



Plattsburgh City School District Internal Controls Over Extra-classroom Activity Funds and Information Technology

Report of Examination

Period Covered:

July 1, 2006 — November 30, 2007

2008M-31



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	3
EXECUTIVE SUMMARY	5
INTRODUCTION	7
Background	7
Objective	7
Scope and Methodology	7
Comments of District Officials and Corrective Action	8
EXTRA-CLASSROOM ACTIVITY FUNDS	9
Recommendations	10
INFORMATION TECHNOLOGY	12
Computer System Access	12
Audit Logs	15
Physical Security Over Component Parts	16
Disaster Recovery	16
Recommendations	16
APPENDIX A Response From District Officials	18
APPENDIX B Audit Methodology and Standards	21
APPENDIX C How to Obtain Additional Copies of the Report	22
APPENDIX D Local Regional Office Listing	23

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

May 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 Plattsburgh City School District, entitled Internal Controls Over Extra-classroom Activity Funds and Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution, and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller
Division of Local Government
and School Accountability*



State of New York Office of the State Comptroller

EXECUTIVE SUMMARY

The Plattsburgh City School District (District) is located in the City of Plattsburgh, Clinton County. The District is governed by the Board of Education (Board) which comprises nine elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

Scope and Objective

The objective of our audit was to determine if the District had established effective internal controls over extra-classroom activity funds and information technology for the period July 1, 2006 to November 30, 2007. Our audit addressed the following related questions:

- Are internal controls over extra-classroom activity funds adequate?
- Are internal controls over the District's information technology system appropriately designed and operating effectively to adequately protect electronic data?

Audit Results

We found instances where the Board did not establish critical internal controls or the controls that had been established were not implemented and operating effectively. As a result the District is vulnerable to the possibility of errors and/or irregularities occurring and not being detected in a timely manner.

There were weaknesses in the controls over extra-classroom activity funds. Although the Board has established a policy to govern the operations of the extra-classroom activity fund and appointed both a middle and high school central treasurer, the Board has not appointed a faculty auditor and fund monies are not maintained as the policy directs. Our testing disclosed that District extra-classroom activity fund officials did not deposit 18 cash receipts totaling \$29,553 for 11 days or more after receipt and that two press-numbered receipts were missing. Due to these control weaknesses, there is an increased risk that errors could occur and activity fund monies could be lost or misused.

Internal controls over the information technology system are not appropriately designed and operating effectively. Passwords are not complex, there is no requirement to change them periodically and they are not always stored in an encrypted format. In addition, passwords are not always unique or required, and access rights are not revoked upon a set number of failed sign on attempts. We also

found several users have greater access than necessary and the ability to be involved in multiple aspects of financial transactions, and District officials do not control physical access to the IT system or have a formal disaster plan in place. As a result, the District's IT systems and electronic data are subject to an increased risk of loss or misuse.

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 initiated they planned to initiate corrective action.

Introduction

Background

The Plattsburgh City School District (District) is located in the City of Plattsburgh, Clinton County. The District is governed by the Board of Education (Board) which comprises nine 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 five schools in operation within the District, with approximately 1,830 students and 390 employees. The District's budgeted expenditures for the 2007-08 fiscal year are \$35.6 million, which are funded primarily with State aid, real property taxes, and grants.

The District reported approximately \$32.2 million in general fund expenditures during the 2006-07 fiscal year. During the same year, the extra-classroom activity fund recorded more than \$312,000 in receipts and disbursements. The District has approximately 1,200 individual computers that are networked together. District employees use computers in day-to-day operations for instructional purposes and to process financial transactions.

Objective

The objective of our audit was to determine if the District had established effective internal controls over extra-classroom activity funds and information technology. Our audit addressed the following related questions:

- Are internal controls over extra-classroom activity funds adequate?
- Are internal controls over the District's information technology system appropriately designed and operating effectively to adequately protect electronic data?

Scope and Methodology

We examined the District's control environment and its internal controls over extra-classroom activity funds and information technology for the period July 1, 2006 to November 30, 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 initiated 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*.

Extra-classroom Activity Funds

Extra-classroom activity funds are raised through charges for, by, or in the name of, organizations whose activities are conducted by students. Students raise and spend these funds to promote the general welfare, education, and morale of all students, and to finance the normal and appropriate extracurricular activities of the student body. The District's 35 accounts in the extra-classroom activity fund (activity fund) recorded more than \$387,000 in receipts and disbursements during the period July 1, 2006 to November 30, 2007 and had a combined cash balance of approximately \$63,000 as of November 30, 2007.

The Regulations of the Commissioner of Education (Regulations) require the Board to establish policies and procedures that describe the records that District personnel and students must maintain, and the duties and control procedures they must follow, for the safeguarding, accounting and auditing of all monies received and derived from extra-classroom activities. Regulations also require the Board to appoint a central treasurer to be responsible for the activity fund receipts and disbursements and a faculty auditor to oversee the management of activity funds. Having these controls in place helps to ensure that activity fund monies are accounted for properly and minimizes the risk that errors or irregularities could occur and remain undetected.

The Board has established a policy to govern the operations of the activity fund and appointed both a middle school and high school central treasurer to be responsible for receipts and disbursements. However, the Board has not appointed a faculty auditor to oversee the management of activity funds and activity fund monies are not maintained as the policy directs. For instance, although the policy requires faculty advisors to ensure that student ledgers are maintained for each activity fund showing receipts, disbursements and a running balance, none are maintained. As a result, neither the Board nor District officials have assurance that activity fund monies are accounted for properly in compliance with regulations.

As a result of the internal control weaknesses we identified, we reviewed 30 disbursements totaling \$58,271 remitted from 19 of the 35 activity fund accounts during the audit period to determine if the expenditures were made for appropriate student activities. We found no discrepancies.

We also examined 15 cash receipts totaling \$10,587 for five middle school activity fund accounts to verify that the monies were deposited timely in accordance with good business practices. We found that for three cash receipts totaling \$5,144 it took 12 days or more from the date funds were received until they were deposited. Similarly, we examined 15 cash receipts totaling \$24,409 for 10 high school activity accounts during our audit period. We found that for all 15 cash receipts, it took 11 days or more from the date funds were received until they were deposited. For example, a receipt totaling \$500 was collected on May 26, 2006 and not deposited at the bank until 95 days later on August 29, 2006. Additionally, receipts totaling \$10,334.40 (including \$1,575 in cash) were collected on January 23, 2007 and not deposited at the bank until 13 days later on February 5, 2007. When cash is not deposited promptly, it is subject to increased risk of loss or misuse.

Finally, we examined the extra-classroom central treasurers' ledgers and supporting documentation during the audit period to verify that checks and cash receipts were issued sequentially and could be accounted for. We found all checks that were disbursed during our audit period were issued sequentially and could be accounted for. We also scanned approximately 260 press-numbered receipts issued by the central treasurers during our audit period. Because two of the numbered receipts were missing, we were unable to verify whether all cash receipts collected by activity funds during our audit period were properly accounted for by the central treasurers.

The Board and District officials should take appropriate steps to better account for activity fund monies. The Board must improve oversight and District officials should perform their duties in accordance with Regulations and good business practices. The failure to comply with established policy requirements, appoint a faculty auditor, ensure that deposits are made on a timely basis and properly account for cash receipts increases the risk that errors and irregularities could occur and remain undetected and that activity fund monies could be lost or misused.

Recommendations

1. The Board and District officials should ensure that activity funds are maintained in accordance with District policy and the Regulations of the Commissioner.
2. Faculty advisors should ensure that a student ledger is maintained for each activity account showing all receipts, disbursements and a running balance.

3. The Board should appoint a faculty auditor to oversee the management of extra-classroom fund monies.
4. District officials should ensure that cash and checks collected for extra-classroom activities are deposited on a timely basis.
5. The central treasurers should ensure that all activity fund receipts can be accounted for properly.

Information Technology

The District relies on its information technology (IT) system for computer education, access to the Internet, e-mail communication, storing student data, maintaining financial records and reporting to State and Federal agencies. Therefore, the IT system and the data it holds are valuable resources. If the IT system fails, the results could range from inconvenient to catastrophic. Even small disruptions in electronic data systems can require extensive employee and consultant hours to evaluate and repair. The Board and District officials are responsible for controlling and monitoring access to IT systems and developing a formal disaster plan to reduce the risk of misuse, alteration or loss of computerized information and data, and to provide guidance on the recovery of information and data in the event of a disaster.

Controls over the District's fiscal management system and network were inadequate. The Board and District officials did not control and monitor access to the District's IT system or have a formal disaster plan in place. Because the Board and District officials did not develop policies and procedures to address these issues, the District's IT systems and electronic data have been subject to an increased risk of loss or misuse.

Computer System Access

Strong password and other access controls must be in place, and access to computerized applications¹ and administrative rights must be restricted, to provide reasonable assurance that computer resources are protected from unauthorized modifications and to reduce the risk that the District's IT system and electronic data will be subject to loss or misuse.

Passwords — Passwords are associated with user accounts, and are used to identify, authenticate, and limit the access of individuals attempting to access a computerized system or application. The more complex a password, the more difficult it is for an unauthorized user to obtain access to the District's system. As passwords can be guessed, copied, or overheard, passwords must be held to complexity requirements and changed periodically, and access rights must be revoked upon a set number of failed sign on attempts. Additionally, passwords must be stored in an encrypted format to prevent browsing and compromise. Using these techniques significantly increases the

¹ The District uses one financial software application to process payroll and maintain employee leave accrual records, and a different financial software application to process all other financial transactions.

District's protection and reduces the risk that unauthorized users can gain access to sensitive information.

We found the District's passwords are not complex, there is no requirement that they be changed periodically, and they are not always unique or required. In addition, access rights are not revoked upon a set number of failed sign on attempts and passwords are not always stored in an encrypted format.

The District's IT Department provides students with a password when they are first given access to the network, whereas employees create their own passwords. Student passwords consist of only four digits and employee passwords are only required to be four characters in length. Furthermore, once granted access to the network students and employees are not required to change passwords periodically. Additionally, access rights are not revoked upon a set number of failed sign on attempts.

We also found the District's payroll and leave accrual financial applications do not require passwords to access the applications. Currently, the Assistant Superintendent for Business, District Treasurer, Business Office Coordinator, District Clerk, payroll clerk, and accounts payable clerk have access to both applications which are installed on their computers. As a result, if these employees are signed into their computers, anyone could access the payroll and leave accrual financial software applications through an unattended workstation.

In addition, the tax collector, District Treasurer, Business Office Coordinator, payroll clerk, and accounts payable clerk have access to the application used for maintaining records of tax collection. Although passwords are required to access the application, the passwords are basic and lack any complexity requirements. Furthermore, once users are assigned access to the application, they are not required to change passwords periodically and access rights are not revoked upon a set number of failed sign on attempts. We also found that all of the individuals with access to the application, except for the tax collector, use the same user name and password, which is the vendor default account.

Further, the financial software applications used to process all other financial transactions contain password fields to access the applications. However, the passwords are basic and lack any complexity requirements, password changes are not enforced on a periodic basis, and access rights are not revoked upon a set number of failed sign on attempts. Additionally, we found that if users have

not established a password within the system for these applications, these individuals are capable of accessing the software application without the use of a password. Furthermore, passwords are not stored in an encrypted format within the applications to prevent browsing and compromise. As a result, individuals with administrative rights to the application have the ability to view all users' passwords, and thus have the capability to sign on as any user that has been given access to the applications.

Access Limits — To provide for a proper segregation of duties and internal controls, a financial management system must only allow users access to the computer functions that are necessary to fulfill their job responsibilities and prevent users from being involved in multiple aspects of financial transactions. In addition, because administrative rights provide the ability to add new users, change users' passwords and rights, and control and use all aspects of the software, a person with administrative rights must not be involved in the Business Office function.

We found that several users have greater access than necessary to fulfill their job responsibilities and the ability to be involved in multiple aspects of financial transactions. In addition, two individuals involved in the Business Office function also have administrative rights.

The District's payroll, leave accrual, and tax collection financial software applications do not have access controls. As a result, the applications do not allow for the ability to restrict the access levels of different users, which allows users to have full access to all levels of the application. Currently, the Assistant Superintendent for Business, District Treasurer, Business Office Coordinator, District Clerk, payroll clerk, and accounts payable clerk have access to the payroll and leave accrual software applications, although only the payroll clerk and District Treasurer's job responsibilities entail processing payroll and/or leave accrual transactions on a day-to-day basis. Additionally, the tax collector, District Treasurer, Business Office Coordinator, payroll clerk, and accounts payable clerk have access to the tax collection software application, although only the tax collector's job responsibilities entail maintaining records of tax collection on a day-to-day basis.

The software applications used to process all other financial transactions have access controls. The four access categories allowed are "All Access," "Some Access," "Read Only," and "No Access." The ability to restrict the access levels of different users is a good control feature for computerized financial software applications. However, several users have been granted access to functions that are not needed for them to

fulfill their day-to-day job responsibilities. For instance, the Business Office Coordinator and Director of Buildings and Transportation have the ability to create vendors and cash disbursements, and also the ability to print checks, although these functions are not needed for them to fulfill their day-to-day job responsibilities. Furthermore, the payroll clerk has the ability to create vendors and funds, although these functions are not needed for her to fulfill her day-to-day job responsibilities.

We also found that the Assistant Superintendent for Business and District Treasurer have administrative rights to the District's financial software applications, which give them the ability to add new users as well as change users' passwords and rights. With this ability, these individuals are able to control and use all aspects of the financial software applications providing an opportunity for the manipulation and concealment of transactions.

Due to these control weaknesses, we performed a variety of tests of payroll payments, maintenance of leave accruals and accounts payable payments to verify that the transactions made during the audit period were appropriate. Our testing did not reveal any material exceptions. However, the failure to have strong password and access controls in place and to restrict access to business functions and administrative rights increases the risk that unauthorized users can gain access to sensitive information and exposes the District's IT system and electronic data to the risk of loss or misuse.

Audit Logs

A computerized fiscal management system should provide a means of determining, on a constant basis, who is accessing the system and what transactions are being processed. Audit logs (commonly known as audit trails) maintain a record of activity by system or application. The audit log must provide information such as the identity of each person who has accessed the system, the time and date of the access, what activity occurred, and the time and date of sign off. Ideally, management or management's designee would review this audit log to monitor the activity of users who access the software. This tool provides a mechanism for individual accountability, reconstructing events and problem monitoring.

The District's fiscal management software does not generate the reports needed to properly monitor financial activity. Specifically, the software will not generate change reports showing, for example, vendor changes, or additions or deletions of general and subsidiary ledger accounts. In addition, the software does not have the ability to generate reports showing the identification of those who entered transactions into the system (audit logs). These are significant internal

control weaknesses, which could allow unauthorized activities to occur and remain undetected and unresolved.

Physical Security Over Component Parts

District officials are responsible for physically securing and controlling access to network servers and components to ensure that the District is protected from loss and the assets are used effectively for their intended purpose. However, we found that four wiring racks were not physically secured; but located in unlocked rooms. As a result, unauthorized individuals could gain access to these wiring racks, which could result in services being disrupted, costly equipment being damaged, destroyed or stolen, and personal information being compromised.

Disaster Recovery

The District's internal control system should include a formal disaster 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 must 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. However, the Board has not established a formal disaster plan, and consequently, in the event of a disaster, District personnel have no guidelines or plan to follow to minimize or prevent the loss of equipment and data or guidance on how to implement data recovery procedures.

Recommendations

6. District officials should adopt policies and procedures to strengthen internal controls relating to the use of complex passwords, enforcement of password changes on a regular basis and the revocation of access rights after a set number of failed sign on attempts.
7. District officials should ensure that all financial software applications include strong passwords and other access controls, and provide for the storage of passwords in an encrypted format and the ability to create audit logs and other reports to monitor user activity.
8. District officials should remove vendor default accounts from all applications as they are added to the system.
9. District officials should evaluate employee job descriptions and assign computer system access rights to match the respective job functions.
10. The Board should give the responsibility for assigning user access to the financial software applications to someone who is independent of the Business Office.

11. The Board should adopt policies and procedures to strengthen internal controls relating to IT equipment storage and disaster recovery.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

Plattsburgh City School District

49 BROAD STREET
PLATTSBURGH-NY-12901-3396
518-957-6000 (Office)
518-561-6605 (FAX)
www.plattscsd.org

James M. Short
Superintendent of Schools
518-957-6002
jshort@plattscsd.org

Jay C. Lebrun
Assistant Superintendent for Business
518-957-6003
jlebrun@plattscsd.org

Thelma M. Carrino
Director of Instruction
518-957-6006
tcarrino@plattscsd.org

May 3, 2008

[REDACTED]
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, NY 12901

Dear [REDACTED]

This letter has been prepared in response to the preliminary draft findings of the Office of the State Comptroller's examination of the Plattsburgh City School District. As I mentioned during the exit conference, the examination process was one which my staff and I found very useful and rewarding. The field auditors who completed this examination were thorough yet personable, and we enjoyed many constructive discussions with them about internal controls.

On behalf of the Superintendent and the Board of Education Audit Committee, I wish to express our general agreement with the comments contained in the examination report. I believe that most Districts recognize the extra-classroom activities as a source of vulnerability of controls, and while PCSD's efforts may well be impressive relative to most Districts, there remain areas of improvement therein. As was discussed during the exit conference, meetings with the various club advisors, and the inception of formalized system of record-keeping (ledgers) have already taken place. I have found these advisors, in general, to be a conscientious group, and I am confident that your comments will yield a higher level of attention to the timeliness of deposits and to the detailed recording of all financial activities. Further, in anticipation of the 2008-2009 fiscal year, the PCSD Board of Education will discuss the recommended creation of a faculty auditor for the extra-classroom activities.

The other area of comment – information technology – continues to be an area of focus for PCSD's central administration. Discussions regarding the complexity and frequency of change of passwords have taken place since before the introduction of the Comptroller's 5-point plan. As we discussed during the exit conference, concerns about the number and complexity of passwords which our staff must manage have created concern that passwords might be written down in an accessible location – thereby undermining the information security intent of the recommendation. Discussions and research about the appropriate strategy for managing such passwords continue. The physical vulnerability of the District's IT infrastructure is currently being addressed via the introduction of locking mechanisms on equipment storage spaces, and

– MISSION –

Our mission is to educate each student of the Plattsburgh City School District by creating challenging, supportive, and interactive learning that advances intellectual, physical, social, and cultural development.

the segregation of such IT spaces from general storage space. Finally, I have begun investigating (with other Districts and with NERIC officials) the move to another financial management system – one which better addresses the control concerns outlined in your report. In the meantime, I understand that [REDACTED] is working diligently to address these very issues, and I will monitor their progress towards that end.

Again, my colleagues and I view the outcome of this process quite positively. While we take any recommendations seriously, I view the comments outlined in your report as easily addressable and, in the context of your office’s findings statewide, relatively minor. The Board of Education at PCSD contracted for Internal Audit services before such a requirement was introduced by the Comptroller, and I believe that this forward-looking initiative has proven effective. I look forward to your eventual return to Plattsburgh City School District, and I wish you every success with your ongoing efforts.

Sincerely,



Jay Lebrun

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 objectives and scope by selecting for audit those areas most at risk. We selected internal controls over extra-classroom activities and information technology for further audit testing.

Within extra-classroom activity funds, we reviewed all District policies relating to extra-classroom activities and interviewed the central treasurers. We also observed transactions, and examined extra-classroom activity fund records such as the central treasurers' ledgers, payment order forms, cancelled checks, bank statements, validated deposit slips, student activity deposit forms, cash receipts, and cash receipts book to determine the effectiveness of internal controls over extra-classroom activity fund functions and any associated effects of deficiencies in those controls.

Within information technology, we reviewed all District policies related to computer use and information technology. We interviewed the District's technology coordinator and senior network and systems administrator specifically regarding network passwords, physical access to the system, controls within the fiscal management software, and disaster recovery plans. We physically inspected the location of system equipment and viewed Business Office employees' computer screens to determine the software that each employee could access. Additionally, we examined the following records and reports: purchase orders, claims packages, warrants, payroll journals, payroll transaction reports, personnel files, Board minutes, collective bargaining agreements and individual employment contracts, leave accrual summaries, timesheets, cancelled checks, cash receipts, and bank reconciliations.

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

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
<http://www.osc.state.ny.us/localgov/>

APPENDIX D
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Steven J. Hancox, Deputy Comptroller
John C. Traylor, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BUFFALO REGIONAL OFFICE

Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Room 1050
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie,
Genesee, Niagara, Orleans, Wyoming counties

ROCHESTER REGIONAL OFFICE

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe,
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates
counties

SYRACUSE REGIONAL OFFICE

Eugene A. Camp, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison,
Oneida, Onondaga, Oswego, St. Lawrence counties

BINGHAMTON REGIONAL OFFICE

Patrick Carbone, Chief Examiner
Office of the State Comptroller
State Office Building, Room 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Otsego, Schoharie, Sullivan, Tioga, Tompkins
counties

GLENS FALLS REGIONAL OFFICE

Karl Smoczynski, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Clinton, Essex, Franklin, Fulton, Hamilton,
Montgomery, Rensselaer, Saratoga, Warren, Washington
counties

ALBANY REGIONAL OFFICE

Kenneth Madej, Chief Examiner
Office of the State Comptroller
22 Computer Drive West
Albany, New York 12205-1695
(518) 438-0093 Fax (518) 438-0367
Email: Muni-Albany@osc.state.ny.us

Serving: Albany, Columbia, Dutchess, Greene,
Schenectady, Ulster counties

HAUPPAUGE REGIONAL OFFICE

Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE

Christopher Ellis, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Orange, Putnam, Rockland, Westchester
counties