



# Perry Central School District Information Technology

Report of Examination

Period Covered:

July 1, 2005 — June 20, 2007

2007M-285



Thomas P. DiNapoli

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	3
<b>INTRODUCTION</b>	5
Background	5
Objective	5
Scope and Methodology	6
Comments of District Officials and Corrective Action	6
<b>INFORMATION TECHNOLOGY</b>	7
Access to Network Servers	7
Security of Backup Data	8
Disaster Recovery	8
Filter By-Pass	8
Recommendations	10
<b>APPENDIX A</b> Response From District Officials	11
<b>APPENDIX B</b> Audit Methodology and Standards	14
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	15
<b>APPENDIX D</b> Local Regional Office Listing	16

# 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 can also identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Perry Central School District, entitled 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 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*

# Introduction

## Background

The Perry Central School District (District) is located primarily in Wyoming County, in the Towns of Perry, Castile, Warsaw, Covington, and a small portion of Leicester in adjoining Livingston County. The District is governed by the Board of Education (Board) which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are two schools in operation within the District, with approximately 1,030 students and 200 employees. The District's budgeted expenditures for the 2005-06 and 2006-07 fiscal years were approximately \$15 million each, funded primarily with State aid, real property taxes and grants.

The District contracts with EduTech, through their local BOCES, for the support of its computers and other related technology and equipment. According to District officials, they have approximately 515 networked computers. District staff use computers in the day-to-day operations of the school for instructional purposes and to process financial transactions. EduTech, maintains the District's two servers and hardware and various software applications. They also provide hardware and software support and establish and maintain the District's virus protection and firewall programs. The District also has policies addressing issues such as appropriate use of computer resources and restrictions on internet use.

## Objective

The objective of our audit was to determine if internal controls over information technology were appropriately designed and operating effectively to adequately safeguard District assets. Our audit addressed the following related questions:

- Did the Board establish comprehensive policies and procedures concerning access rights and computer usage to monitor and control access to computerized data and hardware?
- Did the Board establish policies and procedures to ensure computerized data is physically secure and establish plans to prevent or help address potential disasters to equipment and data?

**Scope and  
Methodology**

During this audit we examined internal controls over information technology of the District for the period July 1, 2005 through June 20, 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 that they have initiated 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*.

## Information Technology

One of the Board's responsibilities is to ensure that a system of internal controls is designed and implemented, which incorporates policies and procedures to provide reasonable assurance that all assets and resources are used in accordance with laws, regulations, policies and sound business practices and protected against waste, loss and misuse. The District relies on an information technology (IT) system for providing computer education; accessing the internet; communicating by e-mail; storing student data; maintaining financial records; and reporting to State and Federal agencies. Therefore, the IT system and the data it holds are a valuable District resource. If the IT system fails, the problems that result could range from inconvenient to catastrophic. Even small disruptions in electronic data systems can require extensive employee and consultant hours to evaluate and repair.

District officials should control and monitor access to IT systems to reduce the risk of misuse and/or alteration of data and a potential financial loss to the District. The Board should ensure that a formal disaster recovery plan is developed to provide appropriate guidance on the prevention of loss of computer information and the recovery of data in the event of a disaster. We found that internal controls over the District's computerized financial system were inadequate: District personnel failed to put controls in place to protect servers and component parts, did not secure data backup tapes, and failed to implement a formal disaster recovery plan. In addition, the District was not adhering to the terms of their filter by-pass agreement nor monitoring the use of such by-pass. Due to these weaknesses, the District's IT systems and electronic data have been subject to an increased risk of loss or misuse.

### **Access to Network Servers**

Maintaining adequate security over District assets helps to ensure that items are protected from loss and used effectively for their intended purpose. District officials can establish security over IT systems and equipment by controlling access to servers and components and by physically securing network components in a locked room. However, we found that the District's two network servers are located on open shelving in a file room in the Business Office. The file room is adjacent to an unlocked door which opens to a hallway in the high school. The door to the file room was routinely open due to climate control issues. Physical access to the servers is significantly vulnerable because the doorway adjacent to the high school hallway is the main entry point for anyone entering the Business Office from the high school.

Under existing conditions, it would be difficult for District officials to prevent unauthorized and/or malicious access to these assets. As a result, services could be disrupted and costly equipment damaged, destroyed or stolen.

### **Security of Backup Data**

Data should be backed up (i.e., a copy made) on a routine basis and the backup copy stored at an environmentally and physically secure off-site location. The District has not established formal policies or procedures for the back up of District information including financial data. The District's Technology Coordinator told us that daily backups are performed each night in addition to weekly backups that cover a one month period. He also indicated that there are five weekly backup tapes that are used in rotation and taken to the adjacent elementary building and locked in the vault. We tested this process and found that all of the tapes, daily and weekly, were being stored on a shelf next to the servers and were not being taken to a secure off-site location as we were told. The District risks losing most, if not all, of its computer processed data if the system becomes compromised and a backup is not available to restore it to normal operation.

### **Disaster Recovery**

The District's internal control system should include a formal disaster recovery plan to address the possible loss of computer equipment and data and establish procedures for recovery in the event of such a loss. The plan should detail the precautions to be taken to minimize the effects of any disaster and enable the District to either maintain or quickly resume its mission-critical functions. The plan should include a significant focus on disaster prevention as well. However, District officials have not established a formal disaster plan for approval by the Board. We were provided with a draft version of the District's Disaster Recovery Plan. We found that the plan currently lacks many details. For example, the plan references an alternate processing site to be identified by the Superintendent, but does not specify the actual site. Consequently, in the event of a disaster, District personnel have no specific guidelines or plan to follow to help minimize or prevent the loss of equipment and data or guidance on how to implement data recovery procedures.

### **Filter By-Pass**

The District has a password that allows a user to override the system's filter, and thus gain access to internet sites that would normally be restricted from access within the District. District officials told us that the intent of having such a filter by-pass allows students to research topics for school projects that would otherwise be blocked by the filter. The school resource officer is to monitor student usage. An agreement between the District and LakeNet (a Division of EduTech), regarding the password, states that the password belongs to one individual and that it is not to be shared. In this case, the password belongs

to the District librarian who was a signatory to the agreement. The agreement states that “the use of the password and the sites that it may access will be monitored.”

We requested a filter by-pass activity report for the fiscal year and were told by a LakeNet representative that the report would be too large to generate and send to us as it would contain information on every time someone from outside the District tried to penetrate the District’s filter and every time someone from inside the District attempted to go through the filter. The LakeNet representative generated a filter by-pass usage report for one day. The report consisted of individual e-mails sent to LakeNet each time the password was used that day. However, the sites listed on this report only include the first site visited after the by-pass password was used. The LakeNet representative indicated that he was surprised at the frequency that the password was used; 16 times that day. He also mentioned some of the sites that were identified in the report: games, auction, photo, personal e-mail, retail, and dating. We obtained similar activity reports from the same LakeNet representative for four days during the 2006-07 fiscal year.<sup>1</sup> According to the information provided, the password was used to gain access an average of 11 times per day for the days chosen. Sites visited on these days included sites similar to those previously mentioned, the most frequently visited sites being for auctions and games. Additional sites visited on these days were personal pages. Many, if not all, of these sites appear to be for other than District or educational purposes.

The technology coordinator told us that he does not monitor the use of this password or the sites that are visited using the password. In addition, it appears that LakeNet is not monitoring the usage of the password, since they were surprised at its frequent use and the sites visited. The librarian, who is responsible for the password, told us that she has shared the password with various coworkers in the past. She also allows her son to use the password to play video games using a computer located in the library. This is clearly a violation of the terms of the agreement.

Use of the District’s computer equipment to access blocked internet sites for personal use is an imprudent and inappropriate use of District resources. The District may also be subjecting the IT system to harmful viruses or other intrusions.

---

<sup>1</sup> We chose dates during the 2006-07 fiscal year because the District has dynamic IP addresses, which means they change each time the computer connects to the internet. Our intent was to trace the IP addresses identified in the activity reports to specific computers in the District and we thought that we would be more successful with more recent activity dates. However, we were unable to match the IP addresses.

## **Recommendations**

1. The District's Technology Coordinator should ensure that network servers are kept in a secure, climate-controlled location; access should be limited and monitored.
2. The District's Technology Coordinator should ensure that data backup tapes are routinely transported to a secure off-site location.
3. The Board should ensure that a formal disaster recovery plan is developed and implemented.
4. The District's Technology Coordinator should ensure that the filter override password is used appropriately, as intended, and within the terms of the agreement.

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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

# Perry Central School District

PERRY, NEW YORK 14530

February 6, 2008

[REDACTED]  
Office of the State Comptroller  
Buffalo Regional Office  
295 Main Street-Room 1050  
Buffalo, NY 14203

[REDACTED]:  
Perry Central School District is in receipt of the Draft Report and Examination of the audit conducted by your office. We thank you for the opportunity to respond to these findings in a productive way. This letter addresses the findings and recommendations of the report and will form the basis of our corrective action plan.

## 1. Access to Network Servers

The file/server room in question will remain closed and locked at all times. Access will only be granted by authorized personnel through obtaining a key from the Business Office or District Office. This process is currently in place.

Climate control issues will be addressed via the District's current capital project through the installation of additional ventilation. The estimated completion of the installation of additional ventilation is September of 2008.

## 2. Security of Back-Up Data

The District will continue the process of performing back-ups each night in addition to continuing the weekly back-ups that cover a one week period. Edutech also performs daily off site back-ups of the financial data, and will continue to do so. The District Technology Coordinator has developed a procedure for the secure storage of the District's in-house back-ups in a safe at an off site location. This procedure is currently in place and will be verified periodically by the Superintendent of Schools.

## 3. Disaster Recovery

The District's Technology Coordinator, in collaboration with the Technology Committee and Edutech, has developed a Disaster Recovery Plan. The draft of this plan was reviewed by the Office of the State Comptroller. The comments from that review were

considered and the plan was adjusted in order to contain more specific information. It will continue to be reviewed and refined by the Technology Committee on a yearly basis.

#### 4. Filter By-Pass

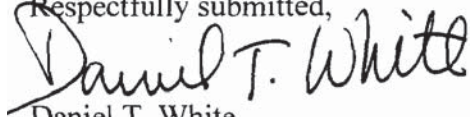
The District understands the importance of ensuring that the filter override password is used appropriately and as intended. The District has removed all previous filter override passwords. Any personnel now needing filter override passwords must receive authorization from the Technology Coordinator, the Superintendent of Schools and LakeNet. These authorized users must also sign a statement ensuring they understand the appropriate uses of the by-pass and agreeing to not provide the override password to other personnel.

LakeNet now notifies the District's Technology Coordinator via e-mail of each instance of override activity. This e-mail includes the by-pass user ID and the site visited. The District's Technology Coordinator will report any potentially inappropriate use to the Superintendent of Schools. Any use of the filter by-pass that falls outside of the terms of the agreement will result in the removal of the by-pass capability from that individual. These procedures are currently in place.

Perry Central School District would like to thank the Office of the State Comptroller for providing this report. The District takes all of the findings and recommendations very seriously and will ensure that the corrective actions highlighted in this letter continue. All of the above corrective actions will be reviewed by the District's Audit Committee on a yearly basis.

The District is proud that the financial control systems, procedures and policies were found to be acceptable and will continue to be steadfast in that area as well.

Respectfully submitted,



Daniel T. White  
Superintendent of Schools

## APPENDIX B

### AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard District assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, 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 internal controls over information technology for further audit testing. Certain observations and lesser findings related to employee separation compensation were discussed with District officials to help them strengthen internal controls in that area.

In order to satisfy our audit objectives concerning information technology, we interviewed officials, observed physical controls and examined the following records to determine the effectiveness of internal controls pertaining to these functions and any associated effects of deficiencies in those controls:

- District policies and agreements relevant to information technology
- Filter override activity reports

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-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**

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