



Hastings-on-Hudson Union Free School District

Internal Controls Over Selected Financial Activities

Report of Examination

Period Covered:

July 1, 2006 — August 3, 2007

2007M-303



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	3
EXECUTIVE SUMMARY	5
INTRODUCTION	7
Background	7
Objective	7
Scope and Methodology	8
Comments of District Officials and Corrective Action	8
INFORMATION TECHNOLOGY	9
User Access Rights	10
Software Changes	13
Disaster Recovery	14
Risk Management	14
Recommendations	16
CASH DISBURSEMENTS	17
Recommendations	18
PAYROLL	19
Segregation of Duties	19
Board Authorization for Additional Benefits	20
Recommendations	20
APPENDIX A Response From District Officials	21
APPENDIX B Audit Methodology and Standards	24
APPENDIX C How to Obtain Additional Copies of the Report	26
APPENDIX D Local Regional Office Listing	27

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

March 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 Hastings-on-Hudson Union Free School District, entitled Internal Controls Over Selected Financial Activities. This audit was conducted pursuant to Article V, Section 1 of the State Constitution, and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

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

Respectfully submitted,

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



State of New York Office of the State Comptroller

EXECUTIVE SUMMARY

The Hastings-on-Hudson Union Free School District (District) is governed by the Board of Education (Board) which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are three schools in operation within the District, with 1,633 students and 366 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$37 million, which were funded primarily with State aid and real property taxes.

The District obtains information technology (IT) hardware and software support from the Lower Hudson Regional Information Center (LHRIC). The District paid the LHRIC \$562,900 for its services during the 2006-07 fiscal year. The Director of Technology is responsible for managing the District's IT system. Her duties include coordinating services provided by LHRIC; overseeing the District's computer system; and assigning and terminating user rights in the District's network and student data software. The Business Official is responsible for assigning and terminating user rights in the District's financial software application.

Scope and Objective

The objective of our audit was to examine the internal controls over selected financial activities for the period July 1, 2006 to August 3, 2007. Our audit addressed the following related questions:

- Are internal controls over the District's information technology system appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over cash 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?

Audit Results

Our audit of the IT system disclosed weaknesses in the controls over users' access to the District's financial information and student data applications. District officials have not adopted policies and procedures to address password and log-in security requirements. The District had no formal

procedures for the proper authorization, assignment, modification, and documentation of user access rights to the computer system. The Business Official assigned certain Business Office employees and business officials user rights that were not consistent with their duties, weakening the segregation of duties within the financial software application. Further, there was no formal process or responsibility assigned for notifying the Director of Technology and the Business Official when employees were hired or terminated. As a result, the user rights of five former employees were not terminated in a timely manner when the employees left District service. 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 adopted policies and procedures that address changes made to the District's computer hardware and software systems. There is no system to document what changes were made, when, and by whom. Additionally, District officials have not assessed the risks associated with the outsourcing of IT functions and have not instituted a data classification system to adequately safeguard data from inappropriate modification or disclosure. District officials also have not developed a formal disaster recovery plan. Therefore, District personnel have no guidelines to prevent the loss of equipment and data, and no data recovery procedures to follow 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.

The District's internal controls over cash disbursements were inappropriately designed and operating ineffectively. District officials have not established formal policies and procedures describing employees' responsibilities for cash disbursements. The payroll and accounts payable clerks had unsupervised access to the Treasurer's signature disk and retained custody of checks until they were mailed. Further, the Treasurer did not compare checks to an approved claims warrant or certified payroll register before or after they were signed. As a result of these control weaknesses, the District is at increased risk of errors or improper payments being made without being detected and corrected.

Finally, the District has not established policies and procedures for processing payroll. The payroll clerk's duties were not adequately segregated and included entering all payroll changes, processing the payroll, and distributing the payroll checks. In addition, the Board did not authorize payment made in excess of \$17,000 to the Director of Technology for additional administrative technology consulting work. As a result of these inadequate controls, there is an increased risk that errors or irregularities could occur, and District officials do not have adequate assurance that payments are for legitimate District purposes.

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 agreed with our recommendations and indicated that they have initiated, or planned to initiate, corrective action.

Introduction

Background

The Hastings-on-Hudson Union Free School District (District) is located in the Village of Hastings-on-Hudson in Westchester County. The District is governed by the Board of Education (Board) which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are three schools in operation within the District, with 1,633 students and 366 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$37 million, which were funded primarily with State aid and real property taxes.

The District obtains much of its information technology (IT) hardware and software support from the Lower Hudson Regional Information Center (LHRIC). The District paid the LHRIC \$562,935 for its services during the 2006-07 fiscal year. The Director of Technology is responsible for managing the District's IT system. Her duties include coordinating services provided by LHRIC and overseeing the District's computer system. The Director of Technology is also responsible for assigning and terminating user rights in the District's network and student data software. The Business Official is responsible for assigning and terminating user rights in the District's financial software application.

Objective

The objective of our audit was to examine the internal controls over selected financial activities. Our audit addressed the following related questions:

- Are internal controls over the District's information technology system appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over cash 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?

Scope and Methodology

We examined the internal controls over selected financial activities of the District for the period July 1, 2006 to August 3, 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 agreed with our recommendations and indicated that they have initiated, or 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*.

Information Technology

The District's IT system is a valuable and essential part of the District's operations, used to provide computer education, access the Internet, communicate by electronic mail (email), store student data, and maintain financial records. The potential consequences of a failure of the IT system range from inconvenient to severe; even small disruptions in processing can require extensive time and effort to evaluate and repair. Accordingly, District officials are responsible for establishing internal controls over the IT system to ensure that District assets are protected against waste, loss, and misuse. Such controls should address:

- User Access Rights — Restriction and monitoring of users' access to the IT system through secure passwords, system "lock-out" protection, appropriate restriction of access rights based on employees' job responsibilities, and policies and procedures for establishing and modifying user accounts
- Software Changes — Policies and procedures for the proper authorization, implementation, and documentation of changes to the District's software
- Disaster Recovery — A formal disaster prevention and recovery plan, including contingency procedures, to minimize disruption and/or resume critical operations in the event of a system failure
- Risk Management — An ongoing risk management process to identify, measure, monitor, and address potential risk from contractual arrangements with outside vendors, and classification of the District's data according to the level of risk.

The District incurred \$562,935 during the 2006-07 fiscal year for IT-related services provided by the Lower Hudson Regional Informational Center (LHRIC). Specifically, the District contracted with the LHRIC to provide computer hardware and software support that included installing and maintaining computer hardware and software; resolving technical hardware and software problems; providing security for all networks and software applications; performing data backups and warehousing the data; and providing disaster recovery services. Given the LHRIC's involvement in and access to the District's IT system, District officials have a

fundamental responsibility for monitoring all work performed by the LHRIC to ensure that services are provided as contracted, and that the District's IT system and data are adequately safeguarded.

Our audit found that District management did not establish sufficient internal controls over the key components of the District's IT system. As a result, the District's IT system and data are exposed to potential misuse, loss, or improper disclosure, increasing the risk that the District could incur costly disruption of its critical operations.

User 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 include:

- Secure password requirements and a “lock-out” mechanism to help block attempts at unauthorized access
- Segregation of duties within the IT environment by limiting user access rights to only those applications necessary for employees' day-to-day responsibilities
- Policies and procedures for authorizing and documenting changes to user access rights, for notifying IT personnel of required changes, and for limiting administrator accounts which allow individuals to change user access rights.

We found that District management has not developed policies and procedures for password security or other automated controls to safeguard against unauthorized access to the District's IT system. The Director of Technology did not establish requirements for password complexity, diversity, and confidentiality, and did not implement a system lock-out feature to protect against unauthorized access. Additionally, the District had no formal procedures for authorizing, assigning, changing, and documenting user permissions. Responsibility for notifying the Director of Technology and Business Official of personnel changes was not properly established, and the notification process used to add or remove user accounts was haphazard. As a result, the District's IT system and data is at an increased risk of misuse or damage, with the potential for unauthorized transactions

and changes to data being made without being detected and corrected in a timely manner.

Passwords/Lock-Out Policy — The use of passwords and the implementation of a lock-out policy work together to help protect computer resources from unauthorized modification. 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. District employees were not required to create complex passwords or keep them confidential. For example, one employee used family member names as passwords, and we observed another employee verbally giving his password to the Director of Technology. Additionally, employees did not change their passwords, and the lock-out function was disabled on all four computers in the Business Office, increasing the opportunities for unauthorized users to attempt system access. As a result, the District is at an increased risk of loss, exposure, or unauthorized modification of its sensitive information.

User Rights/Segregation of Duties — To ensure that adequate internal controls exist, District employees' rights to computer software applications should be based on their job responsibilities. Limiting user rights helps provide assurance that computer resources are protected from unauthorized use or modification. Good business practices require the separation of duties for recordkeeping, transaction approval, cash disbursements, cash custody, and bank statement reconciliations. By ensuring that no one individual controls all or most aspects of the cash management function, District officials can have greater assurance that the District's assets are being properly accounted for and safeguarded, reducing the District's risk of incurring errors and irregularities.

The Business Official did not adequately limit user rights to the District's financial software application. Business Office staff members had access to aspects of the accounting system that were not a required part of their job function, resulting in inadequate segregation of duties within the IT environment. For example, the accountant had access to the entire accounting and payroll modules including cash receipts and disbursements, payroll processing, bank reconciliation, and check signing functions. The Treasurer had user access to disbursements and budgetary fund transfers and had the ability to produce Federal 1099 tax reporting forms, even though all those functions were the assigned responsibility of the accounts payable clerk.¹ District officials indicated that additional access rights were provided to the staff to facilitate cross-training of various Business Office functions. Although there are legitimate reasons (such as cross-training) for granting additional access rights, such rights should be provided only on a limited basis and removed when they are no longer necessary for staff to perform their assigned duties. Because of these weaknesses in internal controls over access rights, we examined all payments made to the accountant, payroll clerk, and Treasurer, and related payroll items, for our audit period. We found no exceptions with these payments. However, inadequate controls over users' system access rights diminish the reliability of computerized data, and result in an increased risk of inappropriate modification or disclosure of data and the potential loss of District assets.

Authorization and Notification of Changes to User Access Rights — Effective access controls require that authorized users' specific needs, and any modifications, are approved by a senior manager and directly communicated in writing to the technology director or official in an equivalent position. It is especially important that an employee's termination or revocation of access rights be communicated immediately. A formal process for transmitting these authorizations, including standardized access request forms, reduces the risk of errors and misunderstandings. Although notification may be provided by the human resources department or by others, policies should be in place that clearly assign responsibility for such notifications. In addition, proper documentation of user access rights and authorizations helps District officials to ensure the segregation of duties, monitor the work of third-party providers of IT services, and identify and correct

¹ The Treasurer's assigned duties included recording cash receipts and reconciling bank statements. Although the Treasurer did not actually perform cash disbursements and budgetary fund transfers, having user access rights to those transactions – while also handling cash receipts and bank reconciliations – increases the opportunity for one individual to control the key incompatible aspects of the cash management function.

any errors or irregularities that may arise from unauthorized system access.

District officials have not developed policies and procedures for authorizing, making, and documenting changes to user accounts. There was no formal procedure to notify the Director of Technology when employees were hired or terminated, or to ensure that user accounts were promptly deactivated when employees left District service. For four out of 10 employees who left the District during our audit period, access to the financial system remained active for periods ranging from two days to approximately three months after they left District service. In addition, access rights to the student data software for a teacher who left the District on June 30, 2007 were not terminated until September 1, 2007.

Additionally, nine LHRIC staff members had administrator rights to the District's IT system, allowing them to change users' access rights to the financial software application. Although such changes were authorized by either the Director of Technology or the Business Official, extensive administrator rights – combined with inadequate documentation procedures – increase the difficulty of monitoring and controlling user access permissions.

The failure to establish policies and procedures to limit user access to those applications necessary for employees' job duties increases the risk of unauthorized changes being made. The lack of a formal notification process for user access rights increases the risk that former employees' access to the computerized information system is not terminated in a timely manner, placing the District's data at an increased risk of misuse, loss, or inappropriate disclosure. Further, if a problem did arise, the lack of proper documentation would hinder District officials in determining who authorized access rights, what those rights were, and when they may have been granted or revoked.

Software Changes

Establishing controls over the modification of software helps to ensure that only authorized changes and modifications are implemented. These controls include policies, procedures, and techniques for proper authorization, testing, approval, and documentation of all software and software modifications; and for properly controlled access to the distribution of software. The use of a standardized change request form and system-generated change logs, showing changes made to the software, helps ensure that requests are clearly communicated and approvals documented. Periodic reviews of change logs help verify that system changes match the approved change requests. Without effective change controls, there is an increased risk that security features could be inadvertently or deliberately omitted, that software

modifications may not work properly, or that processing irregularities could be introduced into the system.

The Director of Technology does not have a process to document who authorizes software changes, what changes are authorized, who makes them, and when they are made. Without a system to monitor software modifications the District is at risk of unauthorized software modifications, inadequate testing or implementation, or difficulties in subsequent modifications to the system.

Disaster Recovery

A system of strong internal controls includes a disaster recovery plan to address the potential loss of computer equipment and data, as well as procedures for recovery in the event of an actual loss. A disaster recovery plan includes precautions to minimize the effects of a disaster so that the district can maintain or quickly resume mission-critical functions. Typically, disaster recovery planning requires an analysis of business processes and continuity needs and may also include disaster prevention. If a district employs a third party for IT services, district officials are responsible for ensuring that the service provider safeguards the district from potential losses in the event of a disaster. Contracts with third parties must clearly specify the service provider's responsibilities for system backup and protection, including equipment, programs, and data files; maintenance and periodic testing of a disaster recovery plan, and of contingency operating procedures to follow if a disaster occurs; and communication of those test results to the district. Third-party contracts should also include business recovery timeframes that meet the district's operational requirements.

District officials have not developed a disaster recovery plan or contingency operating procedures, nor has the LHRIC done so. Although District officials stated that the LHRIC is responsible for disaster recovery, the District's contract with the LHRIC does not require the LHRIC to develop a disaster recovery plan or contingency procedures for the District. Further, the contract does not require the LHRIC to test the disaster recovery plan and contingency procedures regularly and provide the results to the District.

These contract deficiencies place the District at risk of losing important financial data and incurring serious interruption to District operations, such as not being able to process checks to pay vendors or employees. Because it lacks a disaster recovery plan and does not require the LHRIC to have adequate contingency procedures in place, the District may not be able to recover its data and/or promptly resume operations should a disaster occur.

Risk Management

Risk management is the process of identifying, measuring, and monitoring risk so that appropriate action can be taken to minimize

that risk. The pervasive use and complexity of a school district’s computerized applications can produce internal control risks such as unauthorized access to data, unauthorized changes to master files, and the potential loss or misuse of data. District officials are responsible for evaluating, overseeing, and addressing the risk related to its IT system and processes, including the risk arising from contractual relationships with IT service providers. An effective risk management process requires that a district’s management and board establish risk-based requirements in contracting with IT service providers; continuously monitor the nature and level of risk; and ensure that procedures, roles and responsibilities, and reporting mechanisms are clearly established and documented.

District management has not assessed the operational risk² associated with having IT functions performed by the LHRIC and has not instituted a system to adequately safeguard data from the risk of inappropriate modification or disclosure. District officials did not know which or how many employees at the LHRIC had access to their financial software application, nor did they monitor the LHRIC’s access to the IT system. In addition, granting nine LHRIC employees³ administrative rights to the District’s financial information — including the ability to change users’ access rights — increases the risk of inappropriate access to, and potential misuse of, the District’s financial data.

Lastly, the insurance maintained by the LHRIC does not insure against the risk associated with unauthorized access to data, unauthorized changes to data in master files, and potential loss of data. The insurance only guarantees replacement of computer equipment owned by the LHRIC. Therefore, if the District experiences a loss of data or financial disclosure resulting from acts of any of the nine LHRIC employees, the District would not be compensated for the loss. The failure of District officials to evaluate and address the risks associated with its contract with the LHRIC is a serious control weakness in the proper safeguarding of the District’s IT system, data, and operations.

Data Classification — The classification of a district’s computerized data assigns levels of protection to help minimize the risk of access and manipulation by multiple users. Accordingly, the most critical data should be classified so as to be subject to the strongest protective controls, and accessible only to those users whose level

² Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events (for example, failure of computer hardware or software, damage to physical assets, employee errors, fraud, and other factors that can disrupt business operations).

³ See “Authorization and Notification of Changes to User Access Rights,” above.

of responsibility requires access to it. The classification definitions should flow directly from the results of an effective risk assessment process that identifies threats, vulnerabilities, and potential negative effects of disclosing confidential data, or of failing to protect the integrity of data supporting critical transactions or decisions. District officials are responsible for developing and enforcing policies and procedures that specify classification categories, and for defining the related criteria on which the classification levels are based. All classifications should be reviewed and approved by a senior district official, maintained on file, and periodically reviewed to ensure that they reflect current condition.

Because the District did not have a risk management process, District officials did not develop policies for classifying data according to risk and for documenting the classification. Therefore, the District's sensitive and confidential data is at an increased risk of inappropriate use or modification, loss, or improper disclosure.

Recommendations

1. District officials should adopt policies and procedures to establish user access controls that safeguard the District's computerized data and other IT assets. These controls should include:
 - Requirements for password complexity and confidentiality, periodic changing of passwords, and limiting the number of unsuccessful log-in attempts
 - Assignment of users' access rights to software and data based on, and limited by, the requirements of their job duties
 - A formal change process for authorizing, establishing, modifying, and promptly deactivating user access rights. District officials should also limit the number of individuals having system administrator rights.
2. The Director of Technology should institute a process where changes to software and hardware are documented. This should include a record of authorizations, when changes were made, and who made the changes.
3. District officials should revise the District's contract with the LHRIC to ensure that it appropriately addresses disaster recovery.
4. District officials should implement policies and procedures for analyzing the risk associated with contracting for IT services, and for addressing those risks. The Director of Technology should institute a process where data is classified according to the level of risk, including documentation of these data classifications and definitions of related criteria.

Cash Disbursements

Effective controls over check processing include proper segregation of duties and appropriate management oversight of check production. When a computerized check signing disk is used, custody of the signature disk should be properly safeguarded and secured, preferably kept in the custody of and used under the sole control of the officer whose signature is on the disk. Restricting custody of the signature disk reduces the possibility for misuse. The employee responsible for preparing checks should not also be responsible for mailing or distributing them. In addition, a check log⁴ is an effective tool to help ensure that all checks are accounted for. Lastly, blank check stock must be adequately secured to guard against unauthorized manual preparation of checks.

Although the District paid approximately \$15 million in cash disbursements during the audit period, District officials have not adopted written policies and procedures describing employees' responsibilities for cash disbursements, nor have they implemented proper controls over checks. As a result, District officials do not have adequate assurance that payments are properly authorized and made for necessary and legitimate District purposes.

The District Treasurer's signature disk was kept inside a safe in the Business Office, which is kept open during the day. Approximately 13 District employees had access to the safe every day, including the payroll clerk and accounts payable clerk. Although the District used a log to keep track of who used the signature disk, this control was ineffective since the payroll clerk and the accounts payable clerk had unrestricted access to the disk. Computerized general-fund checks for claims against the District and payroll checks were processed, printed, signed using the Treasurer's signature disk (with or without the Treasurer being present), and distributed or mailed by the accounts payable clerk and payroll clerk, respectively. When these incompatible duties are performed by the same individual, District officials do not have adequate assurance that signed checks are used for legitimate business purposes.

The Treasurer did not compare checks to an approved claims warrant or certified payroll register before or after they were signed, or use a check log to make sure that all checks processed were accounted for.

⁴ A system-generated sequential listing of all checks issued using the computer system

Additionally, although the manual blank check stock was maintained in a safe, it was kept in an unlocked file cabinet (within the safe) located in the Business Office.⁵

Because of these internal control weaknesses related to check processing, we reviewed 110 contractual payments totaling \$249,758, made to the District's four Business Office employees during the audit period, to ensure the payments were for legitimate District purposes. Of these 110 payments, 104 were for salary and six were for overtime work. We found no exceptions. However, when internal controls over checks are not properly designed, there is an increased risk of waste or loss of District funds.

Recommendations

5. District officials should develop written policies and procedures for cash disbursements, including proper segregation of duties and managerial oversight.
6. The Treasurer should ensure that the payroll clerk and the accounts payable clerk use the signature disk only under her direct supervision.
7. District officials should ensure that someone independent of the check preparation process should mail or distribute checks.
8. The Treasurer should compare checks to an approved warrant or certified payroll register before they are signed.

⁵ Subsequent to our fieldwork, the Business Official put a lock on the file cabinet to secure the blank check stock and developed a check log to track all checks issued.

Payroll

Payroll is the District's most significant operating cost, accounting for approximately \$20 million in costs during our audit period. Therefore, it is essential that management design and implement effective controls over the payroll process. An effective system of internal controls includes well-developed policies, practices and procedures, effective managerial oversight, and proper segregation of duties. The Board must also ensure that appropriate controls over stipends (such as payment for consulting services) are established. These controls should ensure that stipend payments are made only when authorized by the Board through negotiated agreement, contract, Board policy, or Board resolution, and that such payments are calculated and made in the manner authorized by the Board.

Segregation of Duties

Proper segregation of duties results in payroll functions being divided between multiple employees so that no one employee performs most or all aspects of payroll, including the ability to add new employees to the computer system, update salary information, process payrolls, and print and distribute checks. District officials are responsible for implementing mitigating controls when they cannot adequately segregate duties. Such controls could include policies and procedures that provide for mandatory vacation, rotation of duties, and independent review of employees' work.

District officials have not developed policies and procedures for processing payroll and have not segregated payroll duties or instituted mitigating controls. The payroll clerk performed the incompatible duties of adding new employees into the computerized payroll system, inputting and updating salaries, inputting biweekly payroll information, and printing and distributing the payroll checks. As a result, the payroll clerk could have initiated improper transactions and concealed them.

To address these weaknesses in the segregation of payroll duties, we reviewed eight payroll changes made during August 2007 to determine if they were made according to Board authorization. We also selected 10 employees hired in fiscal year 2006-07 to determine if their hiring was authorized by the Board and if their salaries were paid according to contract. Our testing did not reveal any exceptions. However, when internal controls over payroll are not appropriately designed and/or are not operating effectively, there is an increased risk that errors or irregularities could occur and not be detected in a timely manner.

Board Authorization for Additional Benefits

All staff appointments require Board approval. Any change to an employee's pay or benefits that is not part of a signed collective bargaining agreement requires Board authorization, which must be documented in the Board's meeting minutes. The District's human resources department should then prepare documentation authorizing the payroll department to execute the changes. Without such authorization, payroll personnel lack the authority to execute changes to the payroll. Any additional compensation paid for special services is considered a change to the payroll and requires the same level of authorization as the hiring of new employees.

We reviewed payments to five of the highest-paid District employees to determine if their rate of pay was authorized by the Board and if payments were made according to their contract. There were no exceptions with four of the five employees tested. However, one employee was paid an additional \$17,379 for technology consulting services. Although these services were performed, there were no records to support Board authorization of the additional payment. When changes to employee payments are made without proper Board authorization, District officials do not have adequate assurance that District funds are spent for legitimate District purposes.

Recommendations

9. District officials should establish policies and procedures for payroll processing describing employee responsibilities and assigning duties so that incompatible functions are segregated.
10. Someone independent of the payroll process should periodically review changes to employee pay or benefits entered into the system, and compare these changes to documented approvals to verify that they were properly authorized.
11. The Board should authorize any additional compensation paid to employees.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

**HASTINGS-ON-HUDSON
UNION FREE SCHOOL DISTRICT**
27 Farragut Avenue
Hastings-on-Hudson, New York 10706

Phone: (914) 478-6201

Fax: (914) 478-3293

Ronnie Stowell
Interim Director of Business,
Operations and Finance

[REDACTED]
Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

March 3, 2008

Dear [REDACTED]

The following is in response to the preliminary audit findings issued by your office:

Information Technology

The Board of Education will formally adopt policies and procedures to establish user access controls that safeguard the District's computerized data and other IT assets. A draft policy, the goal of which is to ensure that financial networks and systems are adequately secured, has had its first reading by the Board of Education. The policy delineates a formal user password procedure that requires, among other things, users to change passwords every 90 days, a procedure that has already been instituted. The policy also sets forth a formal change process to authorize, establish, modify and change user rights, sets forth a formal user permission protocol to be based upon job responsibilities, outlines a backup and disaster recovery procedure, details the role of the Business Official for the responsibility of segregation of duties and defines the role of the systems administrator relating to remote access, security, risk, and reporting.

Additionally, the systems administrator for IT services has centralized the storage of all software and license agreements which are kept in a locked cabinet inside the server room. The District maintains a log of all software licenses detailing the date the software was placed on the server.

Cash Disbursements

The Board of Education has had its first reading of a policy relative to cash disbursements which includes disbursement procedures that require segregation of duties. The Treasurer has ensured that the payroll clerk and the accounts payable clerk are only using the signature disk under direct supervision. Someone independent of the check preparation process will mail and/or distribute the checks. The treasurer will compare checks to an approved warrant or certified payroll register before they are mailed.

Payroll

The Board of Education has had its first reading of a payroll policy that includes payroll procedures describing employee responsibilities and ensures appropriate segregation of duties. The business official and/or the treasurer will review changes to employee pay or benefits periodically to ensure that these changes are properly authorized and documented. The Board of Education will authorize any additional compensation paid to employees.

Sincerely,



Ronnie Stowell

Interim Director of Business, Operations and Finance

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 information technology, cash disbursements, and payroll for further audit testing.

Our audit procedures included:

- Interviewing employees in the District's Business Office to determine if the District officials adopted policies and procedures concerning payroll, cash disbursement, and information technology, and how they monitored compliance with these policies
- Interviewing employees in the District's information technology (IT) department and the Business Office concerning the network passwords, administrative rights in the District's financial software, and overall operations
- Interviewing Lower Hudson Regional Informational Center (LHRIC) staff concerning employees' access to the financial software system and to determine if the LHRIC carried adequate insurance to protect against risk associated with data loss and disclosure
- Reviewing the audit trail (report) of system changes to determine if access to the financial software was terminated in a timely manner
- Reviewing the computer-generated report of user access permissions to determine if employees' access to the financial software system was consistent with their job descriptions and to verify that such access did not compromise the segregation of duties

- Reviewing the District's contract with the LHRIC to determine what services it was responsible for providing to the District
- Reviewing the Director of Technology's job description to determine her responsibilities and qualifications
- Reviewing a list of employees who no longer worked at the District during our audit period to determine if access to employees' user rights was terminated in a timely manner
- Reviewing the list of LHRIC employees who had access to the financial software during our audit period to determine if there was risk to the District's data
- Reviewing network query reports to determine if access to the student data software was terminated in a timely manner
- Examining employees' personnel files, collective bargaining agreements, individual contracts, salary notification letters, and Board minutes to determine if employees with extensive access rights were properly authorized and paid according to contract or Board resolution
- Reviewing the vendor history report (which shows all non-wage payments) for our audit period to determine if additional payments were made to employees with extensive access rights. We also tested those payments to determine if they were legitimate payments and supported by adequate documentation
- Reviewing payroll changes performed in August 2007 to determine if they were properly authorized
- Reviewing electronic and/or manually processed cash transfers (which constitute disbursements) for legitimacy, approval, and accuracy.

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

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

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

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

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

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

LOCAL REGIONAL OFFICE LISTING

BUFFALO REGIONAL OFFICE

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

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

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, NY 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Orange, Putnam, Rockland, Westchester
counties