



# Kingston City School District Internal Controls Over Selected Financial Operations

Report of Examination

Period Covered:

July 1, 2006 — December 4, 2007

2008M-162



Thomas P. DiNapoli

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	2
<b>EXECUTIVE SUMMARY</b>	3
<b>INTRODUCTION</b>	5
Background	5
Objective	5
Scope and Methodology	5
Comments of District Officials and Corrective Action	6
<b>CASH RECEIPTS AND DISBURSEMENTS</b>	7
Recommendations	11
<b>PAYROLL</b>	12
Segregation of Duties	12
Board Authorizations	14
Time Records	16
Recommendations	17
<b>INFORMATION TECHNOLOGY</b>	19
Recommendations	24
<b>CLASSIFICATION OF EMPLOYEES</b>	26
Recommendation	26
<b>APPENDIX A</b> Response From District Officials	27
<b>APPENDIX B</b> Audit Methodology and Standards	31
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	33
<b>APPENDIX D</b> Local Regional Office Listing	34

# State of New York Office of the State Comptroller

---

---

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

November 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 Kingston City School District, entitled Internal Controls Over Selected Financial Operations. 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 Kingston City School District (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 14 schools in operation within the District, with approximately 8,000 students and 1,780 full-time and part-time employees. The District's budgeted expenditures for the 2007-08 fiscal year were \$130.8 million which were funded primarily with State aid, real property taxes, and grants. The District, as a public employer, enrolls its eligible employees in the New York State and Local Employees' Retirement System (ERS).

#### **Scope and Objective**

The objective of our audit was to review the District's internal controls over cash receipts and disbursements, payroll, and information technology for the period July 1, 2006 to December 4, 2007. We also reviewed certain payroll schedules for the fiscal years 2003-04 to 2005-06. Our audit addressed the following related questions:

- Are internal controls over cash receipts and disbursements appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over payroll appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over information technology appropriately designed to adequately safeguard District assets?
- Did the District's process for classifying workers ensure that the persons the District enrolls in ERS are entitled to membership in the ERS?

#### **Audit Results**

We found weaknesses in several of the District's financial operations. District officials have not established appropriate policies to guide employees' actions, or officials did not implement established policies. For example, the Treasurer and Deputy Treasurer had administrative access to the IT system

and their duties were not properly segregated. District officials have not established formal policies and procedures describing employees' responsibilities for cash receipts and disbursements. The Treasurer and Deputy Treasurer perform incompatible duties involving the key financial functions of collecting cash and school tax receipts, authorizing transactions, having custody of assets, and keeping records. Even though we found no inappropriate transactions during our testing, there is no assurance that errors and irregularities would be prevented, detected, or corrected timely.

Also, the District has not established policies and procedures for processing payroll. The Payroll Supervisor's duties were not adequately segregated and included entering all payroll changes, processing the payroll, and supervising the distribution of the payroll checks. We also found that payroll transactions totaling \$28,235 were not authorized by the Board and time records lacked the necessary information and signatures. Although our audit testing did not identify any material exceptions, there is an increased risk that errors or irregularities could occur and remain undetected and uncorrected.

Our audit of the District's IT system disclosed weaknesses in the controls over users' access to financial information and student data applications. District officials have not adopted policies and procedures to address password and log-in security requirements. There are no procedures for ensuring that all District data is removed from IT equipment before that equipment is disposed. The District had no formal procedures for the assignment of user access rights and remote user access to the computer system. Because of the inadequate internal controls over the IT system, the District is at an increased risk of unauthorized users accessing the system and causing the misuse, loss, or inappropriate modification or disclosure of the District's sensitive information.

In addition, District officials have not developed formal IT security and disaster recovery plans. Therefore, District personnel have no security guidelines to follow to help prevent the loss of equipment and data and no data recovery procedures to use in the event of a disaster. As a result, the District is at increased risk of costly disruption of its operations and the potential loss of valuable data.

Lastly, we noted a weakness in internal controls over the District's process for classifying workers who the District enrolls in the ERS. Although we found no material exceptions, this weakness could increase the risk that the District could improperly enroll non-employees (independent contractors) in the ERS.

### **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 Kingston City School District (District) is located in the City of Kingston and the Towns of Kingston, Ulster, Hurley, Marbletown, New Paltz, Rosendale, Saugerties, Esopus, and Woodstock in Ulster 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 14 schools in operation within the District, with approximately 8,000 students and 1,780 full-time and part-time employees. The District's budgeted expenditures for the 2007-08 fiscal year were \$130.8 million which were funded primarily with State aid, real property taxes, and grants. The District, as a public employer, enrolls its eligible employees in the New York State and Local Employees' Retirement System (ERS).

## Objective

The objective of our audit was to review the District's internal controls over cash receipts and disbursements, payroll, and information technology. Our audit addressed the following related questions:

- Are internal controls over cash receipts and disbursements appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over payroll appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over information technology appropriately designed to adequately safeguard District assets?
- Did the District's process for classifying workers ensure that the persons the District enrolls in ERS are entitled to membership in the ERS?

## Scope and Methodology

During this audit, we examined the District's internal controls relating to cash receipts and disbursements, payroll, and information technology for the period July 1, 2006 to December 4, 2007. We also reviewed certain payroll schedules for the fiscal years 2003-04 to 2005-06.

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 GML, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

## Cash Receipts and Disbursements

District officials are responsible for establishing internal controls to ensure the District's cash receipts are adequately safeguarded and that cash disbursements are properly authorized. Such controls include policies and procedures that provide for adequate segregation of duties, documented authorization of transactions, and independent oversight of cash operations in a timely manner.

Cash receipts and disbursements policies must contain specific guidance and information for District employees responsible for handling and accounting for cash assets. Effective policies address the collection, recording and deposit of cash; the disbursement of District moneys by check; and prescribed procedures for executing wire transfers. An effective system of internal controls provides reasonable assurances that cash transactions are properly initiated, approved, documented and recorded; cash receipts are deposited in a timely manner; disbursements are proper; and that cash is safeguarded to prevent loss or theft.

An effective system of internal controls over cash operations provides for the distribution of duties so that no one individual controls all phases of a transaction. Proper segregation of duties also requires that the work of one employee be independently checked in the course of another employee's regular duties. When the segregation of incompatible duties is not established, additional controls must be in place that provide for the timely, independent review of all significant transactions. Having key financial duties (i.e., authorizing transactions, keeping records, and receiving and disbursing cash) performed by one or two individuals within one office with little or no oversight weakens internal controls and significantly increases the risk that errors and or irregularities might occur and go undetected and uncorrected.

Although the District has a policy manual, there are no specific written procedures to direct District personnel in the performance of their duties related to receiving, disbursing, transferring and investing cash. The Treasurer's Office is charged with receiving, disbursing, transferring, investing, and accounting for virtually all District moneys. This arrangement does not provide for adequate segregation of these key functions. In addition, there are no compensating controls in place to mitigate the effect of this lack of segregation of duties. Although we found no exceptions, these weaknesses in internal controls place the District at an increased risk of receipts being unrecorded or not

deposited, disbursements being erroneous or improper, and District moneys being inappropriately transferred or invested.

Cash Receipts — In general, the Treasurer and Deputy Treasurer are responsible for collecting and depositing funds, recording receipts, and reconciling bank accounts. The Treasurer and Deputy Treasurer also serve as the Tax Collector and Deputy Tax Collector. They collect taxes and other receipts, make deposits, perform bank reconciliations, make wire transfers and prepare journal entries.

We found weaknesses in the internal controls over general cash receipts and tax receipts. The District has not established written policies and procedures that adequately address the receipt, recording and depositing of general cash receipts and tax receipts. Both the Treasurer and Deputy Treasurer interchangeably collect,<sup>1</sup> record, deposit, and verify District cash receipts. The Treasurer's Office received over \$124 million in general fund revenues for the 2006-07 fiscal year. Cash receipts data is not signed-off on before the information is entered into the accounting system. This weakness in internal controls is further compounded by a lack of sufficient oversight. Bank statements are opened by the same individuals who perform the reconciliations, and are not reviewed by someone independent of the collecting, recording, and depositing functions. Further, the Treasurer does not document his review of the Deputy Treasurer's work and no one independent of the Treasury function reviews the work of the Treasurer. In addition, as discussed in the Information Technology section of the report, these individuals have unlimited access to the District's financial software with little or no independent review.

School tax receipts are one of the District's most significant revenues. For the 2007-08 fiscal year, the District collected over \$62 million in school taxes. These payments, of cash and checks, are received by the Treasurer/Tax Collector's Office through the mail and the collection windows. In this combined office, the same individuals are responsible for both accounting for tax collections and maintaining custody of those moneys.

District management has not established adequate internal controls over the District's tax collection procedures. Two cashiers, the Tax Collector (Treasurer) and the Deputy Tax Collector (Deputy Treasurer) collect tax receipts. In addition, the Tax Collector or the Deputy Tax Collector opens and processes the majority of the school tax receipts received by mail. Each person collecting tax receipts documents their individual daily receipts which are then verified by the Tax Collector or Deputy. In effect, the Tax Collector and Deputy could verify their

---

<sup>1</sup> Other cashiers also are involved in the collection of tax receipts.

own work. A third cashier only posts receipts to the tax collection accounting program. After entry, the Tax Collector or Deputy reconciles the daily postings and prepares and makes deposits. There is no written documentation of any review of the cashiers' work or the Tax Collector's or Deputy's activities.

Because of these weaknesses, we traced 15 tax receipts amounting to \$41,485 from daily cash sheets to the bank statement. We found no errors or irregularities. However, there was no evidence that these cash sheets were reviewed and approved by either the Tax Collector or the Deputy. The lack of written guidance and the failure to properly segregate the District's cash receipt duties could result in cash being collected, not recorded or deposited and not detected.

Cash Disbursements — Generally, the Treasurer and Deputy Treasurer are responsible for signing checks to disburse District funds based upon various authorizations. During the audit period, the Treasurer's Office disbursed over \$186 million, not including payroll checks and tax refunds. Bank reconciliations are performed by the same individuals who sign District checks disbursing funds. These two business functions are incompatible when performed by the same individuals because unauthorized disbursements could be made by an individual and intentionally concealed by that individual in a subsequent bank reconciliation. In addition, the District has not established written policies and procedures that adequately address the cash disbursement function. As a result, we examined 200 checks totaling \$2,695,608 for supporting documentation such as a claim and invoice and to determine if the charges were reasonable and proper. In general, we found that these disbursements were proper and supported.

We also reviewed tax refund checks issued due to overpayments by taxpayers and escrow agents, and corrections of tax bills sent by the assessors. In the 2006-07 fiscal year, 61 refund checks totaling \$89,358 were issued. In the 2007-08 fiscal year, 65 refund checks totaling \$80,562 were issued. We reviewed a sample of 10 school tax refunds and other adjustments amounting to \$4,724 for propriety of amount and authorization. Although our tests did not identify any material errors or improper payments, when one or two individuals are able to disburse District moneys and also reconcile the bank statements, there is an increased risk that inappropriate disbursements could be initiated and concealed.

Wire Transfers — The Treasurer's Office is responsible for making wire transfers and transfers millions of dollars each month. This includes six to nine wire transfers a month from the general fund

checking account alone. The Treasurer or Deputy Treasurer initiates and completes wire transfers. No other District staff are involved in the wire transfer process. The banks that send and receive the wire transfers do not independently confirm the transfer with District officials.

District management has not established adequate internal controls over the District's electronic fund transfers that address the initiating and confirming of wire transfers. We examined nine transfers amounting to \$19,264,581, and found no initiating approval by anyone independent of the Treasurer's Office. For three of the transfers amounting to \$11,500,000, supporting documentation was not signed by the initiator or approved/initialed by a supervisor. For seven transfers amounting to \$11,264,581, there was no evidence of the receiving bank confirming receipt of the transfer. While these transfers were proper, the failure to properly segregate the District's wire transfer duties and receive supervisory approval could result in inappropriate wire transfers being initiated and not detected.

Investment of Cash — General Municipal Law requires school districts to adopt a written investment policy that, among other things, establishes procedures for the monitoring, controlling, depositing and retaining of investments. The District's investment policy, adopted by the Board in April 2006, does not contain these required procedures.

During the audit period, the District had an average of \$23 million in money market accounts. Over the same time period, investments in certificates of deposit (CDs) ranged from \$11.0 to \$33.5 million. Most funds, as they are received by the Treasurer's Office, are deposited in District money market accounts. As the Board-designated investment officer, the Treasurer initiates and records the investment of District moneys in CDs with commercial banks operating in the area. The Treasurer calls the banks for rates, compares those rates to the money market rates and invests in CDs with those banks having favorable rates. He also records the redemption of each certificate and any interest earned on the investment. Employees in the Treasurer's Office also reconcile all bank accounts, including the money market accounts.

The Board has not established adequate internal controls over the District's investing activities. No one independent of the Treasurer's Office reviews the District's banking activity, including the investing of funds. Because of the lack of controls, we examined six investments totaling \$33 million for proper recording in the District's records, proper recording of interest earned, and compliance with District policy and General Municipal Law. We found no errors or irregularities

during our test of investments. However, we found that the Treasurer does not document the CD rates offered by the competing banks.

Given the general lack of segregation of duties found within the Treasurer's Office it is even more imperative that the Board adopt adequate monitoring controls over investment activities (as required by statute). Without improved controls over investing activities, errors or irregularities could occur and go undetected and uncorrected.

## **Recommendations**

1. The duties and responsibilities of the Treasurer and Deputy Treasurer related to general fund and tax receipts should be segregated. When this is not practical, District officials should provide additional oversight of these financial activities.
2. District officials should develop written policies and procedures for cash receipts and disbursements.
3. District officials should implement policies and procedures to ensure that tax collections are properly supervised and that no one individual collects, records, accounts for, and deposits daily tax receipts.
4. The Board should adopt a written policy for wire transfers. The policy should require that wire transfers be authorized by someone independent of the Treasurer's Office. It should also establish specific security procedures for confirming wire transfer orders and require dual approvals for non-routine wire transfer transactions.
5. The Board should develop adequate policies and procedures for the investment of District funds.

## Payroll

An effective system of payroll controls consists of comprehensive policies and procedures that address such things as the proper segregation of payroll duties, Board authorizations of positions and pay rates, and maintenance of adequate time records. Payroll duties must be sufficiently segregated so that no one individual can control all aspects of a transaction. It is also important that access rights to the payroll information system be assigned so that proper segregation is established/maintained. Employee positions and pay rates should be approved by the Board prior to becoming part of the payroll system. Time records need to contain sufficient detail and proper supervisory approvals before payments are made.

The District employed approximately 1,780 full-time and part-time employees throughout 2007 and paid wages and salaries of more than \$68.5 million. Because of the number (and variety) of employees, the breadth of on-site and off-site work locations, and the dollar amounts involved, payroll is a high risk area for the District. An effective system of internal controls can provide District managers with reasonable assurance that those risks are mitigated.

We found weaknesses in the District's internal controls over payroll. Payroll duties are not properly segregated and access to the computerized payroll information is not properly restricted. Employees with payroll responsibilities have the ability to initiate payroll transactions and make changes to all aspects of computerized data. The payroll supervisor has user access rights and is directly responsible for creating computerized employee records, adding and deleting employees from the payroll software, entering all payroll data changes, entering hours worked and salaries paid, and preparing paychecks. These weaknesses could allow an individual to process unauthorized paychecks. In addition, the Board did not authorize certain appointments, conditions of employment and salary increases. Without such authorization, there is no assurance that employees are properly paid. Finally, we found that certain time records (claims) did not contain sufficient detail or the necessary approvals to support their payment. A lack of detail records and approvals increases the risk that employees may be paid for time not worked.

### Segregation of Duties

District officials are responsible for establishing internal controls that provide reasonable assurance that payroll transactions are processed as authorized. To help ensure that payroll transactions are proper, authorizing, processing, and paying responsibilities should be segregated among several individuals. Payroll duties must be

assigned so that no one person has control over all or most of the payroll process. When a proper segregation of duties is established, the information system must support that segregation and not allow for its circumvention. To maintain a proper segregation of duties and internal controls, the information system should limit access for users to only those functions needed to perform their job responsibilities.

When it is not practical to adequately segregate payroll duties, District officials should establish compensating controls. Such controls can include having someone independent of the preparation process perform a review of the completed payrolls and supporting records. These reviews could include a periodic verification that payrolls are based on actual hours or days worked (or authorized and available leave time) and whether the Board authorized the hourly rates or annual salaries used in payroll computations. Periodic reviews could also compare net payrolls to payroll journals and/or analyze the payrolls for unusual names or dollar amounts.

The payroll supervisor is directly responsible for creating computerized employee records, adding and deleting employees from the payroll software, entering all payroll data changes and salaries paid, and preparing paychecks. Although the District has a Personnel Office independent of payroll processing, the payroll supervisor has access to the computerized personnel records. Also, there is no independent review of payrolls and payroll activities. An employee with this range of payroll duties and with no effective supervision could make unauthorized changes to pay rates and/or withholdings or pay nonexistent employees without detection. District officials should correct these control weaknesses to limit the risk that payroll errors or irregularities could occur and not be detected and corrected in a timely manner. Because of these payroll weaknesses, we reviewed payroll payments to five key employees. We also tested a sample of 50 payroll disbursements to other employees and examined employee pay records for changes in withholdings and earnings. Our tests revealed no inappropriate payments.

We reviewed payroll payments to the Treasurer, Deputy Treasurer, Payroll Supervisor, District Clerk and Coordinator of Network and Technology. We reviewed 11 payments to these individuals totaling \$23,390 and found that four overtime payments to three of these individuals, totaling \$3,316, lacked approval by the appropriate supervisor prior to payment. For example, two claims<sup>2</sup> for \$1,312 and \$348 to the Payroll Supervisor and the District clerk (who helps enter time sheet information into the payroll system), respectively,

---

<sup>2</sup> Overtime payments are based on claims submitted which are then entered into the payroll system.

lacked supervisory approval. In addition, no approved time sheet was presented to support a second overtime claim for the Payroll Supervisor of \$856. We found that two of the unapproved overtime claims for \$348 and \$856 for the Payroll Supervisor were entered into the payroll system by the Payroll Supervisor.

We also tested a sample of 50 payroll disbursements to various employees, totaling \$143,692, to trace hours worked, rates paid and additional pay (overtime) to supporting documentation and authorization. We found that for three payments to two substitute teachers and a home teacher, totaling \$2,938, supporting time records had no supervisory approvals. Also, included in the sample were 14 non-routine payments, totaling \$50,069, for retroactive payments, salary changes, longevity payments, sick leave and vacation leave buy-backs. Because these payments are not routine and require extensive calculations, there is a greater risk for error. Despite this increased risk, we found no evidence that anyone reviewed these calculations before the information was entered into the payroll system for processing.

Due to the lack of documented authorizations and segregation of duties, there is an increased risk that payments could be made that employees are not entitled to.

We also found that the Payroll Supervisor made unauthorized changes to her personnel records. Authorizations for changes in deductions and to have moneys withheld from paychecks should be completed and signed by each employee and submitted to the Personnel Office for processing and filing. The Personnel Office then enters this information into the system. This authorization function should be segregated from payroll processing. Because the Payroll Supervisor was able to perform this function, we reviewed her payroll records for changes in earnings and withholdings and found that she personally changed her payroll records six times to increase the number of personal exemptions, without written authorizations. The lack of proper segregation of duties allowed the Payroll Supervisor to make these changes and would also permit her to make changes to other employees' withholdings. While we found no unusual changes to other employee records, without the proper segregation of payroll duties there is an increased risk that errors and/or irregularities might occur and go undetected.

## **Board Authorizations**

As a component of the budgetary process, the Board's approval of contracts and salary agreements with administrators, teachers, and non-instructional employees authorizes pay rates and various benefits, including paid leave, health insurance, and other issues related to their terms of employment. The authorization of positions and salaries by

the Board serves as a limit on payroll expenditures. The Board's involvement also provides some assurance that individuals will not be added to the payroll without proper approvals and that employees will not be paid more than their authorized rates.

We found that payroll transactions were performed without proper Board authorization. Appointments, conditions of employment and salary increases were made by District personnel without Board approval. As a result, the District paid an additional \$28,235 to employees without Board authorization.

Appointments — According to District policy, at the recommendation of the Superintendent, the Board is responsible for appointing all District employees and setting their salary or wages. During our test of the 50 employees for proper authorization, we found that one employee received a stipend of \$12,000 as a supervisor. The Board had appointed this individual as a teaching assistant but not as a supervisor. We were informed that the Assistant Superintendent for Curriculum and Instruction did not seek a Board appointment for the supervisor position because the stipend was included in a grant. Another employee, a teacher, received a similar stipend of \$12,000 (without Board authorization) as supervisor for a second supervisory position in the grant program.

We also found that the Director of Athletics requested payment of a stipend to a coach for an intramural sport. Based on this request, a payroll clerk changed the employee's payroll information to include an \$823 coaching stipend. There was no Board resolution authorizing this appointment. The Assistant Superintendent for Personnel and Administration told us that it has been District practice to have the Board appoint some but not all coaching stipends.

Conditions of Employment — Conditions of employment should be clearly detailed in written contracts, agreements or policies approved by the Board. This helps prevent any misunderstandings or misapplication of the Board's requirements and ensures that costs are properly contained.

Bus monitors submit bi-weekly payroll claims which list the dates worked. The claims we reviewed did not include beginning and ending times. Therefore, the District has no evidence that monitors worked the actual number of hours they were paid. However, District officials said that under past practice, each bus monitor receives pay for a minimum of four hours a day for morning and afternoon trips. We were provided no evidence that this practice was authorized by the Board.

Salary Increases — Depending upon an individual’s employment classification, a Board-approved collective bargaining agreement, a personal contract, or Board policy establishes compensation issues. To control payroll costs all compensation items should be agreed upon and approved by the Board and carefully and uniformly administered.

We tested the salary increases of five Business Office employees to determine if the increases were supported by the terms of the Board-approved payment schedule for the fiscal years 2003-04 to 2005-06. Subsequent to the schedule adoption, the Board Clerk left the District and the Board appointed a new clerk in April 2004 at a salary of \$37,000 annually. In an undated salary memo, the Superintendent set a salary increase of \$1,264 for the new clerk beginning in July 2004. There was no confirming Board resolution for this increase and subsequent salary increases for the Board Clerk.

We examined supporting documentation for 15 new employees hired during the audit period. In September 2006, the Board appointed an employee as a probationary cleaner at a salary of \$24,744 annually. The Payroll Supervisor determined that the salary was from the 2004-05 salary schedule and corrected the salary to \$26,892, an increase of \$2,148, without notifying the Personnel Office or seeking Board authorization. Personnel office staff explained that the warehouse manager had erroneously supplied the 2004-2005 salary for the appointment that was approved by the Board.

Without detailed Board-authorized payroll contracts, agreements and policies, there is an increased risk that inappropriate payments may be made and/or unauthorized individuals may be employed. Without effective monitoring of payroll processes, activities and transactions, there is an increased risk that errors and irregularities will not be detected.

## **Time Records**

Properly designed and maintained time records are an important component of good internal controls over payroll. Employees should maintain daily records of their hours worked and/or absences. These records help supervisors and those individuals processing payroll determine each employee’s regular and overtime (if applicable) hours, as well as update the employee’s accumulated leave balances. Time records need to contain the information necessary to account for an employee’s entire workday, including starting and ending times, leave charges and meal periods. Supervisors must review each completed time record to verify the hours worked and, when satisfied, approve the claim/record before submitting it to payroll for payroll processing. Erroneous or incomplete information on these time records can cause

delays or errors in payments and could result in employees being paid for time that they did not work.

The District pays certain employees based on claim vouchers submitted to document their time worked. School bus monitors are required to submit all of their time worked using claims vouchers. Other employees who provide additional services are also required to submit vouchers for the additional time worked. These claims are then used as a source document (time sheet) for entering information into the payroll system.

We examined 89 claim vouchers, totaling \$21,982, submitted for two payroll periods documenting hours worked by bus monitors<sup>3</sup> and other employees. We reviewed these claims to determine if they contained sufficient time-keeping information and proper supervisory approvals. We found the following:

- No documentation of the dates worked on five claims
- No documentation of the starting and ending times on 47 claims
- No documentation of supervisory approval on 16 claims
- Insufficient information to verify that a proper supervisory review was conducted on 22 claims
- Supervisory approval given one day before the end of the pay period for 19 claims.

Time records lacking complete information, key signatures, or prior approvals should not be processed and should be returned to the department or work unit that submitted them. Using incomplete or unapproved time records to process payroll payments increases the risk that the District may pay employees for work not performed.

## Recommendations

6. District officials should segregate the payroll duties of authorization, processing, and distribution. In order to properly segregate duties, access rights within the payroll system should be appropriately restricted. If proper segregation is not practical, then effective oversight should be provided by someone independent of those duties who should periodically review payroll operations and activities.

---

<sup>3</sup> Because bus monitors are guaranteed a minimum of four hours of pay for each day worked, this reason was provided as justification for the general lack of detail on claim vouchers submitted by bus monitors.

7. All claims for overtime payments should contain supervisory approval and be properly supported.
8. The Board should require that all appointments, conditions of employment, and salary changes be presented for authorization. The Board should also establish methods for monitoring compliance with this requirement.
9. The Board should investigate the payments made without proper authorization and seek reimbursement if appropriate.
10. District officials should require that all claims for payroll purposes contain sufficient detail and proper supervisory approvals prior to payment.

## Information Technology

The use of information technology (IT) affects the fundamental manner in which the District initiates, processes, records, and reports transactions. The extent to which the District uses computer processing in significant accounting applications, as well as the complexity of that processing, determines the specific risks that IT poses to the District's internal control. The District's widespread use of IT presents a number of internal control risks that must be addressed. These risks include unauthorized access to data, unauthorized changes to data in master files, and potential loss of data. The District can use a combination of automated controls and manual controls to address these risks.

An effective system of internal controls includes policies and procedures to protect data from loss by intentional or unintentional manipulation, or corruption. Policies and procedures need to limit user access to only authorized persons; allow data to be restored if it is unavoidably lost or corrupted; and address user privileges, passwords, and disaster recovery. The District should also utilize available system-generated reports to further strengthen internal controls.

District officials did not effectively address the safeguarding of the IT system by establishing appropriate control policies and procedures. Adequate and deliberate protection of computer resources is necessary for operations to proceed smoothly. The District has not developed a comprehensive security plan or a disaster recovery plan. It does not have effective policies and procedures in place regarding access rights, audit logs, passwords, remote access, equipment disposal or confidential information. As a result, the District is placing its IT data and system at risk for possible compromise by theft, intentional or unintentional manipulation, loss, or corruption.

Security Plan — An entity-wide program for security planning and management is the foundation of an entity's security control structure. The program needs to establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

The District does not have an IT security plan. Without a comprehensive, well-designed plan, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or

critical information and resources and/or ineffective use of IT security resources.

Data Backup and Disaster Recovery — An effective internal control system for IT includes a formal disaster recovery plan with policies and procedures to minimize the loss of essential data and to maintain or quickly resume critical operations if a disruption occurs. As part of a formal disaster recovery plan, data stored on computers and servers should be backed up (a duplicate copy of information made) on a routine basis and stored remotely in a secure environment. Such data would then be available to be restored in the event that the original data was lost. Periodically, IT personnel need to verify the integrity of the backup data and test the effectiveness of the restoration process by restoring the data from the backup copy.

The District has not prepared and tested a secure disaster recovery plan for its financial system. District financial data is backed up by Ulster BOCES. However, the District does not periodically restore the data, and therefore is unable to verify the integrity of the data and the effectiveness of the restoration process. Lastly, the District has no plan to help personnel minimize or prevent the loss of equipment and data, or to provide guidance for implementing data recovery procedures. As a result of these control weaknesses, the District's IT assets are at an increased risk of loss and/or damage and potentially costly disruptions to their critical operations.

Access Rights — Internal controls over users' access to the IT system provide reasonable assurance that computer resources — which include equipment, data files, application programs, and computer-related facilities — are adequately safeguarded. To control electronic access, a computer system or application needs a process to identify and differentiate users. Accordingly, user accounts, normally created by the system administrator, contain information on each user such as passwords and access rights to files, applications, directories, and other computer resources. Effective access controls prevent users from being involved in multiple aspects of financial transactions and from accessing unauthorized areas where they can intentionally or unintentionally destroy or change critical data. Key access controls involve the segregation of duties within the IT system by limiting user access rights to only those applications necessary to perform their duties.

District management has not developed policies and procedures for module access rights to safeguard against unauthorized access to the District's IT system. Management did not restrict user access to only those modules that were required by individual employee job descriptions and/or official duties. For instance, the payroll

supervisor can create and maintain computer and manual checks; generate a cash disbursement check; perform automated trust and agency account payment processing; add, update, delete and review employee information; and create and maintain earnings associated with a selected employee. Because the payroll supervisor can enter and delete employees; enter timesheets and earnings; calculate, generate, and print payroll checks; and reconcile payroll, she has the ability to initiate and conceal inappropriate transactions.

In addition, the Treasurer and Deputy Treasurer, the senior account clerk, and one account clerk in the Business Office have override rights to the computerized financial system. These rights allow an individual to make changes to data and/or override existing controls. The granting of override rights to any employee that has significant involvement in business operations and financial transactions increases the risk that financial information or resources could be misused. Because of the segregation of duties issues in the Treasurer's Office and the fact that this office has the authority to prepare and execute wire transfers, create journal entries, and access banking information, with override rights to the accounting system software they have the ability to initiate and then conceal inappropriate transactions.

Audit Logs — A computerized financial system should provide a means of identifying all individuals who have accessed the system and all transactions that were processed. Audit logs (or trails), exception reports, and change reports maintain a record of activity by system or application process, as well as changes to the financial system. Audit logs 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 log-off. Exception reports provide detailed exceptions to ordinary transactions. Change reports provide changes made to the financial application (for example, vendor or payroll changes, or the addition or deletion of general and subsidiary ledger accounts). Management or management's designee should review these reports to monitor user activity and changes to the data, to provide a mechanism for individual accountability, reconstructing events and monitoring problems.

The Treasurer's Office has been assigned user rights to produce audit trail reports. The Treasurer informed us that he does not produce or review these reports on a regular basis. He believes that security was established when user access rights were designated. Other District officials have not been made aware of these reports. In addition, exception and change reports are not used to independently monitor activities.

District officials did not compensate for the lack of segregation of duties in the Treasurer's Office by reviewing audit logs from the District's accounting system. As a result, we reviewed the audit logs for seven periods ranging from several days to several weeks for any indications of inappropriate use or access. We did not find any instances of inappropriate use or access. However, since no District employee had been assigned to routinely perform such reviews, management did not have the ability to detect and properly address unauthorized activities. As a result, errors or irregularities could occur and not be detected.

Passwords/Lock-Out Policy — The use of strong passwords and the implementation of a lock-out policy help protect computer resources from unauthorized access. To access a network, computer, or application, users must enter their user name and password. The computer compares this information with the user account database. If a match is found, access is granted as provided for the user account. A lock-out policy automatically prevents access to the user's account after a set number of failed log-in attempts. Strong passwords contain combinations of uppercase and lowercase letters, numbers, and punctuation, and are at least eight characters long. They should not contain words found in the dictionary, hardware or software names, repeated letters or numbers, addresses, phone numbers, or the user's name, family members' names, or pet names. Passwords should be changed every 30 to 90 days to protect confidentiality. Under no circumstances should passwords be written down or shared with others as this would compromise all the other associated controls.

District management has not adopted and implemented password security policies. We identified significant weaknesses in the District's system related to password security. Due to the sensitive nature of these findings, we have communicated our concerns to the District in a separate, confidential letter.

Remote Access Policy — Remote access is the ability to access the District's computer system from the Internet or other external source. Remote access causes security risks for an otherwise secure network because remote computers, even if physically secure, may be vulnerable to threats from other systems. Remote access needs to be controlled, monitored, and tracked so that only authorized individuals are allowed to access the District's computer system or to retrieve data from it.

The District has not implemented policies and established written procedures that address how remote access is granted, who is given remote access, and how remote access to the District's networked computer system and financial computer data is monitored, tracked

and controlled. All staff have remote access capabilities to their e-mail accounts. Certain administrators are also given remote access to student or financial accounts through a secure gateway. The servers allow access if their name is on the system. Remote users are cautioned to be sure their home systems are secure. The appropriate Assistant Superintendent authorizes the access. However, no written policies exist for remote access.

Because virtually all District accounting records and reports are computer generated, and no audit log is produced to monitor or control remote access, an unauthorized user could change computer data (i.e., add/delete employees, change pay rates, add/delete vendors, and change vendor information) and the unauthorized activity could go undetected and uncorrected. As a result, the District is at risk of unauthorized changes to the system, programs, or data without the knowledge of District officials.

Equipment Disposal — Sensitive and confidential information and software must be safeguarded throughout its useful life. Such information must be cleared from computer hard drives, disks, thumb drives, and other equipment and media before they are disposed of or transferred to another use. Organizations need to have a plan that clearly describes the organization's security management program and the policies and procedures that support it, including procedures for the secure disposal of electronic information.

The District's hard drives (and other storage devices) are not cleaned and sanitized when disposed of. The District does not have procedures to clear sensitive information and software from computers, disks, and other equipment or media when disposed of or transferred for other use. If sensitive/confidential information is not fully sanitized, it may be recovered and inappropriately used or disclosed by individuals with access to the discarded or transferred equipment and media.

Confidential Information — Confidential information in electronic format needs to be closely protected. Confidential information includes sensitive District financial information, and personal identity information for students and staff. Security of confidential information is achieved by establishing usage restrictions and implementation guidance for portable and mobile devices; documenting, monitoring, and controlling device access to District networks; and having appropriate officials authorize the use of portable and mobile devices.

E-mails, floppy disks, CDs or thumb drives are cost-effective, convenient methods of storing, transporting, and downloading electronic information. However, the ease of use, small size, and

minimal technological constraints of these devices create risks that must be assessed and controlled. These devices enable electronic data, including confidential records, to be removed from District control with little difficulty and subsequently accessed by unauthorized individuals.<sup>4</sup> They are easily concealed — or lost — and require no complex set-up procedure to use. Accordingly, it is essential for the District to have a security management program that includes policies and procedures for the secure storage and transport of sensitive information on these auxiliary devices.

The District does not have policies and procedures to guide its employees concerning confidential information found in the District's databases and in the secure use of e-mails, floppy disks, CDs or thumb drives. Without adequate controls over the use of these devices, the District is at an increased risk of the retrieval and misuse of confidential information by unauthorized individuals.

## Recommendations

11. District officials should develop and implement a comprehensive security plan that identifies and addresses its significant IT risks. This plan should be updated periodically.
12. District officials should implement a disaster recovery plan that includes the secure back-up and retrieval of critical data. The plan should also include guidance for personnel to follow to prevent or minimize the impact of disasters and to follow in the event that the system is compromised.
13. District officials should review current access rights and limit each employee's access to only those rights they need to perform their assigned duties. These rights should be reviewed periodically to ensure that proper segregation of duties is maintained through the granting of access rights. Override rights should be limited and assigned only to someone without business and financial responsibilities.
14. District officials should routinely review audit logs, exception reports and change reports for unusual or unauthorized activities.
15. District officials should establish a password policy and improve controls over password security.
16. District officials should review its current remote access procedures and limit such access based on business needs. A

---

<sup>4</sup> The casual use of these devices also increases the risk of transferring computer viruses to District computers.

formal policy should be adopted that defines these business needs and establishes controls over remote access.

17. District officials should establish policies and procedures for the proper sanitizing of computer data from all equipment and media prior to transfer or disposition of these items.
18. District officials should establish policies and procedures for the secure storage and transport of sensitive information residing on computer hard drives, portable media, and peripherals.

## Classification of Employees

Local governments and school districts obtain services from both public employees and independent contractors and consultants. It is important that public employers enroll only public employees, elected officials and public officers in ERS to ensure that only persons entitled to New York State and Local Employees' Retirement System (ERS) membership receive ERS service credit. The Office of the State Comptroller's *Financial Management Guide for Local Governments*<sup>5</sup> provides information to help distinguish between independent contractors and employees. The ERS provides its own checklist of indicators<sup>6</sup> that can help localities and school districts make this determination correctly. In addition, as of April 3, 2008, the Office of the State Comptroller (OSC) made enhanced regulations available that more clearly define how local governments and school districts can determine whether providers of professional services are employees or independent contractors. These regulations are posted on the OSC website.<sup>7</sup>

For the period July 1, 2006 to February 14, 2008, we audited the status of persons the District enrolled in ERS to determine whether these individuals met the criteria for employee classification as established by the *Financial Management Guide for Local Governments* and ERS indicators. Although we did not find any material exceptions, we identified a weakness in the District's controls over the classification process.

The District does not have formal criteria (procedures) applied to new positions or hires to determine if the individual performing services should be reported to the ERS as an employee or if the individual should be classified as an independent contractor. Unless District officials correct this control weakness, they are at an increased risk of improperly enrolling non-employees in ERS.

### Recommendation

19. District officials should strengthen controls over worker classification processes to help ensure that they correctly determine the status of individuals who work for the District in compliance with the Guide and the regulations posted on the OSC website.

<sup>5</sup> *Financial Management Guide for Local Governments*, Subsection 8.4020, page 1, issued December 1992

<sup>6</sup> The ERS Checklist, entitled Distinguishing Between an Employee and an Independent Contractor, is available from ERS.

<sup>7</sup> [www.osc.state.ny.us](http://www.osc.state.ny.us)

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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



**KINGSTON CITY SCHOOL DISTRICT**

SIXTY-ONE CROWN STREET KINGSTON, NY 12401  
Phone 845.339.3000 • Fax 845.339.9279

DAVID M. FLETCHER, D.M.D.  
PRESIDENT-BOARD OF EDUCATION

GERARD M. GRETZINGER  
SUPERINTENDENT

November 13, 2008

[REDACTED]  
Office of the State Comptroller  
22 Computer Drive West  
Albany, New York 12205-1695

**RE: Response Letter - Report of Examination 2008M-162**

Dear [REDACTED]

I am responding to the Kingston City School District Audit Report regarding the Internal Controls over Selected Financial Operations covering the period July 1, 2006 through December 4, 2007. Overall, I am pleased to say that the Audit was a fair examination of the District's financial operation. The Kingston City School District strongly believes in continuous improvement of our operations in order to become more efficient and serve our students, staff, and community members to the best of our ability. We are grateful for the manner in which your staff conducted the State Comptroller's Audit. We found them to be very professional and knowledgeable when interacting with District personnel and Board of Education trustees, and felt that the entire process was a good learning experience.

I have discussed the recommendations found in the Audit Report with my review committee and we are in the process of taking the necessary steps to develop our Corrective Action Plan (CAP) that will adequately address the auditors' recommendations. In the subsequent paragraphs, we have outlined a response to each of the auditors' recommendations. The District's response in some instances reflects improvements and/or compensating controls over processes that were implemented during the audit process.

I. Cash Receipts and Disbursements

1. Compensating controls were implemented during the audit process to mitigate risk associated with general fund cash receipts. The Assistant Superintendent for Business and Operations and other staff outside of the Treasurer's Office are now providing oversight regarding the cash receipt process that includes bank statements and reconciliation review and sign off. The District has implemented procedures to document review by noting signature and date on all paperwork.

Kingston City School District Mission:

*To educate, inspire, and graduate students who are excellent in scholarship and character  
and are empowered to reach their maximum potential as responsible and productive members of society.*

The District recognizes that the tax receipt process needs to have independent review and oversight, even though no material weaknesses or exceptions were found during the course of the audit. We will work to adjust this process accordingly and will elaborate further in our Corrective Action Plan (CAP).

2. The Board of Education and District Officials have recognized the need for written policies and procedures for all District financial and non-financial activities in order to give guidance to District staff on correct procedures to take when performing tasks and to ensure that adequate controls are in place to mitigate risk. The Kingston City School District is working diligently to complete our written polices and procedures which are inclusive of tax collections, wire transfers, and investment of District funds as outlined in the Audit Report.

## II. Payroll

1. During the course of the audit process, the District implemented additional oversight requirements via review and signature of payroll reports (i.e. exception reports) by the Assistant Superintendent for Business and Operations. However, after reviewing the Audit Report, we realize that more in-depth, periodic reviews of payrolls need to be performed in order to mitigate risk.
2. In order to segregate the duties in the payroll office, the Kingston City School District has hired a payroll clerk who will assume some of the duties now performed by the payroll supervisor. In addition, we are working to segregate the human resources functions from the payroll functions and restrict access in our financial system accordingly. We will elaborate further when our Corrective Action Plan is finalized.
3. The Kingston City School District is working to establish methods for monitoring compliance with the requirement that all appointments, conditions of employment, and salary changes are properly authorized by the Board of Education. Our Corrective Action Plan will appropriately address the auditors' recommendations.
4. The District is in the process of investigating the payments noted in the Audit Report that lacked proper authorization and will seek reimbursement, if appropriate.
5. The Kingston City School District is in the process of revising payroll forms, including timesheets, to include sufficient detail and updating procedures to ensure that proper supervisory approvals are noted prior to payment.

## III. Information Technology

1. During the Audit process, the District's technology department had draft copies of plans written, but they were not finalized or yet approved by the Board of Education. We are in the process of reviewing and finalizing our comprehensive security plan that will identify and address significant information technology risks with a methodology regarding periodic review and update. We will elaborate further in our Corrective Action Plan.
2. The Kingston City School District recognizes the need for a disaster recovery plan that includes secure back-up and retrieval of critical data. We are working to create policies and procedures that adequately address this issue to "...minimize the loss of essential data and to maintain or quickly resume critical operations if a disruption occurs." Furthermore, the plan will include guidance for personnel to follow to prevent or minimize the impact of disasters and to follow in the event the system is compromised. The plan will have a methodology for periodic testing, review, and update.
3. The Kingston City School District recognizes the importance of safeguarding sensitive District information and the integrity of our computer network system. As such, we are working to

develop comprehensive policies and procedures regarding access rights, passwords and lock outs, remote access, equipment disposal, and safeguarding confidential information as noted in the Audit Report.

4. We will review employee access rights and determine the needs associated with job duties. Authorizations regarding access to vital District information will be adjusted accordingly and measures implemented to review and update these needs periodically.
5. A District Official outside of the IT Department will begin to review audit reports/logs, exception reports and change reports periodically to identify unusual or unauthorized activities.

#### IV. Classification of Employees

The Kingston City School District recognizes the need for written policies and procedures governing classification of workers, as either employees reportable to employee retirement systems or as independent contractors, to mitigate the risk of improperly enrolling non-employees in the retirement systems. We will utilize the resources afforded by the Office of the State Comptroller and ERS to formalize a written set of policies and procedures on classifying new hires or positions in order to strengthen our controls. The use of a checklist utilizing the enhanced regulations implemented by the State Comptroller as of April 3, 2008, will be implemented to assist District Officials in determining classification.

The State Comptroller's Audit has given the Kingston City School District an opportunity to thoroughly review our internal controls and has provided us with recommendations for improving upon our financial operation of the District. We will work diligently to develop and implement our Corrective Action Plan in order to run a more efficient and effective operation, thus giving more accountability for our taxpayer dollars. Again, on behalf of the District, I would like to thank you for the informative and comprehensive report regarding the financial operations of the Kingston City School District.

Sincerely,



Gerard M. Gretzinger

/ak

## APPENDIX B

### AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard District assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, and payroll and personal services.

During the initial assessment, we interviewed appropriate District officials, performed limited tests of transactions and reviewed pertinent documents, such as District policies and procedures manuals, Board minutes, and financial records and reports. In addition, we obtained information directly from the computerized financial databases and then analyzed it electronically using computer-assisted techniques. This approach provided us with additional information about the District's financial transactions as recorded in its databases. Further, we reviewed the District's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed, and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided upon the reported objectives and scope by selecting for audit those areas most at risk. We selected cash receipts and disbursements, payroll, and information technology for further audit testing.

- We interviewed employees in the Business Office concerning school tax receipts, cash disbursements, wire transfers and investments, and the segregation of duties for cash disbursements and procedures used in payroll processing.
- We interviewed employees in the Business Office and IT Department concerning access rights to the computerized financial system. We also reviewed user rights and permissions documentation, and selected certain users to determine if their user rights were appropriate.
- We interviewed employees in the Personnel Office concerning payroll and leave benefits.
- To identify any associated effects of the deficiencies found, we selected various claims for review for multiple procedures (legitimate, reasonable, proper and supported, and that endorsements were proper). We focused on adherence to policies, procedures, laws and regulations pertinent to cash receipts and disbursements and payroll.
- We reviewed tax collections and disbursements. We traced collections to deposit records and bank statements to assure that funds received were deposited. We tested tax refunds and traced to supporting documentation.
- We also reviewed payments to various employees, wire and automated clearinghouse transfers, and samples of payroll disbursements. We verified that employees receiving compensation

were not fictitious by reviewing the Detailed Payroll Check Register Reports, and personnel files for supporting documentation.

This testing included an examination of the following:

- Transaction history reports
- Claims packets
- Cancelled checks
- Cash control accounts
- Board minutes
- School Tax Receipts
- Employee personnel files
- Collective bargaining agreements and individual employment contracts
- Leave accrual records
- Computerized payroll registers and employee earnings records
- Salary history screens.

Within the classification of employee area, we reviewed the District's process for classifying workers to ensure that the persons the District enrolls in ERS are valid public employees rather than independent contractors.

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, Suite 1032  
Buffalo, New York 14203-2510  
(716) 847-3647 Fax (716) 847-3643  
Email: [Muni-Buffalo@osc.state.ny.us](mailto:Muni-Buffalo@osc.state.ny.us)

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

##### **ROCHESTER REGIONAL OFFICE**

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

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

##### **SYRACUSE REGIONAL OFFICE**

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

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

##### **BINGHAMTON REGIONAL OFFICE**

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

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

##### **GLENS FALLS REGIONAL OFFICE**

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

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

##### **ALBANY REGIONAL OFFICE**

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

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

##### **HAUPPAUGE REGIONAL OFFICE**

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

Serving: Nassau, Suffolk counties

##### **NEWBURGH REGIONAL OFFICE**

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

Serving: Orange, Putnam, Rockland, Westchester  
counties