



# Schoharie Central School District Internal Controls Over Selected Financial Activities

Report of Examination

Period Covered:

July 1, 2005 — June 25, 2007

2007M-245



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	8
Comments of District Officials and Corrective Action	8
<b>COMPUTERIZED DATA AND ASSETS</b>	9
Installation of Software	9
User Access	10
Passwords	11
Disaster Recovery Plan and Backup	12
Physical Security	12
Recommendations	13
<b>AUDIT OF CLAIMS</b>	15
Recommendations	15
<b>PAYROLL</b>	16
Recommendations	17
<b>APPENDIX A</b> Response From District Officials	18
<b>APPENDIX B</b> Audit Methodology and Standards	23
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	25
<b>APPENDIX D</b> Local Regional Office Listing	26

# State of New York Office of the State Comptroller

---

---

## Division of Local Government and School Accountability

February 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 Schoharie 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*



## State of New York Office of the State Comptroller

---

# EXECUTIVE SUMMARY

The Schoharie 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 District also employs a Business Administrator who is responsible for managing the finance-related operations of the District and overseeing the work of the Business Office staff, including the District Treasurer.

The Board is also responsible for adopting policies and procedures ensuring that computerized data and assets are safeguarded and that claims are properly audited and approved prior to payment. In addition, the Board and the Business Administrator have the responsibility to assess the risks associated with the payroll process and institute appropriate internal controls to mitigate those risks. This includes segregating job duties so that the work performed by one individual is verified in the normal course of another employee's regular duties.

### **Scope and Objective**

The objective of our audit was to determine if District officials were properly managing District operations to safeguard District assets for the period July 1, 2005 through June 25, 2007. Our audit addressed the following related questions:

- Did the Board establish comprehensive policies and procedures addressing the safeguarding of computerized data and assets?
- Did the Board ensure that claims were properly audited and approved prior to payment?
- Did the Board and Business Administrator adequately address control risks inherent in the District Treasurer's duties to ensure that she was accurately accounting for payroll-related transactions?

### **Audit Results**

The Board has not established comprehensive policies and procedures to effectively address the safeguarding of computerized data and assets. Specifically, formal policies and procedures relating to installation of personal software on District's computers; addition, modification, and deletion of

user access rights; and a strong password system have not been adopted. The Board also has not developed a formal disaster recovery plan or policies and procedures for the backup of financial and non-financial data. These weaknesses significantly increase the risk that sensitive or mission-critical data and hardware and software systems may be lost, compromised, or damaged, or that the computer data system could be disrupted.

The Board did not audit claims, nor did they appoint a claims auditor to do so, until December 1, 2006. As a result, approximately 77 percent of all claims, totaling approximately \$13.2 million, paid during our audit period were not audited. Further, the claims auditor who was appointed does not report directly to the Board. While our testing did not reveal any material discrepancies, the failure of the Board to ensure that claims are audited increases the risk that moneys could be expended for inappropriate purposes, and that errors and irregularities could occur and go undetected or uncorrected in a timely manner.

The Board and Business Administrator did not adequately address control risks inherent in the District Treasurer's duties to ensure that she was accurately accounting for payroll-related transactions. The District Treasurer has complete control over the payroll process. In addition the Treasurer and senior account clerk have full user access rights to the payroll functions in the financial software. Although we did not find any material discrepancies, the concentration of key duties with one individual and granting access to the payroll software with insufficient oversight increases the risk that errors and/or irregularities could occur and go undetected and uncorrected in a timely manner.

### **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 Schoharie Central School District (District) is located in five towns in Schoharie County, and one town in each of Schenectady, Albany and Montgomery Counties. 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 District also employs a Business Administrator who is responsible for managing the District's financial operations and overseeing the work of the Business Office staff, including the District Treasurer.

There is one school in operation within the District, with approximately 1060 students and 200 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$17.4 million, which were funded primarily with State aid, real property taxes, and grants.

The Board is responsible for adopting policies and procedures and developing controls to safeguard computerized data and assets. The District uses one networked computer system to process and store financial and non-financial data, supported by three servers located at the school. Financial data is stored on a separate and dedicated server. The Information Technology (IT) administrator oversees the network system, and is an employee of the Northeastern Regional Information Center (NERIC).

The Board is also responsible for ensuring that claims are properly audited and approved prior to payment. In addition, the Board and Business Administrator have the responsibility to assess the risks associated with the payroll process and institute appropriate internal controls to mitigate those risks. This includes segregating job duties so that the work performed by one individual is verified in the normal course of another employee's regular duties.

## Objective

The objective of our audit was to determine if District officials were properly managing District operations to safeguard District assets. Our audit addressed the following related questions:

- Did the Board establish comprehensive policies and procedures addressing the safeguarding of computerized data and assets?

- Did the Board ensure that claims were properly audited and approved prior to payment?
- Did the Board and Business Administrator adequately address control risks inherent in the District Treasurer’s duties to ensure that she was accurately accounting for payroll-related transactions?

**Scope and Methodology**

We examined the District’s safeguards over computerized data and assets, the audit of claims, and payroll for the period July 1, 2005 to June 25, 2007. Our audit disclosed areas in need of improvement concerning information technology controls. Because of the sensitivity of this information, certain specific vulnerabilities are not discussed in this report but have been communicated to District officials so they could take corrective action.

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*.

## Computerized Data and Assets

District officials rely on computerized data to make financial decisions and report to State and Federal agencies. If the computers on which this data is stored fail or if the data is lost or altered, the results could range from inconvenient to catastrophic. Even small disruptions can require extensive employee and consultant hours to evaluate and repair. To this end, installation of unauthorized software should be prevented, access should be controlled and monitored, data should be backed up on a timely basis and stored in a secure offsite location, a formal disaster recovery plan should be established, and the computerized data and assets should be physically secure.

The Board is responsible for adopting policies and procedures and developing controls to safeguard computerized data and assets. In addition, the Superintendent and IT administrator are responsible for ensuring that District officials and employees adhere to adopted policies and procedures. The Board has not effectively addressed the safeguarding of computerized data and assets by establishing and monitoring policies and procedures.

### Installation of Software

Prohibiting the installation of unauthorized software by users is a crucial step in preventing potentially harmful software from being installed on District computers. Unauthorized programs could transfer personal or sensitive information to outside networks and/or potentially slow down the network or cause system crashes. The District's computer use policy requires users to obtain authorization before software is installed on District-owned computers. To ensure that authorization is received, District computers should be configured to only allow the installation of software by the IT administrator.

We found that users can install unauthorized software onto District computers. Due to this control weakness, we reviewed six District-owned computers (three desktops and three laptops) to determine if users had installed unauthorized software. We found that unauthorized software had been installed on one desktop. We also found that this computer had adware<sup>1</sup> installed on it. Further, the IT administrator informed us that during the 2006-07 fiscal year he found that a keylogger<sup>2</sup> had been installed on another District desktop

<sup>1</sup> Adware is a form of spyware. Spyware records the users' activity and consumes valuable computer memory. Because spyware is using memory and system resources it can cause system crashes and/or general system instability.

<sup>2</sup> A keylogger is a type of surveillance software that records the users' keystrokes. A keylogger can be used to record and steal user account IDs, passwords and other sensitive information.

computer. The IT administrator estimated that it had been on the computer for at least three months and believed it was installed by a student. The IT administrator informed us that no sensitive data is believed to have been compromised. However, because no formal records are maintained, we were unable to verify this.

The ability of users to install unauthorized software on District-owned computers significantly increases the risk that sensitive or mission-critical data and hardware and software systems may be lost, compromised, or damaged.

## User Access

Policies and procedures should be designed to limit access to computer data. Access should be based on the needs of particular job functions and each user should only be assigned one user account. Any changes to user accounts including additions, deletions, and modifications should be authorized and approved, in writing, by an appropriate official, for example the Superintendent. User accounts should be deactivated as soon as employees leave District service. Further, computer-use agreements<sup>3</sup> should be retained on file.

We found that the Board did not develop and adopt policies and procedures designed to limit access to data, as follows:

- The financial software currently used for payroll and personnel matters does not have the capability to limit user access based on job duties. All users<sup>4</sup> with access to the payroll and personnel modules have full user privileges within these modules. In addition, the administrative account in the general ledger and budgeting modules of the financial software have not been assigned to a particular user. Therefore, all users<sup>5</sup> with access to the general ledger and budgeting modules have full user privileges within these modules.
- Multiple-user accounts are created for employees. We found eight employees with two user accounts.
- There are no procedures to ensure that changes to access accounts are documented. The IT administrator adds and modifies access accounts based only upon a verbal directive

---

<sup>3</sup> Employees are required to initially sign a computer-use agreement before they are granted access to the network. Then, at the beginning of each fiscal year, each employee is required to again sign a computer-use agreement.

<sup>4</sup> The Treasurer and senior account clerk have access to the payroll module. The Treasurer, senior account clerk, and Business Office secretary have access to the personnel module.

<sup>5</sup> The Business Administrator, Treasurer, senior account clerk, and Business Office secretary have access to the general ledger module. The Business Administrator, Treasurer, and senior account clerk have access to the budgeting module.

by a department head supervisor or the Superintendent. There is no written documentation to indicate who authorized access, when access was given or revoked, and what access was permitted.

- User accounts are not deactivated in a timely manner. We found that 35 user accounts were active on the system that belonged to former employees and consultants. In some instances, these accounts were active for more than four years after these individuals had left the District. The IT administrator immediately deleted these user accounts when we brought this to his attention.
- The annual computer-use agreements were not retained on file. The person responsible for maintaining these agreements informed us that she discarded them at the end of each fiscal year. As a result, we were unable to determine if all users on the network had signed the agreement or if they were assigned user access rights in accordance with the agreement.

The failure to establish policies and procedures to limit user access increases the risk that individuals could inappropriately gain access to the system and change, destroy, or manipulate data and computerized assets. Without proper documentation, if a problem arises, it would be difficult to determine who authorized access, when access was given or revoked and what access was permitted.

## Passwords

System users are required to enter user names and passwords to gain access to networks, computers, and applications. To protect computerized data, the Board should adopt policies and procedures that require the use of strong passwords<sup>6</sup>; changes to passwords every 30 to 90 days; limiting attempts to access the system without a valid password to three or four; and provide for a network time-out<sup>7</sup> after a reasonable period of inactivity.

We found that the Board has not adopted comprehensive policies and procedures to address the use of strong passwords, limiting attempts to access the system and the timing-out of computers after a reasonable period of inactivity. Password selection is left up to individual users. In addition, there is no number or digit requirement, password changes are not required, and there is no limit as to the number of invalid attempts to access the system. Further, computers are not set up to time-out after a period of inactivity. There are also no password requirements for certain portions of the District's financial software.

<sup>6</sup> Strong passwords contain a combination of upper- and lower-case letters, punctuation and at least eight characters.

<sup>7</sup> Thus requiring employees to re-enter their user names and passwords to gain access

If a password system is not strong, or if a computer does not time-out after a period of inactivity, unauthorized persons could gain access to, change or delete sensitive information. If there are no limitations as to the number of failed attempts to access the system, unauthorized persons could try thousands of words or names until a valid password is found.

## **Disaster Recovery Plan and Backup**

A disaster<sup>8</sup> recovery plan should be established to prevent the loss of computer equipment and data, and provide procedures for recovery and precautions necessary to minimize the effects of disaster, so that mission-critical functions can be maintained or quickly resumed. Data stored on computers should be backed up on a routine basis and back-up copies should be stored in a secure offsite location to enable restoration.

The Board has not established a disaster recovery plan or adequate procedures to ensure computer data is adequately backed up and protected from loss. All computerized data is backed up automatically Monday through Friday to a tape drive. The back-up tapes are located in a locked office in the school. Once a week, back-up tapes are taken offsite, but they are not stored in a secured location.

The school is located in a flood plain, and therefore there is greater risk that a natural disaster could occur. If there was a disaster causing computer failure rendering the school site inaccessible, back-up copies stored on-site would be inaccessible, causing irreplaceable data to be lost. Data in unsecured locations is also at a greater risk of being compromised, misused, or lost. This could lead to serious interruptions of District operations, such as not being able to process checks to pay vendors or employees.

## **Physical Security**

The physical security over computerized assets is an important component of adequately safeguarding and protecting computerized assets. Limiting access to those assets, securing assets from fire and water damage and ensuring that assets are located in a climate-controlled environment is necessary to physically secure the District's computerized assets.

District officials have not adequately physically secured their computerized assets. The District has three servers. The two non-financial servers and a wiring closet are located in an unsecured area that is left opened and unlocked during the school day. Non-authorized personnel and students could potentially access this server

---

<sup>8</sup> A disaster is defined as a sudden, unplanned catastrophic event that compromises the integrity and data of the IT systems. This could include a fire, computer virus, or inadvertent employee action.

room. The financial server is located in a locked office. However, numerous custodians and the IT administrator all have keys to this office, and the access to this room is not monitored or tracked. The IT administrator also informed us that climate control for the room was an open window. During the summer months, the temperature in the room can be very high. In addition, we found that the wiring closets are located in unsecured areas (i.e., classrooms and wiring closets that are not always locked). Furthermore, the servers and wiring closets are located in areas that are not secure from fire and water damage.

Without physical security, all other security measures may be meaningless. Physical threats, whether internal or external, malicious or inadvertent could lead to damaged or stolen hardware and release of personal or confidential information. These security breaches can cost thousands of dollars and countless work hours to correct and possibly could lead to costly litigation for the District.

## **Recommendations**

1. The Superintendent and IT administrator should monitor and enforce the computer use policy to ensure that unauthorized software is not installed by users.
2. The Superintendent and IT administrator should review the network setup to ensure that only the system administrator has the authority to install software onto District computers.
3. The Board should develop and adopt procedures that require that all computer usage agreements are kept on file until new signed agreements are received.
4. The Board should adopt policies and procedures over the administration of network and financial software user access accounts that require:
  - User access in the District’s financial software to be assigned based on job functions
  - Users should only be assigned one user account.
  - Modifications, deletions, and additions to user access rights are authorized in writing.
  - User accounts are deactivated as soon as employees leave District service or the account is no longer in use.
5. The Board should ensure that a strong password system exists by adopting policies and procedures that require:

- The creation of strong passwords requiring users to select passwords that are at least eight characters, containing upper- and lower-case letters, and punctuation
  - Employees to change their passwords at least every 30 to 90 days
  - Limiting the number of failed log-in attempts
  - All computers to time-out after a set period of time of inactivity.
6. The Board should adopt policies and procedures to ensure that backups of financial and non-financial data are stored in a secure off-site location.
  7. The Board should adopt a comprehensive disaster recovery plan that details specific guidelines for the protection of private and essential data against damage, loss, or destruction.
  8. The Board should protect computerized assets by requiring that access to the server room and wiring closets are:
    - Restricted to only designated officials
    - Protected from fire and water damage
    - Located in a climate-controlled area.

## Audit of Claims

An effective internal control system requires that all claims are audited and approved before the District pays them. The Board is responsible for auditing District claims for payment. The Board may appoint a claims auditor to perform this function. The claims auditor should report directly to the Board. The claims auditor should conduct a deliberate and thorough review to determine that proposed payments are proper and valid charges against the District. In essence, the claims auditor is responsible for ensuring that all claims are legitimate District charges before the claims are paid.

The Board did not audit claims, nor did they appoint a claims auditor to do so until December 1, 2006. As a result, approximately 77 percent of all claims, totaling approximately \$13.2 million, paid during our audit period were not audited. Claims were properly audited after December 1, 2006, when the claims auditor was appointed. However, the claims auditor who was appointed does not report directly to the Board. Instead, the claims auditor consults with the accounts payable clerk to resolve any questions.

Due to these control weaknesses, we reviewed 35 claims totaling \$307,843 paid prior to December 1, 2006, and 15 claims totaling \$18,051 paid after December 1, 2006, to ensure that they were for legitimate District purposes and were properly supported. While our testing did not reveal any material discrepancies, the failure of the Board to ensure that claims are properly audited and approved prior to payment increases the risk that moneys could be expended for inappropriate purposes, and that errors and irregularities could occur and go undetected or uncorrected in a timely manner.

District officials informed us that the Board did not appoint a claims auditor until December 1, 2006, because they did not search for a claims auditor until they appointed a permanent Superintendent and Business Administrator in July 2006.

### Recommendations

9. The claims auditor should continue to audit and approve all claims prior to payment.
10. The claims auditor should report directly to the Board.

## Payroll

The Board and Business Administrator have the responsibility to adequately address control risks inherent in the District Treasurer's duties to ensure that she is accurately accounting for payroll-related transactions. An effective component of any payroll process is proper segregation of duties. Payroll duties should be segregated and computer access should be granted based upon job responsibilities to ensure that no one person controls all phases of the payroll cycle, such as adding and deleting employees, entering and modifying pay rates, processing the payroll, signing the payroll checks, and reconciling the payroll bank account. If it is not feasible to segregate duties, the Board and Business Administrator should consider mitigating this weakness by having someone independent of the process review completed payrolls. At a minimum, the review should include random checks to verify that payrolls are based upon actual hours or days worked and that Board authorized hourly rates or annual salaries are used. There should also be a comparison of net payrolls to payroll journals and an assessment of payrolls for reasonableness.

The Board and Business Administrator did not adequately address control risks inherent in the District Treasurer's duties to ensure that she was accurately accounting for payroll-related transactions. The Treasurer has complete control over the payroll process and full user access rights to the payroll functions in the financial software. She is directly responsible for adding and deleting employees, entering payroll changes, collecting timesheets, entering the hours worked and salaries paid, preparing and signing paychecks, and reconciling the payroll bank account. The senior account clerk, who is the backup when the Treasurer is unavailable to process the payroll, also has full access to the payroll functions in the financial software.

Due to the lack of segregation of duties over the payroll process, we reviewed certain compensation payments made to 11 employees to determine if the Treasurer was accurately accounting for wages and benefits and if payments were made in accordance with Board-approved rates and employee contracts. We also reviewed retirement system reports and personnel files to determine that employees receiving compensation were not fictitious. Although our testing did not reveal any material discrepancies, the concentration of key duties with one individual and granting access to the payroll software with little or no oversight increases the risk that errors and/or irregularities could occur and go undetected and uncorrected in a timely manner.

The Business Administrator informed us that due to the fact that the District is small and has limited staff, and that because there have

never been any problems discovered before with the Treasurer's work, District officials have not found it necessary to segregate the payroll-related duties.

## **Recommendations**

11. The Board and Business Administrator should provide for an adequate segregation of duties so that no one person controls all aspects of the payroll process. If it is not feasible to adequately segregate these duties, the Board should consider having someone independent of the payroll preparation process perform a review of the completed payrolls.
  
12. The Business Administrator should review the assignment of user access rights in the payroll software and assign access rights based on job duties only.

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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

The response has been included in its entirety except for sensitive information technology details that were redacted for security reasons.

# Schoharie Central School

PO Box 430, 136 Academy Drive, Schoharie, New York 12157

BRIAN D. SHERMAN  
Superintendent of Schools  
(518) 295-6600 ext. 79

MARYELLEN GILLIS  
Elementary School Principal  
(518) 295-6600 ext. 51

JAMIAN P. ROCKHILL  
Athletic Director  
(518) 295-6600 ext. 21



IN THE PURSUIT OF EXCELLENCE

ROBERT W. BONAHER  
Business Administrator  
(518) 295-6600 ext. 73

STACEY A. BIRDSALL  
Jr./Sr. High School Principal  
(518) 295-6600 ext. 01

LINDA M. NEVULIS  
Director of Curriculum & PS  
(518) 295-6600 ext. 57

February 22, 2008

[REDACTED]  
Binghamton Regional Office  
State Office Building, Room 1702  
44 Hawley Street  
Binghamton, NY 13901-4417

Dear [REDACTED]

This letter is a response to the draft findings of the audit of the Schoharie Central School District, which was discussed with us on January 31, 2008. Let me first thank your staff for their professionalism, assistance, and guidance. We believe the findings to be of great assistance in implementing our technology plan as well as updating our procedures, policies, and practices in our accounting office. We certainly appreciate your IT staff accepting our invitation to assist us with our efforts to bring us into the 20<sup>th</sup> century (We are still working to enter the 21<sup>st</sup> century.).

What follows are the response to the recommendations contained within the Advisory Draft and also the report of the examination. Recommendation # 1 - page 11, recommends that the Superintendent and IT administrator monitor the installation of software and the adherence to the Computer Use Policy. The District has responded by installing two software products on all computers in the district, with the exception of fourteen units used by administrative personnel. The [REDACTED] product locks the image of the computer disk in place, and upon re-booting the computer returns any changes (desktop icons, new folders, etc.) back to the original image. The [REDACTED] product does not allow downloaded software or unauthorized software to execute. Of the remaining units, modifications should be completed by the end of March 2008, as each disk image is highly individualized.

Recommendation #2 asks that only the system administrator have the ability to install software on district computers. Network security is in place, which only allows the system administrator access to modifying network resources. Specific individuals in the District (authorized by the

Superintendent) have varying levels of access to network resources in order to carry out their job functions.

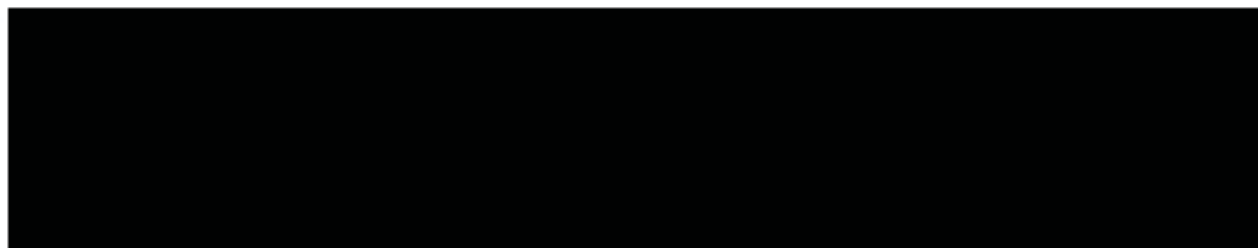
Recommendation #3 stipulates that the Board develop procedures that require computer usage agreements to be kept on file and updated annually. That recommendation has been implemented and the files are kept in the Superintendent's office.

There were several items under recommendation #4 that have been implemented, or partially implemented. To the degree possible at present, access to accounting software based on job description has been implemented. We replaced all of the [REDACTED] accounting software with the newer [REDACTED] versions, with the exception of the two remaining modules – payroll and human resources. The [REDACTED] version of the software did not permit multiple security levels, based on jobs being done by our personnel. The newer modules all have appropriate security levels, only the IT administrator has rights to make a change. All modifications must be authorized by the Superintendent. The two remaining [REDACTED] modules are in the budget for purchase after July 1, 2008 and the Human Resources module is not due to be released until after July 1<sup>st</sup>. We are currently assisting the developer with [REDACTED] modification. All computer users who leave the District have their accounts deleted, unless authorized by the Superintendent to not do so.

With regard to password procedures, the administration will be implementing new, more secure procedures in September. This addresses all items listed in recommendation #5.

Regarding recommendation #6, the District has just ordered the necessary software to create a virtual server from the current financial/accounting server, which will be used to run a mirror image of the accounting server on any personal computer, should disaster recovery be needed. The plan is to use the virtual server DVD to install/run the software on any PC just as if it were a workstation in the accounting office. The data, stored separately (for security reasons) would be installed on that PC when required. Our timeline is to prepare the mirror images and test the process over the next three months, with final changes being made as we install the two remaining [REDACTED] modules so that full security can be implemented. This is expected to occur prior to September of 2008. We are also preparing a mirror image of the existing financial server on a spare server in the District. This will then be stored off-site and the daily back-up data tapes can be brought to it as needed. We believe that this process will meet the needs of recommendation #7 for a comprehensive data disaster recovery plan.

Recommendation #8 calls for the physical security of the District's servers and wiring closets. At the present time, several of the servers are being moved to more secure offices and the finance/accounting server will be moved to a secure and climate controlled location. Door security items and cabinet security for the student server and switching closets are being addressed as we modify the fiber optic infrastructure over the next six months.



The previous comments have addressed the recommendations for Information Technology. The following passages are responses from the School Business Administrator and the Superintendent of Schools, regarding the financial portion of the audit:

The audit report states: "The Board and Business Administrator did not adequately address control risks inherent in the District Treasurer's duties to ensure that she was accurately accounting for payroll-related transactions.... Although we did not find any material discrepancies, the concentration of key duties with one individual and granting access to the payroll software with insufficient internal controls increases the risk that errors or irregularities could occur and go undetected and uncorrected in a timely manner."

We would hope that the final report from the Comptroller's Office would indicate that the District had a major changeover occur in Board membership starting with the 2006-2007 school year, and that a new Superintendent and new School Business Administrator came on board in July of 2006. In the previous five years, there were five different Superintendents and three different business officials employed by the District. Obviously, we can only address the audit comments since July 2006. The key phrase, I think, is "we did not find any material discrepancies." We are very pleased with this finding.

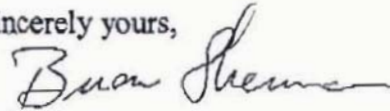
We can report to you that as part of the current role of the Business Administrator, with regard to the payroll process, he conducts a very thorough and detailed review of all payroll-related work papers before they are signed on the certification form. There is extensive documentation regarding who is being paid and how much they will receive and he maintains a roster of all current employees which is prepared and maintained by an individual other than the Treasurer. He uses that tool to verify that the payee is, indeed, an employee of the district. Additionally, he regularly attends NYSASBO workshops and works with a team that attends the School Management Institute. The focuses of the past year's three-day and five-day workshops (just mentioned) have been on payroll. We understand the concern about risk due to the concentration of payroll processing duties with one person in the District Business Office. While we are comfortable and have great assurance with the expertise of the employee and the supervision of the process by the Business Administrator (who is responsible for certifying each payroll), we recognize that we need to have a better segregation of duties and cross-training. We are now implementing this. Also, secured access to the payroll software module will be better controlled once the updated version of the software has been installed (as mentioned above in the IT comments section).

We are also pleased to report that in addition to the interim actions of our audit committee to monitor the warrants since the departure of our internal claims auditor last month, the Board will be appointing a new claims auditor at its next Board meeting on February 27<sup>th</sup>, 2008. She has an accounting background and is also the claims auditor for the neighboring school district. She will be reporting directly to the Board of Education on a regular basis.

It is our sincere hope that we have appropriately addressed the concerns, the suggestions by your team, and the recommendations contained within the draft report. As you can see, we are well on our way in developing a rigorous action plan to respond to the recommendations in the report. Contrary to the usual horror stories we often hear, your staff was a valuable and very helpful asset to our financial and IT operations. It was a pleasure to work with them. On behalf of the

Administration, Board of Education, and the accounting staff, we would again like to thank your team for their work with Schoharie Central School.

Sincerely yours,



Brian D. Sherman  
Superintendent of Schools

cc: Mr. F. Christian Spies, Board President  
Mrs. Rose Wilber, Clerk of the Board  
Mr. Robert Bonaker, SBA

File

## **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, 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 objective and scope by selecting for audit those areas most at risk. We selected safeguards over computerized data and assets, the audit of claims, and payroll for further audit testing.

To accomplish the objective of this audit, we performed the following steps:

- Interviewed officials and employees as to existing internal control systems
- Reviewed computer access and security protocols, policies, and procedures
- Inquired as to the procedures in place for the installation of software on District computers
- Reviewed District computers for acceptable use
- Inquired as to the user access procedures including the addition, deletion, and modification of user rights to the network and financial software
- Reviewed user access account reports
- Inquired about the access into the network including the password system
- Inquired as to recovery protocols and procedures including the backup of computerized data
- Reviewed the physical security over the District's computerized data and assets

- Interviewed the current claims auditor
- Determined the total amount expended by the District for non-payroll purposes and the total amount expended that had not been audited and approved
- Verified that selected claim packages were for legitimate District purposes, and had been audited and approved by the claims auditor
- Tested employee compensation payments made during the 2005-06 and 2006-07 fiscal years to determine if employees were being paid in accordance with established rates and contracts
- Verified that employees receiving compensation were not fictitious by reviewing retirement system reports and personnel files
- Verified that any additional benefits paid to the Superintendent and Business Administrator were paid in accordance with their employee contracts
- Tested separation payments made to employees leaving District service to ensure that they were accurate and in compliance with employee contracts
- Tested payroll payments to ensure that they were accurate and were made in compliance with established rates and contracts
- Verified that leave time was accurate and in compliance with employee contracts
- Verified that payroll withholdings were accurate and adequately supported.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## APPENDIX 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-Bufferalo@osc.state.ny.us](mailto:Muni-Bufferalo@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**

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, NY 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