's IT system, District officials have a fundamental responsibility for monitoring all work performed by the MHRIC to ensure that services are provided as contracted and the District's IT system and data are adequately safeguarded.

District management has not established sufficient internal controls over the key components of the District's IT system. As a result, the

District's IT system and data are exposed to potential misuse, loss, or improper disclosure, increasing the risk that the District could incur costly disruption of its critical operations.

User Rights/Segregation of Duties

To ensure that adequate internal controls exist, user rights within the computer software applications should be assigned to staff based on their job responsibilities. Limiting user rights provides reasonable assurance that computer resources are protected from unauthorized use or modifications.

Three Business Office employees, two Transportation Department employees and the District Clerk had access to aspects of the accounting system that were not required as part of their job functions. This access resulted in inadequate segregation of duties within the IT environment. For example, the payroll clerk had user rights that allowed her to record cash receipts, generate cash disbursements and make budget transfers. The accounts receivable clerk had the ability to create cash disbursements, budget transfers, and vendor accounts. Also, the Business Official had user rights to access cash receipts. In addition, she was the financial system's administrator and, therefore, she had the ability to add, delete, and change her own access rights.[1] Because the Business Official is significantly involved in financial transactions, she should not have the ability to control access to the system and determine how the system works. The Business Official should have only the rights she needs to perform her job duties. Prior to the end of the fieldwork, we informed District officials of this internal control weakness, and they rectified the situation by transferring the administrative rights for the financial software to the Director of Technology.

Because of these weaknesses, we examined all payments, including payroll items, totaling approximately $191,000, made to the payroll clerk, accounts receivable clerk, and Business Official for our audit period. We found no exceptions with these payments. However, weak access controls diminish the reliability of computerized data and increase the risk of inappropriate modification or disclosure of data and the loss of District assets.

Change Notification

A good system of access controls requires that a list of authorized users with their respective specific needs, and any modifications, be approved by a District manager and directly communicated in writing to the Director of Technology. A formal process for transmitting these

[1] We were informed by the Business Official that she was not aware that she had administrative rights to the financial application. She also stated that the application vendor set all access rights to the financial application.

authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstanding. The Director of Technology should review authorizations for new or modified access privileges and discuss any questionable authorizations with the authorizing official. Approved authorizations should be kept on file. The Director of Technology should be notified immediately when an employee is terminated or is no longer authorized to access the District IT system. Notification may be provided by the Human Resources Department or by others, but policies should be in place that clearly assign responsibility for such notifications. Employees who are terminated or transferred to different jobs and who continue to have access to critical or sensitive resources pose a major threat to the organization.

District officials have not adopted policies and procedures to assign responsibility for the financial software system and for instituting a process to add, change or deactivate user accounts. The Business Official was not aware that she was the District's financial software system administrator; therefore, there was no process for adding, deleting and changing access rights to the financial software system. The Director of Technology derives his authorization to add and delete employees' access to the financial software system from the Board's agenda. Throughout the year, the Director of Technology reviews Board agendas and authorizes the computer technician to add, delete or change access rights in the student information software application and financial software system.

The District did not deactivate the access rights for five of 14 employees who left District employment during our audit period. Four employees continued to have access to the student's information software from eight days to approximately four months after they left District service. District officials did not terminate a fifth employee's access to the financial system in a timely manner. According to District records, this employee left the District on July 27, 2007 but the District did not terminate his access to the financial system until January 7, 2008. The failure to establish policies and procedures to limit user access increases the risk that unauthorized users could inappropriately gain access to a system and change, destroy or manipulate data and computerized assets.

Disaster Recovery

A system of strong internal controls includes a disaster recovery plan to address the potential loss of computer equipment and data, as well as procedures for recovery in the event of an actual loss. A disaster recovery plan includes precautions to minimize the effects of a disaster so that the District can maintain or quickly resume mission critical functions. Typically, disaster recovery planning requires an analysis of business processes and continuity needs and may also

include disaster prevention. If the District employs a third party for IT services, District officials are responsible for ensuring that the service provider safeguards the District from potential losses in the event of a disaster. Contracts with third parties must clearly specify the service provider's responsibilities for system backup and protection, including equipment, programs, and data files; maintenance and periodic testing of a disaster recovery plan, and of the contingency operating procedures to follow if a disaster occurs; and communication of those test results to the District. Third-party contracts should also include business recovery timeframes that meet the District's operational requirements.

District officials have not developed a disaster recovery plan or contingency operating procedures, nor has the MHRIC done so. Although District officials stated that the MHRIC is responsible for disaster recovery, the District's contract with the MHRIC does not require the MHRIC to develop a disaster recovery plan or contingency procedures. Further, the contract does not require the MHRIC to test the disaster recovery plan and contingency procedures regularly and provide the results to the District.

These deficiencies place the District at risk of losing important financial data and incurring serious interruption to District operations, such as not being able to process checks to pay vendors or employees. Because it lacks a disaster recovery plan and does not require the MHRIC to have adequate contingency procedures in place, the District may not be able to recover its data and/or promptly resume operations should a disaster occur.

Risk Management

Risk management is the process of identifying, measuring, and monitoring risk so that appropriate action can be taken to minimize that risk. The pervasive use and complexity of a school district's computerized applications can produce internal control risks such as unauthorized access to data, unauthorized changes to master files, and the potential loss or misuse of data. District officials are responsible for evaluating, overseeing, and addressing the risk related to its IT system and processes, including the risk arising from contractual relationships with IT service providers. An effective risk management process requires that a district's management and board establish risk-based requirements in contracting with IT service providers; continuously monitor the nature and level of risk to identify and evaluate changes in risk from the initial assessment; and ensure that procedures, roles and responsibilities, and reporting mechanisms are clearly established and documented.

District management has not assessed the risk associated with contracting some IT related functions to the MHRIC and has not

instituted a system to adequately safeguard computer and network resources. The District contracted with the MHRIC to provide firewall protection and monitoring, and data back-up. Firewalls filter internet traffic to mitigate risks and losses associated with security threats to the network and information systems. Data backups that are performed frequently and restored occasionally ensure that data can be restored in the event of a disaster. The Director of Technology told us that he was not aware of how the MHRIC maintained or monitored the District's firewalls. He was also not aware of how and when data backups were performed, and how many generations of backups the MHRIC maintained for the District. In addition, he was not aware if the MHRIC occasionally restored the District's data backups to ensure data could be restored in the event of a disaster.

Contracting for IT services does not reduce the fundamental risks associated with IT. Risks such as loss of funds, damage to reputation, improper disclosure of information, and regulatory action remain with the District. As such, the District needs to evaluate the risk associated with outsourcing the IT function and address those risks appropriately.

Data Classification

The classification of a district's computerized data assigns levels of protection to help minimize the risk of access and manipulation by multiple users. Accordingly, the most critical data should be classified so as to be subject to the strongest protective controls and accessible only to those users whose level of responsibility requires access to it. The classification definitions should flow directly from the results of an effective risk assessment process that identifies threats, vulnerabilities, and potential negative effects of disclosing confidential data, or of failing to protect the integrity of data supporting critical transactions or decisions. District officials are responsible for developing and enforcing policies and procedures that specify classification categories, and for defining the related criteria on which the classification levels are based. It is essential that all classifications be reviewed and approved by a senior District official, maintained on file, and periodically reviewed to ensure that they reflect current condition.

Because the District did not have a risk management process, District officials did not develop policies for classifying data according to risk and for documenting the classification. Therefore, the District's sensitive and confidential data is at an increased risk of inappropriate use or modification, loss, or improper disclosure.

Remote Access

Remote access is the ability to access the District's computer system from the internet or other external source. Remote access should be controlled, monitored, and tracked so that only authorized

individuals are allowed to access the District's computer system or to retrieve data from it. The District has not implemented policies and established written procedures that address how remote access is granted, who is given remote access, and how remote access to the District's networked computer system and financial computer data is monitored, tracked and controlled.

The Director of Technology informed us that all District employees are granted remote access to the District Network and the Business Official has access to the financial computer system from home. However, the District does not have a process in place that documents authorization and provides for monitoring and tracking remote access. As a result of this weakness, District data is at increased risk of being manipulated which could result in errors and irregularities occurring and not being detected.

Recommendations

13. District officials should limit the ability of system users to access software and data based on the relevance of their job duties.

14. District officials should institute a procedure to deactivate user accounts as soon as employees leave District service or change user accounts as soon as employees are assigned new responsibilities.

15. District officials should revise the contract with the MHRIC to include disaster recovery or should consider developing their own disaster recovery plan.

16. District officials should adopt policies and procedures for analyzing the risk associated with contracting for certain IT functions and for addressing those risks.

17. The Director of Technology should institute a process where data is classified according to risk and is documented.

18. District officials should adopt policies and procedures that address remote access to the District's computer system.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

HIGHLAND FALLS – FORT MONTGOMERY
CENTRAL SCHOOL DISTRICT
Post Office Box 287, Highland Falls, New York 10928

A Place Where Talents Are Developed

August 22, 2008

[redacted]
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Dear [redacted]:

This letter shall serve as the District's official response to the New York State Office of the State Comptroller's draft audit report reviewed with the District in an exit conference on August 1, 2008. During this exit conference we discussed the written findings and recommendations contained in the report. As the new incoming Superintendent of Schools, I wish to thank your representative for taking additional time to review the process and documents with us in such a thorough manner. Our new Business Official and I will work with our administrative team to develop the corrective action plan.

The Board of Education views the audit as both a valuable tool and important opportunity to improve our stewardship of District resources and management of our schools. Under the previous administration, the District has already implemented some of the recommendations presented in the report. In general, the District concurs with the findings of the audit report and we will work diligently to implement the necessary changes.

The District would like to thank the Office of the State Comptroller for identifying areas for improvement. Our staff has shared with me that your staff demonstrated exemplary professionalism during the audit. They exhibited a cooperative attitude and professional demeanor that enabled the audit to run smoothly with minimal impact on operations.

Development and implementation of the District's corrective action plan will strengthen our internal controls and provide a heighten level of fiscal accountability to the community.

District Response to Audit Report Findings

Personnel Policies

The District has implemented procedures to insure all employees and contractors having contact with students undergo criminal background checks and fingerprinting as prescribed by law. The District has undertaken a systematic review of all personnel records to insure compliance with this mandate and complete personnel records, including employment eligibility documentation.

Payroll

All staff appointments, including temporary summer staff, will only commence with Board authorization. Employees shall not work for the District before this authorization has occurred.

Adequate segregation of duties ensures that no employee controls all phases of a financial transaction. In a small office, however, segregation of duties is more challenging and logistically difficult to achieve. Staff in the District are called upon to "wear many hats" and hiring new employees is not always financially possible or operationally justified.

Based on your audit findings the District has introduced greater segregation of duties in the payroll process by assigning the district clerk the task and system access rights for entering employee records and salary data while the District payroll clerk processes payroll. This insures that two people are involved in the payroll process decreasing the internal control risks. It is important to note that audit testing revealed no problems or exceptions with payroll changes made during a sample three-month period.

The district has adopted the recommendation for periodic payroll payout audits whereby employees must sign for paychecks and provide identification to show proof of their identity. Someone other than the payroll clerk who is responsible for processing and printing payroll checks will conduct these audits.

The District will consider how best to revise and clarify policies and procedures concerning compensatory time including a limit on the time that may be accrued.

Purchasing

The audit found segregation of duties was lacking in the following areas: purchasing, cash disbursements, and the duties of the treasurer. In the future, greater segregation of duties will be introduced enabling cash disbursements to be performed by an accounts payable clerk not the business official.

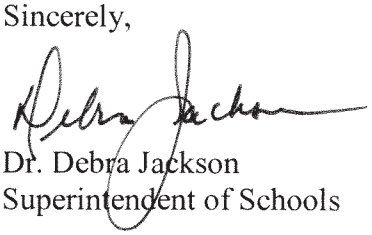
The District will undertake a comprehensive review of procurement activities for professional services including the renewed use of Request for Proposal (RFP) documents to ensure adequate competition. Furthermore, the District will endeavor to enter into written contracts with all professional service providers and have these agreements authorized by the Board. Competitive bidding will be used in full compliance with General Municipal Law.

Information Technology

The District has addressed several of the findings in the area of information technology including instituting a systematic review of user access rights with a provision to limit access only to data and technology systems needed to carry out job functions. A change notification system has also been developed whereby all user account changes are recorded and maintained. The work has begun to improve and document disaster recovery procedures. Finally, the District is about to undergo a significant enhancement to our remote access system utilizing virtual private network technology which will reduce the risk of unauthorized access.

In closing, I would like to thank you for the opportunity to respond to the audit report and for your hard work to improve the fiscal management of schools.

Sincerely,



Dr. Debra Jackson
Superintendent of Schools

APPENDIX B

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 personnel policies, payroll, purchasing, and information technology for further audit testing.

To accomplish our audit objective, our procedures included the following:

- Interviewing key employees in the District
- Testing payroll changes, overtime and compensatory time processes
- Testing purchases and the purchasing process
- Testing the IT system
- Reviewing the District's contract with the Mid Hudson Regional Informational Center (MHRIC) to determine what services they were responsible for providing to the District.
- Examining employees' personnel files, collective bargaining agreements and individual contracts, salary notification letters, and Board minutes in an effort to determine if employees with excessive access rights were properly authorized and paid according to contract or Board resolution
- Reviewing Vendor History report and testing vendor payments.

We conducted this 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 C

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 D

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