



# Millbrook Central School District Internal Controls Over Cash Receipts and Disbursements and Information Technology

Report of Examination

Period Covered:

July 1, 2006 — September 17, 2007

2008M-26



Thomas P. DiNapoli

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	3
<b>EXECUTIVE SUMMARY</b>	5
<b>INTRODUCTION</b>	7
Background	7
Objective	7
Scope and Methodology	7
Comments of District Officials and Corrective Action	8
<b>CASH RECEIPTS AND DISBURSEMENTS</b>	9
Segregation of Duties	9
Wire Transfers	10
Electronic Signature Disk	11
Audit of Claims	11
Recommendations	12
<b>INFORMATION TECHNOLOGY</b>	13
Access Controls	13
Data Storage and Transport	16
Equipment Disposal	17
Data Backup and Disaster Recovery	17
Recommendations	18
<b>APPENDIX A</b> Response From District Officials	20
<b>APPENDIX B</b> Audit Methodology and Standards	25
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	27
<b>APPENDIX D</b> Local Regional Office Listing	28



# State of New York Office of the State Comptroller

---

---

## **Division of Local Government and School Accountability**

June 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 Millbrook Central School District, entitled *Internal Controls Over Cash Receipts and Disbursements and Information Technology*. 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 Millbrook 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.

The Treasurer is primarily responsible for the receipt and disbursement of all District cash. The Treasurer is also generally responsible for the District's day-to-day accounting functions. The Board appointed a claims auditor to examine and approve all District claims prior to payment. The technology coordinator reports to the Superintendent and assists District staff with purchasing and integrating the District's hardware and software.

### **Scope and Objective**

The objective of our audit was to evaluate internal controls over cash receipts and disbursements and information technology for the period July 1, 2006 to September 17, 2007. Our audit addressed the following related questions:

- Are internal controls over cash receipts and disbursements appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over information technology (IT) appropriately designed to adequately safeguard District assets?

### **Audit Results**

We found weaknesses in internal controls over cash receipts and disbursements. The Treasurer's duties – which included receiving, recording, and disbursing District moneys, performing electronic funds transfers, preparing journal entries of cash transactions, and reconciling the bank statements – were not adequately segregated. While our tests of cash receipt records and disbursements did not identify any material errors or improper payments, having the key financial transactions controlled by one individual without sufficient oversight places the District at an increased risk of errors or irregularities occurring without being detected.

The District's controls over wire transfers were inadequate because the Treasurer could transfer funds based on only verbal authorization by the Business Administrator. The Treasurer performed three

wire transfers, totaling approximately \$2,787,000, from an investment trust fund to the construction fund without the written authorization of the Business Administrator. In the absence of written authorization, wire transfers cannot be properly reconciled to the bank statements, and the District is at an increased risk that inaccurate or improper wire transfers could occur without being detected. The Treasurer also allowed the accounts payable clerk and the payroll clerk to apply her signature to District checks when she was not present. Although we found no exceptions in the checks issued, this weakness in controls over the Treasurer's signature disk creates an increased risk that errors or irregularities could occur without being detected and corrected.

Our review of controls over the audit and approval of claims found that 22 of 50 disbursements reviewed, totaling approximately \$151,000, were made before the claims auditor properly audited the corresponding claims. Although we found no erroneous or improper payments, the payment of claims without prior audit and approval is a violation of Education Law. As a result, the District is at risk of making improper payments and District officials do not have assurance that District moneys were spent on necessary goods and services that were actually received.

The District also did not have policies and procedures to adequately safeguard computerized data and assets. The District's physical and electronic access controls were inadequate. District and non-District personnel had unsupervised access to the server room, and a District vendor was allowed unrestricted remote access to the accounting software. District officials assigned comprehensive system administrator rights to the District's teachers for assigned laptops and did not monitor their activities regularly. Additionally, District officials assigned the monitoring of the financial system's audit logs (which can record employees' system activities) to the Treasurer, who performed key financial duties, instead of assigning this responsibility to an official independent of Business Office operations. As a result of these weaknesses in access controls, the District is at an increased risk of deliberate or inadvertent loss, damage, or misuse of its computerized equipment and data.

Additionally, the District had no procedures in place to ensure the secure storage and transport of sensitive information on portable "thumb" drives used by employees, and inadequate plans for properly removing the information residing on computers and media that are discarded or transferred to another use. Although District personnel performed system backups every day, District officials did not develop a secure backup plan for the District's financial and student data. Lastly, the District does not have a formal disaster recovery plan to guide personnel in minimizing the effects of a potential disaster and to provide procedures for recovering lost data. Without such controls, the District is susceptible to the potentially costly disruption of its critical operations in the event of a disaster or the intentional or unintentional actions of employees.

### **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 plan to initiate corrective action.

# Introduction

## Background

The Millbrook Central School District (District) is located in the Towns of Washington, Union Vale, Clinton, LaGrange, Stanford, and Pleasant Valley, in Dutchess 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.

The Treasurer is responsible for the receipt and disbursement of all District cash. The Treasurer is also generally responsible for much of the District's day-to-day accounting functions. The Board appointed a claims auditor, who is responsible for reviewing and approving each claim prior to payment. The technology coordinator reports to the Superintendent and assists District staff in purchasing and integrating the District's computer hardware and software.

There are four schools in operation within the District, with approximately 1,245 students and 180 employees. The District's budgeted expenditures for the 2007-08 fiscal year are \$22,177,563 and are funded primarily with State aid, real property taxes, and grants.

## Objective

The objective of our audit was to evaluate internal controls over cash receipts and disbursements and information technology. Our audit addressed the following related questions:

- Are internal controls over cash receipts and disbursements appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over information technology appropriately designed to adequately safeguard District assets?

## Scope and Methodology

We examined internal controls over cash receipts and disbursements and information technology for the period July 1, 2006 to September 17, 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 plan 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*.

## Cash Receipts and Disbursements

District officials are responsible for establishing internal controls to ensure that the District's cash receipts are adequately safeguarded and that cash disbursements are properly authorized. Such controls include policies and procedures for an adequate segregation of duties, documented authorization of wire transfers, supervised use of electronic signatures, and the audit and approval of all District claims prior to payment.

Although the District had a policy manual, there were limited District-specific procedures available to guide District personnel in the performance of their specific duties.<sup>1</sup> The Treasurer's cash receipt, accounting, disbursement, and reconciliation duties were not adequately segregated, and compensating controls were not sufficient. The Treasurer also performed wire transfers without written authorization, and allowed her electronic signature disk to be used by staff when she was not present. Lastly, District officials allowed the Treasurer to pay claims that were not properly audited and approved in advance by the District's claims auditor. Although we found no exceptions, these weaknesses in internal controls place the District at an increased risk of erroneous or improper payments.

### Segregation of Duties

District officials are responsible for establishing an effective system of internal controls over cash receipts and disbursements. Such controls ensure the separation of duties so that no single individual controls all phases of a transaction. When it is not practical to segregate duties, District officials should establish compensating controls such as having other administrative staff periodically review the work in question, rotating duties among staff members, and/or requiring periodic vacations.

The Treasurer's responsibilities include opening mail, receiving cash, recording receipts, preparing journal entries, making bank deposits, signing all checks, making cash and wire transfers, receiving unopened bank statements and cancelled checks from the bank, and performing bank reconciliations. Although the Treasurer provided the Board with a monthly reconciliation and a list of outstanding checks, we found no evidence that the Board or any other independent District employee compared the bank reconciliation with corresponding records and bank statements to ensure that the bank statements and accounting records were in fact reconciled.

<sup>1</sup> District officials told us they had begun developing written procedures in October 2007.

We tested a sample of 50 payments made by the District throughout the audit period, totaling approximately \$525,400, for evidence that the payments were supported by a proper voucher (invoice), that the expenditures were for valid District purposes, and that the purchased goods or services were received. We also reviewed the District's cash receipt procedures and records and bank reconciliations. Our tests did not identify any material errors or improper payments. However, when one individual controls most or all of the transactions related to receiving and recording cash, making wire transfers and bank deposits, disbursing District moneys, and reconciling the bank statements, there is an increased risk that inappropriate transactions could be initiated and not be detected.

## Wire Transfers

Wire transfers provide a means of direct access to the moneys held in the District's name. Appropriate controls over wire transfer activity include management authorization of a transaction before the transaction is initiated; itemized documentation to support the purpose, source, destination, and amount of the transaction; and documentation to appropriately account for and record the transaction. District officials should also segregate the duties involved in wire transfer activity. If the same individual both initiates wire transfers and performs bank account reconciliations, the individual could make an error that may not be detected, or conceal an unauthorized transfer. If these duties cannot be segregated, someone independent of the wire transfer and bank reconciliation functions should review and approve all wire transfers, in writing, before they are performed. Such a compensating control would allow actual wire-transfer dates, amounts, and destinations to be compared to authorizations to detect any inappropriate transactions.

The District's standard practice required the Business Administrator to approve wire transfers either verbally or in writing. However, without written authorization, there is no evidence that all wire transfers have been independently reviewed and approved, and no way to perform the subsequent reconciliation of bank activity to authorizations. To test for proper authorization and approval of interfund transfers, we reviewed eight wire transfers totaling \$3,361,819 made in September through November 2006 and found that the Treasurer had not obtained the written authorization of the Business Administrator before making three of the transfers totaling \$2,787,166.<sup>2</sup> Although the transfers were for legitimate District purposes, this control weakness places the District at an increased risk of improper wire transfers occurring without being detected.

---

<sup>2</sup> The three transfers were from an investment trust fund to the construction fund.

## **Electronic Signature Disk**

An electronic signature affixed to District check stock provides access to moneys in the corresponding bank account. As the District official responsible for signing checks, the Treasurer must ensure that her signature is not used to make payments that have not been approved. Education Law requires the actual or a facsimile of the Treasurer's signature to be applied to District checks either by the Treasurer or under the Treasurer's direct supervision. The District's disbursements from the general fund averaged slightly over \$4 million per month in the 2006-07 fiscal year.

We identified deficiencies in the Treasurer's oversight of the check signing function. Although the disk containing the Treasurer's signature and the press-numbered blank check stock were kept in separate locked cabinets in the Treasurer's office, the accounts payable clerk used the Treasurer's signature disk to apply the Treasurer's signature to the checks without the Treasurer being present. In addition, the Treasurer allowed other District personnel access to, and use of, the electronic signature disk when she was not present.

We tested 50 claims totaling approximately \$525,400 (referenced under "Segregation of Duties" above) and found no evidence of unauthorized disbursements. However, because the Treasurer does not directly supervise the use of her signature disk, the District is at an increased risk of unauthorized disbursements, and District officials do not have assurance that signed checks are produced for valid District purposes and in the correct amounts.

## **Audit of Claims**

Education Law stipulates that all claims against the District, except for salaries of employees and other rare exceptions,<sup>3</sup> shall not be paid unless an itemized voucher, approved by the officer initiating the claim, is presented to the Board for audit and approval. The Board may appoint a claims auditor to assume its powers and duties of auditing and approving each claim. If the Board appoints a claims auditor, that individual must determine whether each claim is properly authorized and accurate; whether the purchase represents a valid District expense for goods or services; and whether the goods or services were actually received. Audited claims should be included on warrants certified by the claims auditor, and the Treasurer may not sign a check for payment unless the claims auditor has reviewed and certified each claim authorizing the Treasurer to pay it.

The District's claims auditor reviewed claims once a month, before the Board's monthly business meeting. If an item required payment

---

<sup>3</sup> Education Law authorizes the Board to authorize by resolution the payment of certain claims in advance of audit, including those for public utility services, postage and freight, and express charges. All such claims must, however, still be presented for audit subsequent to being paid.

after the current month's claims audit but before the next scheduled claims audit, the check was prepared, signed by the Treasurer, and sent to the vendor. Such claims were then audited before the next month's business meeting. This delay in the audit of claims circumvents key controls and may result in the incorrect or improper payment of claims.

To determine if this internal control weakness allowed errors or questionable payments to occur, we selected a judgmental sample of 50 claims paid throughout the audit period, totaling approximately \$525,400, and examined the supporting documentation for accuracy and propriety. Twenty-two of these claims, totaling \$151,124,<sup>4</sup> were not audited prior to the Treasurer signing and issuing the check. None of the claims were for items that could legitimately be paid prior to audit. While we found no improper payments, without the prior audit and approval of claims, the District is at an increased risk of making incorrect or improper payments. Further, if a subsequent audit of claims were to reveal that incorrect or improper payments were made, the District would then have to recoup the payment from the vendor.

## Recommendations

1. District officials should segregate the Treasurer's duties. If incompatible duties cannot be segregated, officials should establish compensating controls such as requiring the Business Administrator to oversee the duties of the Treasurer's office.
2. District officials should implement procedures to ensure that the Business Administrator provides written authorizations before the Treasurer makes wire transfers. The Business Administrator should also reconcile these authorizations to actual wire transfers each month.
3. The Treasurer should ensure that her electronic signature is used only on checks for approved payments, and her signature disk is used only by the Treasurer herself or by authorized staff under the Treasurer's direct supervision.
4. District officials should ensure that the claims auditor audits and approves all claims prior to payment.

---

<sup>4</sup> These claims were for a variety of goods and services. The most significant claims included a claim for insurance of approximately \$70,500, a claim for programs for handicapped children of \$16,000, and two claims of approximately \$16,000 and \$11,000 paid to software vendors.

## Information Technology

The District's IT system is a valuable and essential part of District operations, used for computer education, access to the Internet, e-mail communication, processing and storing student data, maintaining financial records, and reporting to State and Federal agencies. The pervasive use and complexity of these computerized applications create internal control risks such as unauthorized access to data, unauthorized changes to master files, and the potential loss of data. If the IT system fails, the results could 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 and data to protect District assets against the risk of loss, misuse, or improper disclosure of sensitive data.

District officials can mitigate these risks through a combination of automated and manual controls. Policies and procedures to safeguard the District's IT system and data should address the physical security of IT equipment, remote access privileges granted to software vendors, assignment of system administrator rights, and management review of audit logs to monitor employees' activities on the computer system. Procedures for the secure storage and transport of the District's sensitive information and for the proper deletion of data from obsolete or transferred equipment help to protect District data from corruption or improper use. Lastly, the systematic backup of District data and testing of restoration procedures, combined with a formal disaster recovery plan, are essential controls to help ensure that the District's critical operations resume as quickly and efficiently as possible if there is a disruption of computer processing.

The District did not have adequate policies and procedures to address these issues. District officials did not institute controls to adequately protect the District's computer equipment and data from unauthorized physical and electronic access; to protect sensitive data that is stored on portable drives used by employees, and on computer equipment and media being disposed of; to adequately secure and test backup data; and to develop a disaster recovery plan for the District. As a result of these control weaknesses, the District's IT system and electronic data are susceptible to an increased risk of loss, unauthorized use, or improper disclosure.

### Access Controls

Internal controls over users' access to the IT system provide reasonable assurance that computer resources – which include equipment, data files, application programs, and computer-related

facilities – are adequately safeguarded. Effective access controls include manual and automated measures such as the following:

- Physical security provisions to properly authorize personnel who are allowed access to computer equipment, to ensure that such individuals are supervised or monitored during maintenance activities, and to require access to be recorded in an access log
- Restrictions on remote access (the ability to log onto a network from an off site location), particularly with regard to a software vendor performing system maintenance or updates to the District’s accounting system
- Limiting the number of individuals granted system administrator rights that allow broad authority to install, delete, and modify software files and settings, modify system-generated logs that track user activity, and assign or modify the software access rights of District users
- Routine management review of audit logs (system-generated reports showing users’ computer activity) to help detect unusual or unauthorized transactions.

We found the District’s access controls are insufficient to provide District officials with adequate assurance that the District’s IT system and data are properly safeguarded. As a result, there is an increased risk that District data could be lost or accessed inappropriately.

Physical Security – Maintaining adequate security over District IT assets helps to ensure that the items are protected from loss and are used for their intended purpose. File servers are an integral part of an IT system, and are valuable assets that District officials must protect from intentional or unintentional loss or damage. An effective internal control system restricts physical access to computer resources, such as servers, and helps prevent costly disruptions. Even small disruptions in processing can require extensive time and effort to evaluate and repair.

The District’s network servers reside in a locked wiring closet that also houses the telephone system, the power grids, and the security camera monitor and equipment that are not part of District technology support. Both District and non-District personnel have access to these devices for maintenance. District employees are not accompanied into the server wiring closet, and non-District employees are not always supervised once they have been given access to the server room. Further, the District does not maintain a log of access to the

server rooms. The lack of these security precautions increases the risk of intentional or unintentional damage to the District's IT assets.

Remote Access – Remote access is the ability to log onto a network from off-site locations using a computer, a modem or Internet access, and remote access software. Remote access causes security risks for an otherwise secure network because remote computers, even if physically secure, may be vulnerable to threats from other systems. If remote access capability is allowed to software vendors, the vigilant monitoring of such access helps to preserve the integrity of District systems and data.

The District allowed unrestricted remote access to its accounting software vendor so the vendor could perform software updates. District officials have not established and implemented policies and procedures governing this remote access, which could result in the District's IT resources being compromised. As a result, the District is at risk of unauthorized changes to the system, programs, or data without the knowledge of District officials.

Administrative Rights – Administrative rights allow users to create, delete, and modify files, folders, or settings, including the assignment of users' access rights and the ability to download and install programs. A user with administrative rights (or an unauthorized user who gains access to a system administrator account) can also modify computer-generated log files to cover such actions. Even unintentional changes could cause severe problems for the District. By limiting the number of users having administrative rights – for example, the IT coordinator and a backup person – and providing appropriate oversight of their duties, District officials can significantly reduce the risk of inappropriate changes to the District's network applications and data.

The technology coordinator told us that District teachers (approximately 60 individuals) have operating-system administrative user rights on assigned laptop computers. Additionally, there are no procedures to prevent teachers from downloading and installing software on these computers without the prior knowledge and approval of the technology coordinator. This exposes the District network to potential damage from viruses, "spyware," and other software that may not be properly screened for current technological threats. The laptop computers are also allowed off District premises, further exposing them to unauthorized access. Because the District monitors laptop use only at year-end when recalling the laptops for maintenance, a user with administrative rights could remove evidence of misuse during the year before returning the laptop. The indiscriminate assignment of administrative user rights and the

related lack of controls expose the District's systems and data to an increased risk of loss, corruption, or misuse.

Audit Logs – An adequate system of internal controls over computer-processed data includes policies and procedures regarding the secure and authorized use of computer systems. Such policies and procedures should include the routine production and review of computer-generated reports, such as change reports and audit logs,<sup>5</sup> by management or management's designee to monitor the activity of users who access the District's financial software. These reports help to detect changes that occur in processed data and to identify who made the changes.

Although an update to the District's software in July 2006 provided an audit log report capability, District officials did not use this function until January 2007. At that time, the audit log review was assigned to the Treasurer, who also performed critical functions within the Business Office including the recording, reporting, and reconciling of financial transactions. When audit logs are reviewed by a District official in the Business Office who also records, reports, and reconciles financial transactions, there are increased opportunities for this individual to initiate and conceal unauthorized changes to the District's data without detection and correction.

**Data Storage and Transport** USB "thumb drives" (also known as flash drives, key drives, or jump drives) are compact, portable data storage devices that plug into a computer's external port. Thumb drives offer a cost-effective, convenient method of storing, transporting, and downloading electronic data. However, the ease of use, small size, and minimal technological constraints of these devices create risks that must be assessed and controlled. Thumb drives enable electronic data, including potentially confidential records, to be removed from District premises and subsequently accessed by an unauthorized individual with little difficulty, and can transfer computer viruses to District computers. They are easily concealed – or lost – and require no complex setup procedure to use. Accordingly, it is essential for a District to have a security management program that includes policies and procedures for the secure storage and transport of sensitive information on these auxiliary devices.

The District does not have policies and procedures to guide its employees in the secure use of thumb drives. The District's IT department instructs the staff to copy information from their District-assigned laptop computers to a thumb drive prior to returning

---

<sup>5</sup> Change reports show changes to or deletions of data. Audit logs show when users enter or exit the system, and their activities while logged on.

the laptop at the end of the school year. While District officials encourage the use of thumb drives purchased by employees, the District does not monitor the disposition of the data stored on them. Without adequate controls over the use of these devices, the District is at an increased risk of the retrieval and misuse of sensitive information by unauthorized individuals.

### **Equipment Disposal**

Sensitive information and software must be safeguarded throughout its useful life. Such information must be cleared from computer hard drives, disks, thumb drives, and other equipment and media before they are disposed of or transferred to another use. Organizations should have a plan that clearly describes the organization's security management program and the policies and procedures that support it, including procedures for the secure disposal of sensitive information. If sensitive information is not completely sanitized, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media.

The District has not established policies and procedures regarding the disposal or reassignment of computer equipment and the eradication of the sensitive information stored on those computers and media. The District leases a large portion of its computer equipment from the Dutchess County Board of Cooperative Educational Services (BOCES), and follows BOCES inventory deletion procedures by contacting a third-party vendor for the direct pickup and disposal of the returned equipment. Before surrendering the equipment, District officials do not take any measures to remove sensitive data that may have been stored on hard drives. As a result, the District is at an increased risk of its sensitive and confidential information being retrieved and misused by unauthorized individuals.

### **Data Backup and Disaster Recovery**

An effective internal control system for IT includes a formal disaster recovery plan with policies and procedures to minimize the loss of essential data and to maintain or quickly resume critical operations. Data stored on computers and servers should be backed up (a duplicate copy of information made) on a routine basis so that it can be restored in the event of loss. Periodically, District personnel should verify the integrity of the backup data and test the effectiveness of the restoration process by restoring the data from the backup copy. In addition, the backup data should be stored at a secure offsite location to minimize the risk of loss from a disaster at the server location site.

The District has not prepared and tested a secure backup plan for its financial and student data. Although the Technology Department staff backs up all files every day, the backups are retained in the same room as the servers, which are also accessible to non-technical

District employees and to non-District technicians, until being sent to a nearby District school once a month. Therefore, until such time as they are sent off-site, the backup media are subject to the same risks of loss as the programs and data residing on the servers, and are vulnerable to intentional or unintentional damage or misuse by unauthorized personnel. Further, District personnel do not periodically restore the system and data from the backup tapes, and therefore are unable to verify the integrity of the data and the effectiveness of the restoration process. Lastly, District personnel have no plan to help minimize or prevent the loss of equipment and data, or guidance for implementing data recovery procedures.

As a result of these control weaknesses, the District is at an increased risk of the loss or improper disclosure of its essential computerized data, damage to its IT equipment, and potentially costly disruptions to its business operations.

## Recommendations

5. District officials should protect the District's computerized assets by implementing the following access controls:
  - Require that access to the server room be restricted to only designated individuals. Additionally, access by undesignated District employees should be supervised and documented.
  - Restrict remote access to the accounting software only for updates and support, establish a remote access agreement with outside vendors, and oversee the installation of all software updates.
  - Limit the number of users having operating-system administrative rights and examine available solutions for preventing unauthorized software installation on laptop computers.
  - Identify the financial activities to be tracked and ensure the periodic review of system audit logs by the Business Administrator (or another individual independent of financial operations) for unusual or unauthorized transactions.
6. Establish policies and procedures for the secure storage and transport of sensitive information residing on computer hard drives, portable media, and peripherals, and for the eradication of sensitive data from computer equipment being discarded or transferred to another use.
7. Backup copies of data should be stored at secure and sufficiently remote off site locations, and the integrity of the backups should

be tested periodically by restoring the system data from the backup media.

8. The District should have a formal disaster recovery plan including precautions to minimize the potential effects of a disaster, and procedures for implementing data recovery.

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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



P.O. BOX AA • MILLBROOK, NEW YORK 12545

SUPERINTENDENT OF SCHOOLS 845-677-4200
BUSINESS ADMINISTRATOR 845-677-4201
PUPIL PERSONNEL SERVICES 845-677-4215
DISTRICT CLERK 845-677-4200

ELM DRIVE ELEMENTARY 845-677-4225
ALDEN PLACE ELEMENTARY 845-677-4220
MILLBROOK MIDDLE SCHOOL 845-677-4210
MILLBROOK HIGH SCHOOL 845-677-2510

OFFICE OF THE SUPERINTENDENT

April 28, 2008 (Amended Submission)

To: Office of the State Comptroller

From: Dr. R. Lloyd Jaeger, Superintendent of Schools

Re: District Response to Draft Comptroller's Report

In general terms, our district acknowledges that the draft report provides district staff and the Board of Education with recommendations and strategies which may improve district operations and strengthen controls which safeguard district assets. We wish to further acknowledge and express appreciation for the professional and cooperative manner in which your examiner team interacted with us throughout their work here.

District Responses to Comptroller Observations & Recommendations

Cash Receipts and Disbursements Section

Many of the Comptrollers' Office observations and recommendations will be addressed through the hiring of an additional business office staff member who will enable the district to achieve a greater segregation of duties and cross-training capacity. This Principle Account Clerk (PAC) position has been included in the proposed 2008-09 budget as adopted by the Board of Education for presentation to the voters on May 20, 2008. A tentative job description is enclosed on page 4 of this document.

Table with 2 main columns: Office of State Comptroller (OSC) Observations & Recommendations, and District Response(s). Rows include: No written procedures; Need for more differentiated Segregation of Duties (with sub-points: Rotate/Reassign duties among staff, Treasurer: OSC Observed Current Duties, Open mail).

Receive cash and issue receipts	PAC will backup this duty	
Prepare journals	Function remains with junior accountant	
Bank deposits	PAC- Perform role of Deputy Treasurer	
Sign checks	PAC will backup this duty	
Cash/wire transfers	Business Admin/Super must sign-off	
Bank statements	PAC- Perform role of Deputy Treasurer	
Cancelled checks	Function remains with Treasurer	
Bank reconciliation	PAC- Perform role of Deputy Treasurer	
<b>o Wire Transfers</b>		
Management does not provide documented sign-off on all transfers	Management will sign-off before all transfers (Business Administrator with Superintendent as backup)	
<b>o Electronic Signature Disk</b>		
Not secure - Accounts Payable Clerk is provided access to disk for her use in the absence of the Treasurer	PAC will backup the Treasurer and will have his/her own secure disk.	
<b>o Audit of Claims</b>		
Treasurer should not sign checks until after Claims Auditor has certified them for payment	This procedure was substantially our routine practice as noted in the comptroller's report. It will be our future uniform practice.	
<b>o Specific Recommendations</b>		
1. Segregate Treasurer's duties	On or About 9-01-08	See new PAC duties
2. Business Administrator should sign-off on all wire transfers	This documentation and procedure has been implemented.	
3. Secure the Electronic Signature Disk	PAC will backup the Treasurer and will have his/her own secure disk.	
4. Claims Auditor certify all claims prior to payment	This procedure was substantially our routine practice as noted in the comptroller's report. It will be our future uniform practice.	

### **INFORMATION TECHNOLOGY SECTION**

**Physical Access to Servers:** Access to the server room at the Middle School will be restricted to District staff performing technical support duties only. A log/report will be maintained to document access to the server room by any other District employees or vendors.

**Remote Access to Servers:** Remote access to the financial/accounting software will be disabled by default, and will be enabled each time a request is made by District staff for a vendor to apply a software upgrade or provide technical support. In these instances, remote access will be enabled for a specified period only. A remote access agreement will be drafted by the District, and any outside vendor who provides remote technical support will be required to sign this agreement.

**Laptop Administrative Rights:** All student laptops already have restricted rights to the operating system. Users of these laptops are limited to running software programs from an approved list, and cannot save to or alter the contents of anything on the local drive. Teachers and administrators typically need more rights to their laptop hard drives in order to allow the flexibility needed for classroom use, lesson planning, and record-keeping tasks; however, the District will examine available solutions for preventing unauthorized software from being installed on teacher laptops and administrative use laptops.

**Review of Financial Software Activity Logs:** As of January 2007, the Business Administrator has identified financial activities to be tracked, and is responsible for scheduling periodic reviews of system audit logs for unusual or unauthorized transactions.

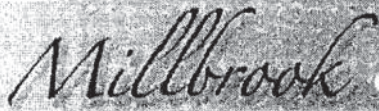
**Data on Portable Devices:** The District acknowledges the importance of protecting sensitive and confidential data, and will begin a study of options that are available to ensure the secure transport of confidential data on USB drives, laptops, and other portable devices. This study will include an analysis of cost, functionality, and staffing requirements.

**Data on Redeployed Computers:** Before redeployment of student or administrative computers, hard drives are routinely erased and completely reloaded using imaging software. There is no opportunity to retrieve old data from these computers.

**Data on Obsolete Computers:** When computers are no longer useful, the District will periodically surplus them through participation in a county-wide BOCES program. A third party vendor is used for this service, which includes removal of equipment and destruction of data. The District will now request a certificate from the vendor to provide documentation that they have removed sensitive data and licensed software from the hard drives.

**Off-Site Backups:** In March 2008, the District subscribed to a centralized backup service being developed by Dutchess County BOCES, which will be fully implemented by fall 2008. Using this service, all daily and periodic backups for all servers will be stored at the remote BOCES site. Data restoration can be completed using data from a hard drive backup and/or backup tape archives, and will be tested periodically.

**Disaster Recovery Planning:** We have budgeted in 2008-09 for the purchase of a new server. The old server will be retained off-site as an operating spare to be loaded with production software and data in the event of an emergency. The District is also currently involved in the planning of a county-wide disaster recovery service through BOCES. The ability to share the additional hardware resources that are required will result in significant savings to each of the participating districts in the county.



P.O. BOX AA • MILLBROOK, NEW YORK 12545

SUPERINTENDENT OF SCHOOLS 845-677-4200
BUSINESS ADMINISTRATOR 845-677-4201
PUPIL PERSONNEL SERVICES 845-677-4215
DISTRICT CLERK 845-677-4200

ELM DRIVE ELEMENTARY 845-677-4225
ALDEN PLACE ELEMENTARY 845-677-4220
MILLBROOK MIDDLE SCHOOL 845-677-4210
MILLBROOK HIGH SCHOOL 845-677-2510

OFFICE OF THE DISTRICT CLERK

JOB DESCRIPTION

Principle Account Clerk

Proposed New Position for 2008-09

Tentative Duties Statement for 2008-09

- Performs back-up duties as Deputy Treasurer to District Treasurer including writing checks, bank reconciliation, and making deposits.
Asset property accounting including the maintenance of the asset inventories, calculation of depreciation and tagging material.
Supervises, trains, and performs back-up responsibility for payroll and accounts payable personnel.
Responsible for entering new employees into human resources system and coordinates all paperwork and State/Federal forms.
Prepares monthly TRS (Teachers' Retirement System) and ERS (Employee Retirement System) reports and researches buy-back issues.
Prepares financial analysis for budget, labor negotiations and operations for management review.
Assists other departments in the accounting of federal/state grants including coding, amending and tracking of resources.
Coordinates FOIL requests including preparation of letters and FOIL materials.
Provides direct supervision of business office staff serving in Senior Account Clerk position(s)

Reports to and Supervised by:

District Business Administrator

Education Requirements:

A.S or B.A. in Business and or Accounting

Experience Requirements:

3 - 5 years of accounting and supervisory experience in a business environment

## 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.

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 cash receipts and disbursements and information technology for further audit testing.

To accomplish the objectives of this audit, our procedures included the following to obtain valid audit evidence:

- We interviewed appropriate District officials and employees to obtain an understanding of internal controls over the District's financial software system.
- We viewed reports of District employees' access rights to the financial software system in conjunction with their duties and responsibilities.
- We reviewed the District's financial records and reports, tested selected records and transactions, and examined pertinent documents to determine whether such records and reports were properly designed and whether cash transactions had been properly recorded.
- We scanned bank statements for unusual activity and verified bank reconciliations. We also examined press-numbered cash receipts for proper use and wire transfers for proper authorizations. We verified that school tax receipts were properly accounted for.
- We examined a judgmental sample of 50 cash disbursements and verified that the cancelled checks matched the information on Board-approved warrants, and we reviewed the propriety of supporting claim documents and the check endorsements.

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, Room 1050  
Buffalo, New York 14203-2510  
(716) 847-3647 Fax (716) 847-3643  
Email: [Muni-Buffalo@osc.state.ny.us](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto:Muni-Newburgh@osc.state.ny.us)

Serving: Orange, Putnam, Rockland, Westchester  
counties

