Northport-East Northport Union Free School District

Internal Audit Report on

Information Technology

TABLE OF CONTENTS

R.S. ABRAMS & CO., LLP
Accountants & Consultants for Over 75 years

Robert S. Abrams, *Managing Partner*
Marianne E. Van Duyne, *CPA*
Alexandria M. Battaglia, *CPA*

Board of Education
Northport-East Northport Union Free School District
158 Laurel Ave
Northport, NY 11768

We have been engaged by the Board of Education (the "Board") of the Northport-East Northport Union Free School District (the "District") to provide internal audit services with respect to the District's internal controls related to information technology for the period July 1, 2011 through April 17, 2012.

The objectives of the engagement were to evaluate and report on the District's internal controls pertaining to information technology and to test for compliance with laws, regulations, and the District's Board policies and procedures.

In connection with the following procedures, we have provided findings and recommendations for the internal controls related to information technology. Our procedures were as follows:

- Reviewed the District's policies, procedures and practices with regards to the internal controls related to information technology;
- Interviewed key District employees involved in information technology and performed a detailed walkthrough of the information technology processes;
- Performed a physical observation of the District's server rooms in the administration building and high school to verify the server rooms were properly secured and that the servers were reasonably protected from fire and floods;
- Reviewed the user permissions within the accounting information system to identify multiple active user accounts, generic user accounts, and possible permissions granted to various employees that may not be consistent with their job responsibilities;
- Performed a comparison of the master vendor file to the master employee file to identify possible conflicts of interest;
- Reviewed the master vendor file to verify that the master vendor file was complete, accurate, up to date and free of duplicate vendors; and
- Reviewed the District's Disaster Recovery Plan to determine that plan identified critical information technology infrastructure and equipment, established the most suitable recovery strategy for each application utilized by the District, and identified those individuals responsible for overseeing the disaster recovery process.

The results of our procedures are presented on the following pages.

Our procedures were not designed to express an opinion on the internal controls related to information technology, and we do not express such an opinion. As you know, because of inherent limitations of any internal control, errors or fraud may occur and not be prevented or detected by internal controls. Also, projections of any evaluation of the accounting system and controls to future periods are subject to the risk that procedures may become inadequate because of changed conditions.

We would like to acknowledge the courtesy and assistance extended to us by personnel of the District. We are available to discuss this report with the Board or others within the District at your convenience.

This report is intended solely for the information and use of the Board, the Audit Committee and the management of the District and is not intended to be and should not be used by anyone other than those specified parties.

Very truly yours,

R. S. Abrams + Co., LLP

R.S. Abrams & Co., LLP
April 17, 2012

GOVERNANCE

During our review of the Board policy manual, we noted that the District has adopted the following policies that relate to information technology:

Computer Network For Education
The District's *Computer Network For Education* policy, No. 4526, discusses access to the District's network and the Internet. The Board has designated the superintendent to establish regulations governing the use and security of the District's network. The superintendent has designated the assistant superintendent for instruction and administration to oversee the use of District computer resources, for preparing in-service programs for the training and development of District staff in computer skills and for incorporating the use of computers in appropriate subject areas. The policy also discusses how students will access the Internet, acceptable use and conduct rules, prohibited activity and uses, no privacy guarantees, sanctions and District responsibilities.

Internet Safety
The District's *Internet Safety* policy, No. 4526.1, discusses the efforts that the District will make to ensure that the Internet is safe and secure to use and the protection measures that will be utilized to block or filter Internet access. The assistant superintendent for instruction and technology is to monitor and examine all District computer network activities and for ensuring that staff and students receive training on their requirements.

Information Security Breach and Notification
The District's *Information Security Breach and Notification* policy, No. 8635, states that the superintendent, in accordance with appropriate business and technology personnel, is to establish regulations that identify and define types of private information that is to be kept secure, establish procedures to identify any breaches of security that result in the release of private information and establish procedures for notifying persons affected by the security breach.

Acceptable Use Policy For Users (Employees, Consultants, Volunteers and Other District Authorized Personnel) Use of District Computers, Networks, Internet Access, and E-Mail System
The District's *Acceptable Use Policy For Users (Employees, Consultants, Volunteers and Other District Authorized Personnel) Use of District Computers, Networks, Internet Access, and E-Mail System* policy, No. 9225, discusses acceptable use guidelines of the District's network services and prohibited uses. The policy also states that the employee shall be responsible for any losses, costs or damages incurred by the District related to violations of the employee computer, network, Internet and e-mail acceptable use policy and rules.

We also noted the following procedures in place at the District regarding information technology:

Compliance with Laws and Regulations
The District has policies and/or procedures related to maintaining confidentiality and integrity of the District's electronic information. Such procedures include, but are not limited to verifying social security numbers are not printed on reports, limiting software application access to only authorized personnel and further restrictions within the software applications to ensure that only authorized personnel have access to confidential information such as IEP's and student data, and using data encryption when transmitting confidential information to third parties such as the IRS, OMNI, and NYS Retirement Systems.

Computer Controls Procedures

The Administrator of Technology has been designated as the system administrator for *Finance Manager*, and network administrator. All access requests, changes to user permissions, additions of new employees and removal of terminated employees from the District's network and applications must be executed by the Administrator of Technology (this will be discussed further in the section titled, "Accounting Information System" and "Other Applications"). The District currently performs a full systems backup on a daily basis (this will be discussed further in the section titled, "Network and Network Security").

NETWORK AND NETWORK SECURITY

Firewalls and Intrusion Detection Systems

A firewall is used to implement access control between two networks. It allows the District's network users to access outside information while preventing those outside the District from accessing the District's systems. The District's firewall consists of a combination of appliances and software that provides several layers of protection against intrusions. Currently, the District has implemented the following security applications:

- ***Cisco ASA 5220*** – Network security device. Provides firewall and network address translation functions. Protects against Internet threats such as viruses and network attacks. Also functions as a virtual private network (VPN) endpoint appliance.
- ***Sophos WS1100*** – content-control appliance. Internet filter that blocks access to Web content deemed inappropriate by administration.
- ***ASSP Spam Filter*** – managed email security service. Protects email threats using a combination of spam filters, anti-virus scanning, fraud protection, content filtering, and email attack protection.
- ***Sophos Endpoint Protection*** – installed on servers and desktops, with antivirus signatures automatically updated.

Back-up Controls

The District is utilizing *Symantec Backup Exec* to perform a full backup each night. All of the District's servers are backed utilizing tapes on a daily basis. The backup tapes are stored in a locked room in the administration building. The *Finance Manager* server is also backed up by BOCES on a nightly basis.

Network and Email Access

The District has implemented *iMail Server* and is utilizing *Active Directory* for the authentication of email and network users. All access requests, changes to user permissions, additions of new employees and removal of terminated employees from *Active Directory* are executed by the Administrator of Technology or the Systems Engineer. The District is currently implementing *Microsoft Exchange Server* which will be integrated with *Active Directory*.

Once an individual has been hired, the human resources department emails the Administrator of Technology with the new employee's name, position, school building location and user account specifications. Based on this information, a network and email account is manually created and a temporary password is assigned to the user. Users are prompted to change the password upon initial login. The District requires the use of strong passwords which must be six characters in length and include a combination of letters and numbers.

Physical Security

The District's Network Operations Center ("NOC") is currently being relocated to the administration building from the Northport High School. Most servers have been transferred to the administration building however approximately six servers are still located within the Northport High School. Both server rooms are temperature controlled and uninterrupted power supply ("UPS") units are in place to protect the District's equipment from an unexpected power disruption that could cause business disruption and data loss.

VPN

A virtual private network ("VPN") is a network that allows the District's remote users to securely access the District's network using a public telecommunication infrastructure, such as the Internet. Currently, the Assistant Superintendent for Instruction and Administration, Administrator of Technology and a Systems Engineer has VPN access to the District's network. In addition, *Finance Manager* also has limited VPN access. When *Finance Manager* needs VPN access to perform server maintenance, they must contact the Administrator of Technology or Systems Engineer to establish a window of time for performing maintenance. *Finance Manager* will then be granted VPN access by the Administrator of Technology for the agreed upon period of time. When this time expires, *Finance Manager's* VPN access will terminate.

ACCOUNTING INFORMATION SYSTEM

Based on our interviews and observations, we noted the accounting information system currently utilized by the District to be as follows:

The District currently utilizes *Finance Manger* as its Accounting Information System ("AIS"). This application was installed by *Finance Manager* and requires *Finance Manger* to perform application updates, database management and, if necessary, system restores. The following modules of *Finance Manager* were identified as being utilized by the District (a description of the modules has been provided):

- ***Accounting Manager*** – Maintains general ledger, accounts payable, budgetary accounting, receipts/revenue, encumbrances/purchasing, project/grant accounting; generates financial documents such as computer-generated checks, purchase orders, account and vendor histories, and assists with controls to maintain data integrity and balanced entries.
- ***Budget Manager*** – Assists in the annual budget preparation.
- ***Human Resource Manager*** – Maintains all employee data, including detailed attendance histories, benefits tracking, educational and PDP credits, observations and evaluations, fingerprint tracking, retirement data and emergency medical information.
- ***Negotiation Manager*** – Creates salary matrices to maintain contract salaries and hourly rates for all personnel. Constructs salary schedules with multiple steps/levels for development of numerous contract scenarios for simple comparison.
- ***Payroll Manager*** – A payroll generation program that provides detailed employee records and custom generation of payroll.
- ***Receivables Manager*** – Provides all relevant financial documents: invoices, billing journals, aging reports, reminder notices, customer histories and revenue source journals.
- ***Requisition Manager*** – Enables individuals throughout the District to electronically submit purchase requisitions and allows for electronic approval of requisitions submitted.

Passwords

The District should have procedures in place to periodically verify its system of controls are working as intended, are still needed, and are cost effective, including a review of the controls over access to information systems. Access to computerized files and transactions should be restricted to authorized individuals. This can be accomplished with the use of passwords and software that restricts users' access and can help ensure that only authorized individuals utilize the computer system.

Finance Manager requires the use of strong passwords. The *Finance Manager* passwords must be six to ten characters in length and include a combination of letters and numbers. *Finance Manager* has also been configured to force users to change their passwords every ninety days. The District has also enabled a three (3) log-on attempt limit in *Finance Manager*.

Permissions

A good internal control framework requires District management to develop a system of controls that includes proper segregation of duties in the District's operations. A proper segregation of duties should exist not only in manual processes, but also within the AIS. *Finance Manager* allows the

system administrator, the Administrator of Technology, to restrict District employee access to functions pertaining to their job description.

User Maintenance

The District's procedures for user maintenance are as follows: For the addition of new users or changes to permissions of existing users, an appropriate administrator or cabinet administrator must email the assistant superintendent for business to request the access within *Finance Manger*. The email must include the type of permissions and appropriation codes, if applicable, being requested. The assistant superintendent for business evaluates the permissions being requested and evaluates the level of access the employee should have. Once approved, the assistant superintendent for business emails the Administrator of Technology to create or update a user account within *Finance Manager*. The email is also printed and signed by the assistant superintendent for business then forwarded to the Administrator of Technology. Once the user account has been updated within *Finance Manager*, the Administrator of Technology emails the assistant superintendent for business to notify her that the request has been processed then indicates the date of change on the printed email. The signed emails are maintained in a binder in the Administrator of Technology's office.

OTHER APPLICATIONS

Based on our interviews and observations, we noted the other applications currently utilized by the District to be as follows:

eSchoolData Systems

eSchoolData Systems ("*eSchoolData*") is the student data management application currently utilized by the District, which allows the District to track attendance, behavior, and grades by student. The system also provides a course catalog, graduation planning, grade book and assists the District in preparing required reports submitted to the New York State Education Department. The entire system is web-based, which allows teachers, instructional administrators, instructional clerical staff and parents to access student information. Further restrictions are applied to the individuals' user privileges to ensure that only authorized users are seeing specific information (i.e. teachers only have access to enter attendance and grades; all other functions are restricted).

Once notified by the office of human resources or an appropriate administrator, users are provided an account within *eSchoolData* by the Administrator of Technology. Passwords must be changed upon initial login and are required to be at least seven characters in length, containing a combination of letters and numbers.

IEP Direct

IEP Direct is the special education student management application currently utilized by the District. *IEP Direct* is a web-based application that is used in conjunction with *eSchoolData,* which allows the District to track student IEP's, evaluations, meetings, and assists with the preparation of New York State required reports. Additionally, *IEP Direct* enables the preparation of STAC forms, facilitating the recovery of Medicaid funds. The system has an optional Medicaid Direct add-on that automates the Medicaid tracking and billing process for maximizing revenue recovery, which improves data accuracy and accelerates collections. Further, *IEP Direct* facilitates District compliance with applicable privacy laws and regulations.

Application access is only granted to authorized individuals, and restrictions within the application prevent unauthorized individuals from viewing student information. Passwords for *IEP Direct* expire every six months and are required to be at least nine characters in length, containing at least one lower case letter, one upper case letter and one number. All changes to user permissions are performed by the system administrator, who is the senior clerk in the office of special education.

INFORMATION TECHNOLOGY AND DISASTER RECOVERY PLANS

Based on our interviews and observations, we noted the following with regards to the Information Technology and Disaster Recovery Plans:

Information Technology Plan

The purpose of the *District Technology Plan* is to define and outline the steps necessary to prepare students for challenges and opportunities in their educational endeavors by providing the best possible technology environment. The *District Technology Plan* discusses the District's plans for architecture, hardware, software, staff training, implementation, and evaluation. The current Technology Plan covers the three-year period from 2010 through 2013.

Disaster Recovery Plan

Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, communications (such as networking) and other information technology infrastructure. While the District would like to ensure zero data loss and zero time loss in the event of a disaster, the cost associated with that level of protection may make the desired high availability solutions impractical.

The District's adopted *Disaster Recovery Plan* is comprised of several sections that document the procedures and resources that are to be followed and used in the event that a disaster occurs at the District. The sections of the *Disaster Recovery Plan* are as follows:

- Introduction;
- Disaster Recovery Teams and Responsibilities;
- Communicating During a Disaster;
- Dealing With a Disaster; and
- Restoring IT Functionality.

INFORMATION TECHNOLOGY TRAINING

The District is committed to providing professional development to District staff for the enrichment of technology use and integration in the classroom. The District's Professional Development Plan facilitates the integration of technologies for improved instruction, student achievement and student services. District staff can schedule on-site classes, workshops and conferences using *Moodle*.

The District employs five information technology resource teachers. Three teachers are assigned to the middle school and high school and two teachers are assigned to the elementary schools. The information technology resource teachers assist various teachers within the District with implementing technology within the classroom. The information technology resource teachers conduct monthly professional development courses each month. There are also computer labs within each school location and a computer aid is assigned to each location to assist staff and students.

FINDINGS AND RECOMMENDATIONS

Based on our interviews, observations and detailed testing, we provide our findings and recommendations below to further strengthen the District's internal controls as they pertain to information technology outlined above.

It should be noted that these recommendations are provided to the District to assist management in improving the District's internal controls and procedures relating to information technology. It is important to note that our findings and recommendations are directed toward improvement of the system of internal controls and should not be considered a criticism of, or reflection on, any employee of the District.

Based on our interviews and observations, our findings and recommendations are as follows:

I. We noted that *Active Directory* passwords for authenticating network and email users are not required to be periodically changed. This leaves user accounts on all systems utilizing *Active Directory* for authentication vulnerable to unauthorized access.

We recommend that the District develop and adopt a password policy to strengthen computer security controls and reduce the risk of unauthorized access. A password policy should include criteria for password length, formation and duration as well as proper password management such as advising network users to never communicate their password by telephone, e-mail or instant messaging.

***

II. We noted that the District is not currently utilizing the account lockout feature of *Windows* password security to prevent attackers from brute-force attempts to guess a user's password.

We recommend that the District consider implementing the *Windows* password security account lockout feature to help deter malicious users and certain types of automated attacks from discovering user passwords. A medium security lockout policy would include an account lockout duration of thirty minutes, an account lockout threshold of three to seven invalid logon attempts, and an automatic account lockout reset of thirty minutes.

***

III. We noted that the District has not enabled the feature within *Windows* that causes a user's workstation to automatically lock out after a specified period of inactivity. If a user does not manually lock their computer before walking away, individuals passing by can have access to files, emails or other data that they are not authorized to see.

We recommend that the District implement a security lockout policy and configure the computers to have a password-enabled screen saver initiate after the computer remains idle for a specified amount of time. By requiring a user to enter their password when they return, it minimizes the risk of an unauthorized individual using an active session while the authorized user is away.

***

IV. We noted that the backup tapes are maintained in the NOC located in the administration building.

While we noted that the District has redundant backup strategies, we recommend that the District evaluate the available options for the off-site storage of backup tapes to determine the optimal storage location for ensuring the safety of data.

***

V. We noted that although the assistant superintendent for business periodically reviews audit trail reports within *Finance Manager* for user activity to identify any activity that appears to be unusual, the review is not documented. Audit trails maintain a record of system activity that can assist system administrators in identifying potential security violations. Further, audit trails are a mechanism that maintains individual accountability for user actions by advising users that their actions are recorded in an audit log. Additionally, we noted that the District does not review the login/logout report within *Finance Manager* to identify users who may be logging into the financial software at unusual times.

We recommend that the District implement procedures whereby the review of audit trails be documented and maintained on file. Additionally we recommend that the District periodically review and document the review of the login/logout report within *Finance Manager* to ensure users are not accessing the financial software at unusual times.

***

VI. We noted that the District does not require the passwords to *eSchoolData* to be changed periodically, which over time increases the risk that an individual's account can be compromised by an unauthorized user.

We recommend that the District require users of *eSchoolData* to periodically change their password to prevent unauthorized access and to reduce the vulnerability of an account to being compromised.

***

VII. While we noted that the District performs daily backups, a system restore has not been performed for all applications and backup information is not periodically tested to verify that the information is restorable.

We recommend that the District perform a restore for all applications to verify that information is complete and restorable. If this is not cost effective, the District should implement procedures to periodically test backups to verify that information is restorable in case of a network or application failure.

***

VIII. We noted that the District has not restricted the ability to download or install software on District owned computers including ipads.

We recommend that the District restrict the rights to download or install software to as few individuals as practical. Software additions or changes should be made by the information technology department to ensure that the software works well with the network, is safe to use, and is for business use.

***

For the detailed testing performed, our procedures, findings and recommendations are as follows:

Required Policies

Procedure Performed: We reviewed the District policies to determine whether the District has adopted the legally required policies pertaining to information technology.

Finding: Although the District has adopted policy No. 8635, *Information Security Breach and Notification*, the District has not established the appropriate regulations regarding the procedures that are to be followed in the event of a security breach.

Recommendation: We recommend that the District develop and adopt a formal *Information Security Breach and Notification* regulation to include, but not necessarily be limited to, identifying individual(s) responsible for checking for breaches, how often inspection is required to be performed, individuals required to be notified in the event of a breach and procedures currently in place. By having the Board formally adopt this regulation, the District will be in compliance with State Technology Law §208.

***

Recommended Policies

Procedure Performed: We reviewed the District policies to determine whether the District has adopted other written policies and procedures surrounding information technology.

Findings: We noted that the District has not developed and adopted a computer controls policy as recommended by the State Comptroller's Office.

Recommendation: We recommend that the District develop and adopt a computer controls policy as recommend by the State Comptroller's Office, which should include, segregation of duties; report generation and approval; passwords and permissions; data input; remote access and data backups. The computer controls policy should also include the internal procedures currently in place. Further, the District should continue to review and update (if applicable) on an annual basis its current procedures to ensure that the District's electronic information integrity has not been compromised and to ensure that the District is in compliance with privacy laws and regulations.

***

Server Rooms

Procedure Performed: We physically inspected the District's server rooms in the administration building and high school to verify the server room is properly secured and that the servers are reasonably protected from fire and floods.

Finding: We noted that the District has not implemented procedures for monitoring server room access to ensure that the network and its components have been protected at the physical level.

Recommendation: We recommend that the District perform a cost benefit analysis of installing a video surveillance camera. The camera should be placed in a location that makes it difficult to tamper with or disable but provides a view of individuals entering and leaving, and should be used to supplement an access log book or electronic access system. Surveillance cameras can monitor continuously, or use motion detection technology to record only when someone is moving about. Surveillance systems can also be configured to send e-mail or cell phone notification if motion is detected during non-business hours.

**

Finding: We noted that the NOC does not have a fire suppression system such as a fire extinguisher. As per the National Fire Protection Association *Standard for the Protection of Information Technology Equipment* (NFPA 75) the server room at a minimum must have a fire detection and alarm, portable fire extinguishers and Emergency Power Off.

Recommendation: We recommend that the District place a fire extinguisher in the NOC, at a minimum, to be compliant with the National Fire Protection Association *Standard for the Protection of Information Technology Equipment* (NFPA 75).

***

Finance Manager Permissions

Procedure Performed: We reviewed the user permissions within *Finance Manager* to identify multiple active user accounts, generic user accounts, and possible permissions granted to various employees that may not be consistent with their job responsibilities.

Finding: We noted that the District has not restricted the ability to delete or modify journal entries within *Finance Manager*. Deleting transactions will cause a break in the transaction sequence, and a partial deletion of the physical audit trail.

Recommendation: We recommend that the District disable the ability to delete or modify journal entries within *Finance Manager* for all users. If a transaction deletion occurs, the District should document the reasons in order to maintain a full audit trail.

**

Finding: We noted that the District is not periodically reviewing and documenting the review of user permissions. Reviews of user permissions within *Finance Manager* will assist the District in identifying potential incompatible duties, help verify that users are assigned to permissions that are within their job responsibility and ensure that only those new user permissions or changes to existing permissions that were approved were made.

Recommendation: We recommend that the District implement procedures whereby user permissions are reviewed periodically and the review be documented, perhaps on a test basis quarterly due to the volume of the reports that would need to be generated and reviewed. This additional control, which is considered a best practice, will serve to strengthen the control environment even further within the District's accounting information system.

**

Findings: We noted thirty individuals who have two active user accounts and two individuals with three active user accounts within *Finance Manager*. Additionally, the District has five active user accounts that appear to be generic templates such as supervisor user, purchasing clerical, system administrator and tech.

Recommendation: We recommend that the District ensure that each individual who has access to *Finance Manager* be given one active user account. Additionally, we recommend that the District review and update its current user accounts within *Finance Manager* to ensure that only those authorized individuals have active user accounts to prevent unauthorized access to the District's financial information.

**

Finding: We noted two retired employees had an active user account in *Finance Manager*.

Recommendation: We recommend that the District disable the user accounts within *Finance Manager*. In addition, the District should implement procedures to ensure that only active employees in the business operations of the District have active user accounts in *Finance Manager*.

**

Finding: We noted that the assistant superintendent for business has the ability to override purchase orders, cash disbursements and the general ledger in an amount up to $250,000 and the accounting supervisor has the ability to override purchase orders, cash disbursements and the general ledger in an amount up to $50,000.

Recommendation: We recommend that the District establish a more reasonable limit for overriding purchase orders, cash disbursements and the general ledger to improve controls surrounding the District's budgetary management and reduce the risk that budget lines will be over expended.

**

Findings: We noted the following example of segregation of duties violations within *Finance Manager* where District employees have been granted incompatible duties by having access to functions not pertaining to their job description:

- The assistant superintendent for business has full access to the *Payroll Manager* module;
- The assistant superintendent for business and two clerks within the accounting department have permissions to perform budget transfers and journal entries;
- The assistant superintendent for business and part-time clerk within the accounting department has permissions to perform cash receipts;
- Three clerks within the payroll department have permissions to add, update and delete employee information for appointments and earnings in the *Payroll Manager* module; and
- A clerk within the accounting department has the permission to post budgetary entries.

Recommendation: We recommend that the District review its current permissions in *Finance Manager* and create a system of controls that ensures the proper segregation of duties and restrict access where necessary.

***

Vendor/Employee Match

Procedure Performed: We performed a comparison of the master vendor file to the master employee file to identify possible conflicts of interest.

Finding: Although no conflicts of interest were identified, we noted that the District has not implemented procedures to identify potential conflicts of interest and to ensure proper classification of vendor versus employee.

Recommendation: We recommend that the District develop and implement procedures to identify potential conflicts of interest, which should include but not necessarily be limited to, a periodic comparison of the master vendor file to the master employee file, identifying and addressing conflicts of interest, and reviewing IRS guidelines regarding employee versus independent contractor classification. The comparison of the master vendor file and employee master file should include a search for address and name matches. In addition, the procedures should identify the individuals responsible for performing the comparison, and establishing procedures to address conflicts of interest.

***

Vendor Master File

Procedure Performed: We reviewed the master vendor file to verify that the master vendor file is complete, accurate, up to date and free of duplicate vendors.

Finding: Although we noted that the District does have procedures in place to validate the master vendor file, we identified thirty five (35) instances of duplicate vendors, which are vendors entered into the vendor master file more than once. Additionally, we noted ten (10) instances in which individuals are set up as active vendors however the company that they work for is also an active vendor. The search for identifying duplicate vendors included finding vendors that have the same address and similar names, but different vendor identification numbers. Typically each instance of the duplicate vendor had a slight variation in the spelling of the vendor name.

Recommendation: We recommend the District review the vendor master file and remove all duplicate vendors. Additionally, we recommend the District review the vendor master file to ensure that only the appropriate vendors that the District conducts business with remain active and inactivate those vendors whose services and/or goods are no longer required by the District.

***

Disaster Recovery Plan

Procedure Performed: We reviewed the District's Disaster Recovery Plan (the "Plan") to determine that Plan identifies critical information technology infrastructure and equipment, establishes the most suitable recovery strategy for each application utilized by the District, and identifies those individuals responsible for overseeing the disaster recovery process.

Finding: No exceptions were noted as a result of applying these procedures.

CORRECTIVE ACTION PLAN

The District is required to prepare a corrective action plan in response to any findings contained in the internal audit reports. As per Commissioner's Regulation §170.12, a corrective action plan, which has been approved by the Board, must be submitted to the State Education Department within 90 days of the receipt of a final internal audit report.

The approved corrective action plan and a copy of the respective internal audit report should be sent to the following address:

New York State Education Department
Office of Audit Services, Room 524 EB
89 Washington Avenue
Albany, New York 12234
Attention: John Cushin