OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Brookhaven Fire District

Procurement and Information Technology

Report of Examination

Period Covered:

January 1, 2013 – May 31, 2014

2014M-339

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

February 2015

Dear District Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as 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 operations and Board of Fire Commissioner governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Brookhaven Fire District, entitled Procurement and Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law.

This audit's results and recommendations are resources for local government 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 Brookhaven Fire District (District), located in the Town of Brookhaven in Suffolk County, is a district corporation of the State, distinct and separate from the Town. The District covers 21 square miles and serves approximately 5,600 residents. The District is governed by an elected five-member Board of Fire Commissioners (Board). The Board is responsible for the District's overall financial management, including establishing appropriate internal controls and safeguarding cash. Additionally, the Board is responsible for approving an annual budget. The District's actual expenditures for 2013 were $2,557,060 and budgeted appropriations for 2014 were $2,547,374, which were funded primarily with real property taxes.

Scope and Objectives

The objectives of our audit were to examine the District's purchasing procedures and to determine whether the District's computer system was adequately safeguarded for the period January 1, 2013 through May 31, 2014. Our audit addressed the following related questions:

- Did the Board ensure that District personnel used competitive methods when procuring goods and services that were not subject to competitive bidding?

- Did the Board ensure that the District's financial software, data and computer hardware were adequately safeguarded?

Audit Results

The Board did not ensure that District personnel used competitive methods when purchasing goods and services not subject to competitive bidding. This occurred because the Board did not require that District personnel obtain quotes or issue requests for proposals in accordance with the Board-adopted procurement policy. District officials paid 27 invoices totaling $83,370 for purchases without obtaining any type of competition. In addition, in both the 2013 and 2014 fiscal years, the Board did not follow its own procurement policy because it approved 22 vendors for use without first obtaining competition. The District also did not seek competition when selecting four professional service providers who received payments totaling $155,865. We also found that the District did not enter into a written agreement with two professional service providers who were paid a total of $35,113 during our audit period. Unless the Board ensures consistent compliance with the District's procurement policy, the District will continue to be at risk of overpaying for goods and services.

The Board did not ensure that the District's financial software, data and computer hardware were adequately safeguarded. The Board has not established written policies or procedures for granting,

changing and terminating access rights to the District's financial system. It has not ensured that each financial system user is assigned only one username and password and has not designated someone independent of Business Office operations to be the financial software system administrator. In addition, the District granted its outside financial consultant remote access to its financial system at any time, without restriction, prior approval, authorization and monitoring. As a result, there is an increased risk that financial data could be manipulated, and errors and irregularities could occur without detection.

Finally, the Board has not adopted a breach notification policy or a disaster recovery plan. As a result, in the event that personal, private and sensitive information is compromised, affected individuals may not be notified. In the event of a disaster, District personnel have no guidelines or plan to help minimize or prevent the loss of equipment and data or to implement data recovery procedures. As a result, the District's information technology assets are at an increased risk of loss or damage and there could be disruptions to the District's critical operations.

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 disagreed with certain findings contained in our report. Appendix B includes our comments on issues District officials raised in their response.

Introduction

Background

The Brookhaven Fire District (District), located in the Town of Brookhaven in Suffolk County, is a district corporation of the State, distinct and separate from the Town. The District covers 21 square miles and serves approximately 5,600 residents. The District's 95 active volunteer members responded to 699 alarms in 2013. The District had 99 active volunteer members in 2014.

The District is governed by an elected five-member Board of Fire Commissioners (Board). The Board is responsible for the District's overall financial management, including establishing appropriate internal controls and safeguarding cash. Additionally, the Board is responsible for approving an annual budget to ensure that the District's resources are being used efficiently. The District Treasurer (Treasurer) is the District's chief fiscal officer and is responsible for receiving, maintaining custody of and disbursing District funds, maintaining financial records and preparing monthly and annual reports. The District's actual expenditures for 2013 were $2,557,060 and budgeted appropriations for 2014 were $2,547,374, which were funded primarily with real property taxes.

Objectives

The objectives of our audit were to examine the District's purchasing procedures and to determine whether the District's computer system was adequately safeguarded. Our audit addressed the following related questions:

- Did the Board ensure that District personnel used competitive methods when procuring goods and services that were not subject to competitive bidding?
- Did the Board ensure that the District's financial software, data and computer hardware were adequately safeguarded?

Scope and Methodology

We examined the District's procurement practices and information technology controls for the period January 1, 2013 through May 31, 2014.

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 is included in Appendix C 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 disagreed with certain findings contained in our report. Appendix

B includes our comments on issues District officials raised in their response.

The Board has the responsibility to initiate corrective action. Pursuant to Section 181-b of the New York State Town Law, 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 Secretary's office.

Procurement

General Municipal Law (GML) states that goods and services that are not required by law to be bid must be procured in a manner to ensure the prudent and economical use of public moneys in the best interests of the taxpayers. GML requires the Board to adopt written policies and procedures for the procurement of goods and services that are not subject to competitive bidding, such as items that fall under the bidding threshold and professional services. These policies and procedures should indicate when District officials must obtain competition, outline the procedures for determining the competitive method that will be used and provide for adequate documentation of the actions taken. The use of competition provides taxpayers with the greatest assurance that goods and services are procured in the most prudent and economical manner, goods and services of desired quality are being acquired on the most favorable terms and conditions and procurement is not influenced by favoritism, extravagance, fraud or corruption. The Board adopted a procurement policy that requires District personnel to obtain quotes and proposals for purchases not subject to competitive bidding requirements.

The Board did not ensure that District personnel used competitive methods when purchasing goods and services not subject to competitive bidding. This occurred because the Board did not require that District personnel obtain quotes or issue requests for proposals in accordance with the Board-adopted procurement policy. District officials paid 27 invoices totaling $83,370 for purchases without obtaining any type of competition. In addition, the Board did not follow its own procurement policy because it approved 22 vendors for use without obtaining competition. The District also did not seek competition when selecting four professional service providers who received payments totaling $155,865. Because the District did not seek competition when procuring goods and services, there is an increased risk that it could be paying more than necessary. Finally, the Board did not enter into written agreements with two professional service providers[1] who received payments totaling $35,113 during the audit period. Without agreements outlining the agreed-upon services and related prices, the District is at risk of not obtaining the services it paid for or paying more for services than necessary.

Quotes – The Board-adopted procurement policy requires that District personnel obtain one to three verbal quotes for purchase contracts

[1] These vendors provided insurance and construction management services to the District.

between $500 and $999, two written quotes for purchase contracts between $1,000 and $4,999 and three written quotes for purchase contracts between $5,000 and $19,999. For public work contracts, the policy requires two written quotes from vendors for contracts between $1,000 and $4,999 and three written quotes for contracts between $5,000 and $34,999.

District officials and staff did not follow the guidelines in the District's procurement policy for purchases and public work contracts that required at least two written quotes. We reviewed 28 invoices[2] for which the District was required to solicit at least two written quotes; however, 27 invoices totaling $83,370 were for purchases obtained without any type of competition. For example, the District purchased a gym membership totaling $7,200 and parts for a vehicle costing $5,010 without obtaining any of the three required quotes from vendors.

In addition, the Board did not follow its own procurement policy because it approved 22 vendors for use without using a competitive process. At the 2013 and 2014 organizational meetings, the Board approved 22 contract vendors to be used by District personnel. The Board did not obtain these vendors through a competitive process before approving them for use. By doing so, the Board ignored its own policy and, in effect, District staff did the same. For example, the District paid $13,357 to a vendor for electrical work. This vendor was on the Board's list of approved contract vendors and District staff did not obtain any quotes when procuring these services, as required by the policy. The failure of the Board and District personnel to comply with the District's purchasing policy increases the risk that goods and services may not be obtained in the most prudent and economical manner and could result in the unnecessary expenditure of taxpayers' money.

Professional Services – While the District is not legally required to competitively bid for the procurement of professional services, GML does require that fire districts adopt policies and procedures governing the purchase of goods and services when competitive bidding is not required. In addition, prudent business practices provide that contracts for professional services be awarded after soliciting competition to ensure the District obtains the needed services on the most favorable terms or for the best value. One way to accomplish this is to request proposals. A request for proposals (RFP) is a highly structured document that specifies minimally acceptable functional, technical and contractual requirements and the evaluation criteria that

[2] These 28 invoices were part of 22 claims reviewed. See Appendix C for Methodology.

will govern the contract award. A written agreement is also essential for establishing the services to be provided, the time frames for those services and the basis for compensation.

The District's procurement policy requires that all contracts for professional services be awarded only after at least two professionals are contacted and asked to submit written proposals. However, we found that District officials and staff did not follow these guidelines when obtaining professional service providers.

We reviewed claims[3] from seven professional service providers who the District paid a total of $227,272 during our audit period. The District did not issue RFPs when selecting four of these providers who received payments totaling $155,865. We also found that the District did not enter into written agreements with two[4] of the seven vendors, who received payments totaling $35,113 during the audit period. Because the District did not have a written agreement with these vendors, it has a greater risk of paying for services that it does not receive or of overpaying for services that do not comply with contractual conditions and rates.

Although the Board-adopted policy required quotes and proposals from vendors, the Board did not make sure that District officials and staff complied with the policy. Unless the Board ensures consistent compliance with the District's procurement policy, the District will continue to be at risk of overpaying for goods and services.

Recommendations

The Board should:

1. Ensure that District personnel comply with the District's procurement policy by obtaining required verbal or written quotes for purchases and public work contracts that are not required by GML to be publicly bid.

2. Ensure that District personnel comply with the District's procurement policy when procuring professional services.

3. Approve purchases from vendors only after District personnel follow the procurement policy by using competitive methods to obtain the vendors.

4. Enter into written agreements with all professional service providers.

[3] See Appendix C for methodology

[4] These vendors provided insurance and construction management services to the District.

Information Technology

District officials are responsible for designing internal controls over information technology (IT) resources that include policies and procedures designed to protect software, data and computer hardware from loss or misuse due to errors, malicious intent or accidents (disasters). District officials should develop written procedures for adding, deleting and changing user access rights within the District's financial software; ensure that users have only those rights needed to complete their job duties and establish procedures to monitor and control remote access to the District's network and financial system by outside vendors and consultants. It is important that the Board and District officials regularly review the policies and procedures and update them to reflect changes in the IT environment.

The Board has not established written policies or procedures for granting, changing and terminating access rights to the District's financial system. It has not ensured that each financial system user is assigned only one username and password and has not designated someone to be the financial software system administrator. In addition, the Board has not implemented policies or established procedures that address remote access to the financial system. Furthermore, the Board did not adopt a breach notification policy or a disaster recovery plan. As a result, the District's IT assets are at an increased risk of loss or damage and there could be disruptions to its critical operations.

User Access

District officials should limit access to the District's computerized system to ensure that outsiders (e.g., attackers) cannot gain unauthorized access to the computer systems or data, that access to sensitive resources, such as operating systems and security software programs, is limited to only the individuals who have a valid business need for such access and that employees and contractors are restricted from performing incompatible functions or functions beyond their responsibilities. There should be written procedures in place that establish authority for granting, changing and terminating access rights to the overall networked computer system and to specific software applications. Generally, a system administrator is designated as the person who has oversight and control of the system and has the ability to add new users and change users' passwords and access rights. To help ensure individual accountability within software applications, each user should have his or her own user account (username and password). If users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

The Board did not establish written policies or procedures to add, delete or modify an individual's access rights to the District's financial software. The financial software application had four active user accounts during our review. One of these was a user account with administrative rights. The remaining user accounts were for the District's outside financial consultant, the Treasurer and the District Secretary. Both the financial consultant and Treasurer also have access under the user account with administrative rights, thereby allowing them to control and use all aspects of the financial software application. This creates the opportunity for the manipulation and concealment of transactions and the inability to trace transactions to a single user.

In addition to sharing administrative rights, the financial consultant and the Treasurer each have their own user account with limited access rights in the financial system. For example, the financial consultant is responsible for overseeing the Treasurer's and Secretary's duties and entries within the financial system. The access granted under his user account restricts him from seeing sensitive data. However, since the consultant also has access under the user account with administrative rights, he has the ability to see sensitive data and is granted unlimited access rights. The Treasurer, under her user account, is restricted from access to certain areas within the financial system such as inventory. However, she has access to everything if she logs in with the user account with administrative rights.

We reviewed an audit log generated by the District's financial software and did not find any inappropriate activity. However, if the District does not limit user access, changes to the financial data can be made that District officials will be unable to trace to a single individual. This increases the risk of unauthorized or inappropriate transactions.

Remote Access

Remote access is the ability to access the District's computer system from the Internet or other external source. Remote access must be controlled, monitored and tracked so that only authorized individuals are allowed to access the District's network and financial systems. District officials should establish procedures that address how remote access is granted, who is given remote access and how it will be monitored and controlled.

The Board has not established policies or implemented procedures that address remote access to the District's computer system to ensure that computerized data is properly safeguarded. The District allows remote access to its computer system to an outside financial consultant. This consultant can access the District's financial system remotely at any time without restriction. In addition, staff employed by the consultant use the consultant's username and password to enter

the system and can log in remotely at any time without the District's prior knowledge, authorization and monitoring.

While we did not find that the consultant gained remote access to the District's system during unusual times, the lack of policies and procedures for remote access increases the risk that the District's financial data could be lost, damaged or misused, which could result in serious interruption to the District's operations.

Breach Notification Policy

New York State Technology Law requires cities, counties, towns, villages and "other local agencies" to develop an information breach notification policy. It is not clear whether the New York State Legislature intended fire districts to be included within the scope of the term "other local agencies." Nonetheless, even in the absence of a clear statutory requirement, we believe it is good practice for fire districts to adopt such a policy. This policy should detail how District officials would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure should be made in the most expedient time possible and consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The Board has not adopted a breach notification policy. As a result, District officials and staff may not understand or be prepared to fulfill their obligation to notify affected individuals in the event that personal, private and sensitive information is compromised.

Disaster Recovery Plan

Disaster recovery is the process by which an entity can resume business after a disruptive event. The event might be something large, such as a major flood, or something small, such as malfunctioning software caused by a computer virus. A disaster recovery plan should be developed to address how employees will communicate, where they will go and how they will continue to do their jobs in the event of a disaster. Plan details can vary greatly depending on the size and scope of the entity and its computerized operations. The plan should address the range of threats to the IT systems and be distributed to all responsible parties. District officials should ensure that it is periodically tested and updated as needed. The plan should focus on sustaining critical business functions during and after a disruption. Typically, disaster recovery planning involves an analysis of business processes and continuity needs and may include a focus on disaster prevention.

The Board did not adopt a disaster recovery plan. In the event of a disaster, District personnel have no guidelines or plan to help minimize or prevent the loss of equipment and data or to implement

data recovery procedures. As a result, the District's IT equipment and data are at an increased risk of loss or damage and there could be disruptions to the District's critical operations.

Recommendations

The Board should:

5. Develop policies and written procedures for granting, changing and terminating user access rights to the financial system.

6. Ensure that each financial system user is assigned only one username and password so that users cannot log in under multiple user names or share user accounts and passwords.

7. Designate someone independent of Business Office operations to be the financial software system administrator.

8. Ensure that excessive user accounts are disabled or deleted.

9. Develop policies and procedures to address how remote access should be granted, who should be given remote access and how District officials should monitor and control remote access.

10. Adopt a breach notification policy.

11. Adopt a comprehensive disaster recovery plan that details specific guidelines for the protection of private and essential data against damage, loss or destruction and the recovery of District systems and data in the event of loss.

District officials should:

12. Monitor remote access provided to the District's financial consultant.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

BROOKHAVEN FIRE DISTRICT

2486 MONTAUK HIGHWAY
BROOKHAVEN, NEW YORK 11719
631-286-0051 • FAX: 631-286-0983

January 30, 2015

Mr. Ira McCracken
Chief Examiner
Division of Local Government
And School Accountability
Office of the State Comptroller
NYS Office Building
Room 3A10, Veterans Memorial Highway
Hauppauge, NY 11788-5533

Re: Report of Examination, Brookhaven Fire District; Procurement and Information Technology; 1/1/2013-5/31/2014, 2014M-339;
Fire District Response and Corrective Action Plan

Dear Mr. McCracken:

This communication is sent as the response of the Board of Fire Commissioners to the draft audit report submitted by your office. We have also detailed the Corrective Action Plan ("CAP") which we will undertake at our fire district to address the recommendations made by your office. We would like to take this opportunity to thank your office for the professional work done by your auditors in reviewing various aspects of our financial system. Their recommendation made during the audit process and in the report will assist us to improve our financial operation.

The following are our responses to each recommendations stated in your report as well as the corrective action that will be undertaken as to each.

Recommendations:

1. Ensure that District personnel comply with the District's procurement policy by obtaining required verbal and/or written quotes for purchases and public work contracts that are not required by GML to be publicly bid.

The Board shall make certain that its audits of claim vouchers in preparation for each meeting include a review of compliance with procurement policy requirements for the obtaining of verbal and/or written quotes for each claim voucher approved.

2. Ensure that District personnel comply with the District's procurement policy when procuring the professional services.

The Board notes that it provided additional detail to audit staff on the multiple quotes obtained for the construction manager contract for its construction project. The Board will review the procurement policy and consider amendments to address the procedures to be utilized to select vendors providing professional services. The claim voucher audit process will then include verification that the special professional service procurement process has been followed for each such claim.

See Note 1 Page 19

3. Approve purchases from vendors only after District personnel follow the procurement policy by using competitive methods to obtain the vendors.

In addition to the correct action spelled out under recommendation numbered "1" above the Board will see that staff is retrained on the procurement process and specific rules that pertain to competitive bidding and the request for proposals process for purchases not covered by competitive bidding. The Board will amend the process of noting approved vendors at the annual organization meeting to make it clear that the list of vendors is a list of vendors approved due to background, experience and past work for the district, but that the quote process still must be undertaken with each purchase. The list of vendors will be approved for emergency purchase assignments in the event that emergencies arise and emergency purchase resolutions are adopted to pre-approve or ratify an emergency purchase.

4. Enter into written agreements with all professional service providers.

The Board notes that it supplied written agreements to audit staff for the architect and construction manager in relation to the construction project in question. Moving forward the Board will make certain that all professional service providers provide written agreements and that payments made to them are based on approved written agreement terms as part of the claim voucher audit process.

See Note 2 Page 19

5. Develop policies and procedures for granting, changing and terminating user access rights to the financial system.

The Board has concerns that with all the computer system security breaches and illegal activities performed by computer hackers on government and private business computer systems that it is irresponsible to publish a report to the public which highlights fire district computer system

See Note 3 Page 19

security shortcomings. While we can accept criticism and work to improve operational efficiency and security of our systems; we cannot agree with a decision that the Office of the State Comptroller may make to publicize these issues. The computer system security vulnerabilities of emergency service providers should not be publicized. We believe that recommendations numbered "5", "6", "8", "9", "11" and "12" should be placed in a separate letter from the Office of the State Comptroller to the Board of Fire Commissioners and not in the public report of external audit.

The Board will work with its IT consultant to develop policies and procedures for granting, changing and terminating user access rights to the financial system.

6. Ensure that each financial system user is assigned only one username and password so that users cannot log in under multiple usernames and/or share user accounts and passwords.

The Board has concerns that with all the computer system security breaches and illegal activities performed by computer hackers on government and private business computer systems that it is irresponsible to publish a report to the public which highlights fire district computer system security shortcomings. While we can accept criticism and work to improve operational efficiency and security of our systems; we cannot agree with a decision that the Office of the State Comptroller may make to publicize these issues. The computer system security vulnerabilities of emergency service providers should not be publicized. We believe that recommendations numbered "5", "6", "8", "9", "11" and "12" should be placed in a separate letter from the Office of the State Comptroller to the Board of Fire Commissioners and not in the public report of external audit.

See Note 3 Page 19

The Board will work with its IT consultant to see that each financial system user is assigned only one username and password so that users cannot log in under multiple usernames and/or share user accounts and passwords.

7. Designate someone independent of Business Office operations to be the financial software system administrator.

The Board will assign the role of financial software system administrator to a Fire Commissioner or another employee not involved in Business Office operations.

8. Ensure that excessive user accounts are disabled and/or deleted.

The Board has concerns that with all the computer system security breaches and illegal activities performed by computer hackers on government and private business computer systems that it is irresponsible to publish a report to the public which highlights fire district computer system

See Note 3 Page 19

security shortcomings. While we can accept criticism and work to improve operational efficiency and security of our systems; we cannot agree with a decision that the Office of the State Comptroller may make to publicize these issues. The computer system security vulnerabilities of emergency service providers should not be publicized. We believe that recommendations numbered "5", "6", "8", "9", "11" and "12" should be placed in a separate letter from the Office of the State Comptroller to the Board of Fire Commissioners and not in the public report of external audit.

The Board will take steps to make certain that excessive user accounts are disabled and/or deleted and will work with its IT consultant to see how this vulnerability can be eliminated in the future.

9. Develop policies and procedures to address how remote access should be granted, who should be given remote access, and how District officials should monitor and control remote access.

The Board has concerns that with all the computer system security breaches and illegal activities performed by computer hackers on government and private business computer systems that it is irresponsible to publish a report to the public which highlights fire district computer system security shortcomings. While we can accept criticism and work to improve operational efficiency and security of our systems; we cannot agree with a decision that the Office of the State Comptroller may make to publicize these issues. The computer system security vulnerabilities of emergency service providers should not be publicized. We believe that recommendations numbered "5", "6", "8", "9", "11" and "12" should be placed in a separate letter from the Office of the State Comptroller to the Board of Fire Commissioners and not in the public report of external audit.

See Note 3 Page 19

The Board will work with its IT consultant to develop policies and procedures to address how remote access should be granted, who should be given remote access, and how District officials should monitor and control remote access.

10. Adopt a breach notification policy.

Although not required by law to have one, the Board will adopt a breach notification policy.

11. Adopt a comprehensive disaster recovery plan that details specific guidelines for the protection of private and essential data against damage, loss or destruction and the recovery of District systems and data in the event of loss.

The Board has concerns that with all the computer system security breaches and illegal activities performed by computer hackers on government and private business computer systems that it is irresponsible to publish a report to the public which highlights fire district computer system

See Note 3 Page 19

security shortcomings. While we can accept criticism and work to improve operational efficiency and security of our systems; we cannot agree with a decision that the Office of the State Comptroller may make to publicize these issues. The computer system security vulnerabilities of emergency service providers should not be publicized. We believe that recommendations numbered "5", "6", "8", "9", "11" and "12" should be placed in a separate letter from the Office of the State Comptroller to the Board of Fire Commissioners and not in the public report of external audit.

The Board will work with its IT consultant to adopt a comprehensive disaster recovery plan that details specific guidelines for the protection of private and essential data against damage, loss or destruction and the recovery of District systems and data in the event of loss.

12. Monitor remote access provided to the District's financial consult.

The Board has concerns that with all the computer system security breaches and illegal activities performed by computer hackers on government and private business computer systems that it is irresponsible to publish a report to the public which highlights fire district computer system security shortcomings. While we can accept criticism and work to improve operational efficiency and security of our systems; we cannot agree with a decision that the Office of the State Comptroller may make to publicize these issues. The computer system security vulnerabilities of emergency service providers should not be publicized. We believe that recommendations numbered "5", "6", "8", "9", "11" and "12" should be placed in a separate letter from the Office of the State Comptroller to the Board of Fire Commissioners and not in the public report of external audit.

See Note 3 Page 19

The Board will assign a Fire Commissioner to periodically review the computer audit trail of the computer activity of the District's financial consult as a check and balance with regard to his access and permitted activities with regard to the financial software.

In summary, this communication shall serve as our response and CAP as required by statute. We will not issue a separate CAP after the report is published and instead will ask your office to accept this letter as the CAP. We will begin working on the corrective actions listed.

Very truly yours,

MICHAEL VERNI
Chairman

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

We made revisions to the report based on additional documentation provided at the exit conference.

Note 2

At the exit conference, District officials provided us with the written agreement for the architect used in the construction project, and we revised the final audit report accordingly. District officials did not provide a written agreement for the construction manager.

Note 3

Our audit reports do not include information that describes weaknesses or vulnerabilities that might lead an individual outside the local government to exploit such weaknesses. Our report does not specify any particular vulnerabilities that could be leveraged by an outside attacker and does not state the specific technologies used for remote access. The findings address the lack of policies, procedures and monitoring as applied to remote access and the lack of a disaster recovery plan. Reporting that the District does not have a disaster recovery plan in place does not increase the chance of unauthorized access to the District's data. It only reveals that the District is risking the availability and integrity of its data and the ability to recover its data in the event of a disaster. However, based on the District's response, we reviewed the report and made additional changes to exclude additional information. We are confident that the weaknesses identified in the final audit report do not expose the District to additional risk.

APPENDIX C

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 condition and oversight, control environment, cash receipts and disbursements, purchasing, payroll and personal services, capital assets and inventories, the length of service awards program and IT.

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 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 or professional misconduct. We then decided on the reported objectives and scope by selecting for audit those areas most at risk. We selected procurement of goods and services not subject to competitive bidding and IT for further audit testing.

To accomplish the objectives of this audit and obtain valid audit evidence, our procedures included the following:

- We performed an initial assessment of internal controls in place for purchasing procedures to determine overall effectiveness. This included interviewing appropriate District officials to gain an understanding of the procedures used.

- We reviewed minutes of the Board's meetings and District policies.

- We sorted the cash disbursement data provided by the District to include payments only to the 22 vendors listed in the organizational meeting minutes as approved "contract vendors" and deleted all payments to these vendors for less than $500 and above bidding thresholds. This brought our number of vendors down to 18 vendors. We used a random number generator to choose one payment from each of the 18 vendors. We eliminated one claim because it included invoices that were each below the $500 threshold. We therefore tested 17 claims. Of the 17 claims, six required one to three verbal quotes according to the Board-adopted policy and 11 required at least two written quotes.

- Starting with the original unsorted cash disbursement data, we deleted transactions to vendors that would not require quotes according to the District's policy, such as utilities and postage, eliminated all disbursements less than $500 and greater than $35,000 and removed all claims paid to the 22 vendors listed in the organizational meeting minutes as approved contract vendors. We wanted a sample selection of 50 claims (about 10 percent of the total population

of claims greater than $500 and less than $35,000 – 482 claims), including the 18 claims from the approved vendors. Therefore, we selected an additional 32 claims. We sorted the data into dollar amount ranges and then in alphabetical order. Using a random number generator, we selected nine payments in the $500 - $999 range, nine payments in the $1,000 - $4,999 range, nine payments in the $5,000 - $19,999 range and five payments in the $20,000 - $34,999 range. We reduced our sample of claims to 25 because seven of the claims did not meet our testing criteria: five claims were subject to bidding requirements, one claim included only invoices below the $500 threshold and one claim was for travel reimbursement to a District employee and not subject to quotes. Of the 25 claims, six required one to three verbal quotes according to the Board-adopted policy and 19 required at least two written quotes.

- Of the 11 claims reviewed from approved contract vendors that required at least two written quotes, one claim was paid to a professional service provider who had been selected by the District through a State contract; therefore, the District was not required to obtain this vendor through a competitive process. Of the 19 claims reviewed that required at least two written quotes, seven claims were from six professional service providers. We reviewed available vendor contracts/agreements for these seven professional service providers.

- We interviewed appropriate District officials to gain an understanding of the IT system and financial software. This included inquiries regarding policies and procedures, user access and remote access.

- We obtained a list of all financial software user accounts and their access rights to determine who had access, if users had their own username and password and if their access to the financial software was consistent with their job responsibilities.

- We reviewed a financial software audit log to determine if there was any unusual access or modifications or deletions to the data.

We conducted this performance audit in accordance with 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 D

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 E

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

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Nathaalie N. Carey, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building - Suite 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

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, 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

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

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, 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: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

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

Serving: Nassau and Suffolk Counties

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

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester 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
Rebecca Wilcox, 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

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313