



# Cherry Valley-Springfield Central School District Computerized Data and Assets

Report of Examination

Period Covered:

July 1, 2006 — February 4, 2008

2008M-87



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>COMPUTERIZED DATA AND ASSETS</b>	9
Passwords	9
User Access	10
Disaster Recovery	11
Physical Security	12
Recommendations	
<b>APPENDIX A</b> Response From District Officials	14
<b>APPENDIX B</b> Audit Methodology and Standards	16
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	18
<b>APPENDIX D</b> Local Regional Office Listing	19

# 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 Cherry Valley-Springfield Central School District, entitled Computerized Data and Assets. 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 Cherry Valley-Springfield 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 Board is also responsible for adopting policies and procedures ensuring that computerized data and assets are safeguarded. The District uses one networked computer system to process and store financial and non-financial data. The Information Technology (IT) administrator oversees the network system, and is an employee of the Otsego Northern Catskill Board of Cooperative Educational Services (ONC BOCES).

#### **Scope and Objective**

The objective of our audit was to determine if District officials were properly managing District IT operations to safeguard District assets for the period of July 1, 2006 to February 4, 2008. Our audit addressed the following related question:

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

#### **Audit Results**

The Board has not established comprehensive policies and procedures to effectively address the safeguarding of computerized data and assets. Specifically, the District has not adopted comprehensive policies and procedures relating to strong passwords, and the addition, modification, and deletion of user access rights. The Board also has not developed a formal disaster recovery plan or physically secured its computerized assets. While our tests did not identify any occurrences of unauthorized activity, District officials should promptly correct the weaknesses we identified to reduce the risk that sensitive or mission-critical data may be lost or compromised, or that systems could be damaged or disrupted.

#### **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 Cherry Valley-Springfield Central School District (District) is located in one town in Herkimer County, two towns in Montgomery County and seven towns in Otsego County. The District is governed by the Board of Education (Board) which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There is one school in operation within the District, with approximately 600 students and 140 employees. The District's budgeted expenditures for the 2007-08 fiscal year are approximately \$11.7 million, which are funded primarily with State aid, real property taxes, and grants.

The Board is also 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, and the system is supported by three servers located at the school. Financial data is stored on a separate dedicated server. The Information Technology (IT) administrator who oversees the network system is an employee of the Otsego Northern Catskill Board of Cooperative Educational Services (ONC BOCES).

## Objective

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

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

## Scope and Methodology

We examined the District's safeguards over computerized data and assets for the period July 1, 2006 to February 4, 2008. 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 separately 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 for the District. Even small disruptions can require extensive employee and consultant hours to evaluate and repair. To this end, District officials should enforce password provisions, control and monitor system access, establish a formal disaster recovery plan, and ensure the computerized data and assets are physically secured.

The Board is responsible for adopting policies and procedures and developing controls to safeguard computerized data and assets, and the IT administrator is responsible for ensuring that District officials and employees adhere to adopted policies and procedures. We found that the Board and District officials have not effectively addressed the safeguarding of computerized data and assets by establishing adequate policies and procedures and monitoring their implementation. While our tests did not identify any occurrences of unauthorized activity, District officials should promptly correct the weaknesses we identified to reduce the risk that sensitive or mission-critical data may be lost or compromised, or that systems could be damaged or disrupted.

### 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>1</sup> and limit attempts to access the system without a valid password to three or four log-in attempts. The District's Desktop Security policy directs users to select a six-character password and states that a user's access to the system will be restricted after three unsuccessful log-in attempts. The IT administrator is responsible for ensuring that policy provisions are monitored and enforced.

We found that the Board-adopted Desktop Security policy was not comprehensive because it did not require the use of strong passwords. In addition, the IT administrator did not monitor and enforce the policy provisions regarding password creation and unsuccessful log-in attempts. Using a generic user account created

<sup>1</sup> Strong passwords contain a combination of upper and lower case letters, punctuation and at least eight characters.

by the IT administrator, we gained access to the system and changed the assigned password to a five-character password. We then attempted to sign into the system using an incorrect password; after six unsuccessful attempts, the system froze for one minute and then allowed us to log-in again. We notified the IT administrator of these weaknesses and then six weeks later we performed the same procedures again. We found that the system weaknesses had not been corrected: we were able to change the password to a single character and it took 13 unsuccessful log-in attempts before the system restricted us from gaining access.

These weaknesses occurred because the IT administrator did not appropriately set up the system to comply with the existing policy provisions. The IT administrator was unable to provide a sufficient explanation as to why appropriate system restrictions were not put in place. The lack of a strong password system increases the risk that unauthorized persons could gain access to, change or delete sensitive information. Further, if the number of unsuccessful attempts to access the system is not appropriately limited, the possibility of unauthorized persons gaining access to the system is increased.

## 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. For example, administrator rights should generally be assigned only to the IT administrator. Any changes to user accounts, including additions, deletions, and modifications, should be authorized and approved, in writing, by an appropriate official (e.g., the Superintendent). User accounts should be deactivated as soon as employees leave District service.

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

- All faculty members and certain administrative staff are given administrator rights on the District computers assigned to them. Administrator rights allow the user to change and/or override computer settings and add and delete software. Due to this control weakness, we reviewed eight District-owned computers<sup>2</sup> (seven laptops and one desktop) for appropriate usage and to determine if users had installed unauthorized software. Our testing did not disclose any inappropriate usage or unauthorized software installations.
- There are no procedures to ensure that changes to access accounts are documented. The IT administrator adds and

---

<sup>2</sup> Four were assigned to administrators and four were assigned to faculty.

modifies access accounts based only on an informal directive 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 five user accounts active on the system belonging to former employees.<sup>3</sup> Four of these accounts were active for more than one and one-half years after these individuals left District service. The IT administrator immediately deleted these user accounts when we brought this to his attention.

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. Further, if a problem arises, it would be difficult to determine who authorized access, when access was given or revoked and what access was permitted without proper documentation.

## **Disaster Recovery**

A disaster<sup>4</sup> recovery plan should be established to help prevent the loss of computerized equipment and data, and provide procedures for recovery in the event of an actual loss. The plan should include the precautions to be taken to minimize the effects of a disaster so that District officials can either maintain or quickly resume mission-critical functions.

The Board has not established a disaster recovery plan to ensure computer data is adequately protected from loss. In the event of a disaster, District personnel have no guidelines or plan to follow to prevent the loss of equipment and data or procedures for data recovery. The lack of a disaster recovery plan could lead to the loss of important financial data and serious interruptions to District operations, such as not being able to process checks to pay vendors or employees.

The Superintendent informed us that District officials had not adopted a disaster recovery plan because, prior to 2007, emphasis was not placed on the IT system. In the summer of 2007, the District had a network assessment conducted and is currently in the process of creating a network security and disaster recovery plan.

## **Physical Security**

The physical security over computerized assets is an important component of adequate protection for computerized assets. Limiting

---

<sup>3</sup> Three substitute teachers, a guidance counselor and a retired teacher

<sup>4</sup> A disaster is defined as a sudden, unplanned catastrophic event that compromises the integrity and data of the IT systems. This could include fire, flood, a computer virus, vandalism, or inadvertent employee action.

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 addressed the physical security of their computerized assets. The IT administrator informed us that, because of inadequate climate control in the server room, he often had to leave the room unlocked and the door open during the school day to avoid damage to equipment from overheating. Therefore, unauthorized personnel and students could potentially access the server room. In addition, we found that the main fiber optic cables are located in an unsecured area (i.e., a room that is not always locked and is accessible to students). Furthermore, the servers and fiber optic cables are located in areas that are not secure from fire and water damage.

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

The Superintendent informed us that District officials are planning to upgrade the server room and make changes to the entire IT system as part of the next District building project, which is expected to begin in 2009.

## **Recommendations**

1. The Board should amend the Desktop Security policy to require that users select strong passwords (i.e., containing at least eight characters, with upper and lower case letters and punctuation).
2. The IT administrator should monitor and enforce the provisions of the Desktop Security policy. To this end, he should ensure that the District's network does not allow passwords that do not meet the Board's specified criteria, and that the system restricts access to users after three unsuccessful log-in attempts.
3. The Board should adopt policies and procedures over the administration of network user access accounts to require that:
  - administrator rights be assigned only to the IT administrator
  - modifications, deletions, and additions to user access rights be authorized in writing, and

- user accounts be deactivated as soon as employees leave District service or when the account is no longer in use.
4. 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.
  5. District officials should protect computerized assets by requiring that servers and fiber optic cables be located in a climate-controlled area and protected from fire and water damage. The server room should be locked, with access restricted to designated officials.

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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

# CHERRY VALLEY-SPRINGFIELD CENTRAL SCHOOL

P.O. Box 485 Cherry Valley, NY 13320 Telephone (607) 264-3265/264-9332 Fax (607) 264-3458

Nicholas J. Savin, Superintendent of Schools  
Victoria P. Gaughan, School Business Official  
Jeffrey J. Bennet, Interim Principal of Curriculum & Instruction  
Steven R. Davis, Interim Principal of Student Affairs & Athletic Director

## BOARD OF EDUCATION

Steve Schneider, President  
Christopher Graham, V. Pres.  
Donald Drake  
Peter Frechafer  
Ellen Johnson  
Paul Mendelsohn  
Kathleen Taylor

June 16, 2008

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

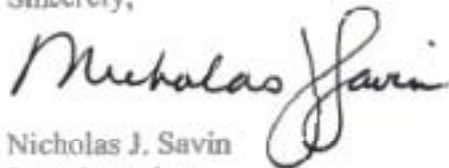
Dear [REDACTED]

On Thursday, May 29, 2008, [REDACTED] and [REDACTED] met with Christopher Graham, BOE Vice-president, Vicky Gaughan, Business Official, and me to discuss the State Comptroller's Audit findings. The meeting and the audit process were helpful in assisting CVS to better manage the district's finances and controls.

We received the initial report and agree with its findings. This past summer with the assistance of Broome BOCES, we started the process of assessing and improving the quality and security controls of our technology network system. The findings and suggested areas of improvement from the Comptroller's Office were helpful in this effort.

After receiving the final audit report, we will develop a plan to address the identified areas in need of improvement. Should you have any questions, please feel free to call me at (607) 264-9332.

Sincerely,



Nicholas J. Savin  
Superintendent

Cc: CVS Board of Education Members  
Vicky Gaughan, School Business Official

## 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 that area most at risk. We selected safeguards over computerized data and assets for further audit testing.

To accomplish the objective of this audit, we:

- Interviewed officials and employees as to existing internal control systems
- Reviewed computer access and security protocols, policies, and procedures
- Inquired about the access into the network including the password system
- Tested the password creation and unsuccessful log-in standards
- Reviewed eight District computers for acceptable use
- Inquired as to user access procedures including the addition, deletion, and modification of user rights to the network
- Reviewed user access account reports
- Inquired as to recovery protocols and procedures
- Reviewed the physical security over the District's computerized data and assets.

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

## APPENDIX 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**

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