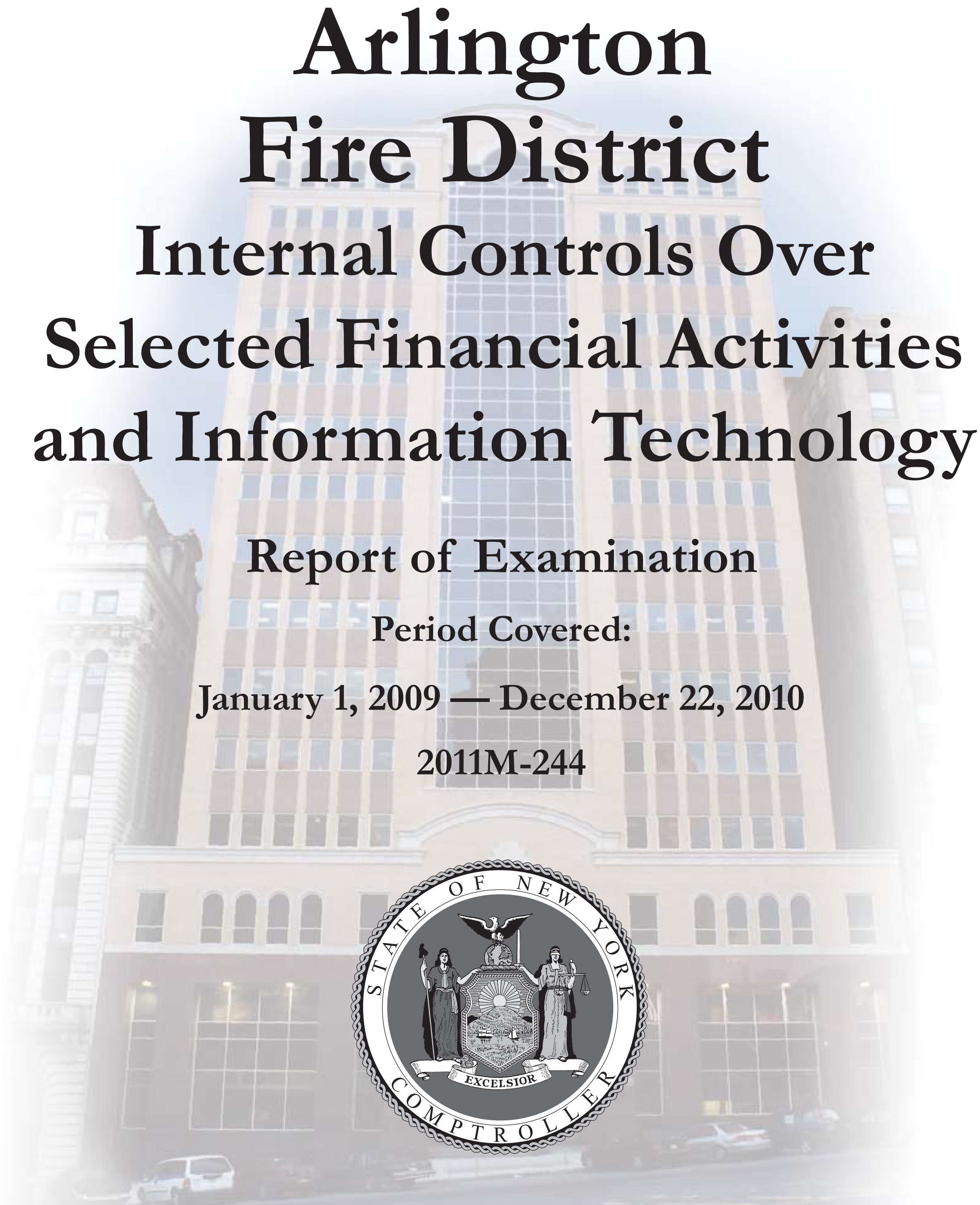
Office of the New York State Comptroller

Division of Local Government
& School Accountability



Arlington Fire District

Internal Controls Over Selected Financial Activities and Information Technology

Report of Examination

Period Covered:

January 1, 2009 — December 22, 2010

2011M-244

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

May 2012

Dear Fire 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 Commissioners' 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 Arlington Fire District, entitled Internal Controls Over Selected Financial Activities and Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for 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

EXECUTIVE SUMMARY

The Arlington Fire District (District) is located in the Town of Poughkeepsie. The District covers approximately 22 square miles and provides fire and emergency medical services to 31,593 residents from four fire stations manned by 78 paid and 83 volunteer members. The District is a corporation of the State, distinct and separate from the Town, and is governed by an elected five-member Board of Fire Commissioners (Board). The Board is responsible for the overall financial management of the District, including establishing appropriate internal controls over fiscal operations and information technology. The District's budget for the 2011 fiscal year was $14.9 million, and was primarily funded by real property taxes.

Scope and Objective

The objective of our audit was to review the District's internal controls over selected financial activities and information technology (IT) for the period January 1, 2009 through December 22, 2010. Our audit addressed the following related questions:

- Does the Board adequately monitor financial activities to ensure that District assets are safeguarded?
- Is the District's Length of Service Awards Program (LOSAP) properly administered to adequately safeguard District assets?
- Are internal controls over IT appropriately designed and operating effectively to adequately safeguard District assets?

Audit Results

The Board needs to improve its oversight of District operations. Because the Board did not adopt or implement adequate policies and procedures, or sufficiently monitor District activities, the District's assets are at an increased risk of being wasted or abused. For example, the Board did not exercise sufficient oversight to ensure that the District was receiving quality services from an IT contractor to whom it paid $147,480. Further, the Board did not do a needs assessment prior to buying three sport utility vehicles, costing a total of $108,060, that the District had not yet put in service nearly two years after they were purchased.

The Board and District officials did not establish sufficient controls over the District's Length of Service Awards Program to ensure that qualified service award credit was being accurately reported for its volunteer members. We found that six of 12 volunteer members reviewed were improperly reported to the program administrator as having attained the points necessary to receive service award credit for the 2010 plan year. Not all service award points given were supported by electronic records or source documents, and the service award point system did not include clear guidance for the calculation of service award points for some categories of activities.

District officials also have not established procedures for the backup of critical electronic data and the verification of the data's integrity, and have not developed a disaster recovery plan. Controls over electronic data were not sufficient to protect sensitive and confidential data stored on District servers, and the District does not have policies and procedures for the transmission of sensitive data on portable drives. Non-technology District personnel have domain and computer operating system administrative rights, and user permissions for the District's financial software were not assigned to restrict access to necessary routines and to adequately segregate incompatible duties. Finally, District computers were used in violation of District policy.

Comments of Local 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. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated that they planned to take corrective action. Appendix B includes our comments on issues raised in the District's response letter.

The Board has the responsibility to initiate corrective action. Pursuant to Section 181-b of the 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.

Introduction

Background

The Arlington Fire District (District) is located in the Town of Poughkeepsie. The District is a corporation of the State, distinct and separate from the Town, and 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 over fiscal operations and information technology (IT), and safeguarding District assets. The Board designates the depositories for District funds, audits and approves claims for payment, and authorizes investments of the District's moneys. In addition, the Board has the power to levy taxes on real property located in the District and to issue debt to finance District activities. The District's budget for the 2011 fiscal year was $14.9 million, and was primarily funded by real property taxes.

The District covers approximately 22 square miles, and provides fire and emergency medical services to 31,593 residents. The District operates out of four stations, manned by 78 paid and 83 volunteer members. District members responded to 5,174 fire and emergency medical calls in 2010. Paid members are represented by the Arlington Professional Fire Fighters Association (APFFA). The District's 2010 expenditures for personal service were $7.7 million. Total expenditures for overtime in 2010 were $1.4 million.

Objective

The objective of our audit was to review the District's internal controls over selected financial operations and IT. Our audit addressed the following related questions:

- Does the Board adequately monitor financial activities to ensure that District assets are safeguarded?
- Is the District's Length of Service Awards Program (LOSAP) properly administered to adequately safeguard District assets?
- Are internal controls over IT appropriately designed and operating effectively to adequately safeguard District assets?

Scope and Methodology

We examined the District's internal controls over selected financial operations, LOSAP, and IT for the period January 1, 2009 to December 22, 2010. Our audit disclosed areas where additional IT security measures should be instituted to help prevent unauthorized access to District assets. Because of the sensitivity of some of this information, certain specific vulnerabilities are not discussed in this report, but have been communicated confidentially to District officials so that they could take corrective action.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix C of this report.

Comments of Local 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. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated that they planned to take corrective action. Appendix B includes our comments on issues raised in the District's response letter.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of the General Municipal Law. 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. We encourage the Board to make this plan available for public review in the Secretary's office.

Board Oversight

The Board is responsible for designing internal controls that help safeguard the District's resources and ensure that these resources are used economically and efficiently. An adequate system of internal controls includes having clear policies and procedures that promote effective operations and the prudent use of resources, and provide for proper oversight by the Board and District officials. The Board should ensure that the District incurs only the overtime costs that are necessary for District operations. Further, the Board should ensure that fuel purchases are made for District purposes and that fuel is safeguarded from misappropriation. In addition, the Board must ensure that controls are in place so that the District purchases only the number of vehicles that are necessary for District operations. Such controls help ensure that taxpayer moneys are spent prudently and for District purposes.

The Board did not adopt and implement comprehensive written policies and procedures to provide adequate guidance and internal controls over overtime, contracted IT services, fuel use, and management of the District's fleet. District officials did not establish procedures to properly monitor the scheduling of overtime and verification of overtime worked and, as a result, incurred excess costs. Controls over fuel tank inventories were weak, records of fuel inventory use were not complete, and information from which to determine the legitimate use of District gas purchase cards was not available. Finally, the District acquired more vehicles than needed and, as a result, three sport utility vehicles valued at $108,060 were not in service almost two years after purchase. As a result of these deficiencies, the Board cannot assure taxpayers that it expended their moneys in the most cost-effective manner.

Overtime

Personal service costs represent the most significant portion of the District's budget. While overtime pay can be an expected cost of doing business for a fire district with paid firefighters, it is a cost that must be carefully monitored and controlled. To establish adequate controls over overtime, District officials must adopt overtime policies and procedures and ensure that they are properly implemented or followed. Effective controls include written pre-approval for the overtime, subsequent supervisory verification on the employees' time cards, and overtime logs to document the date, time, and purpose of the overtime hours worked. Such controls help ensure that overtime is properly authorized, clearly documented in overtime records, and actually performed.

The District's paid firefighters receive overtime for all hours worked over 40 hours per week at a rate of time and a half. Overtime-eligible paid members receive two mandated hours of overtime each week. Paid members may elect to accumulate compensatory time off at the overtime rate instead of being paid for working overtime. In 2010,[1] the District paid $1.4 million for 17,330 overtime hours worked, primarily resulting from the need to cover for vacations, holdovers,[2] and continuing medical education. Members also accrued 977 overtime hours as compensatory time, valued at $34,397.

The District's agreement with the APFFA authorizes a union overtime chairman to use overtime to maintain the minimum staffing levels required by the agreement. District officials have established informal procedures for weekly payments of overtime. However, District officials did not establish procedures to properly monitor the scheduling of overtime and verification of overtime worked. Specifically, District officials:

- Did not review overtime assigned by the union overtime chairman to maintain minimum staffing. (The union overtime chairman is a paid member eligible for overtime and, therefore, another official should review his overtime to ensure that it is accurate.)

- Did not require documented approval of overtime assigned for purposes other than minimum staffing, or subsequent supervisory verification of the time worked

- Did not verify that overtime work for purposes other than training was actually performed

- Did not approve the payment of overtime or earning of compensatory time in lieu of payment.

When procedures are not in place to adequately monitor overtime, the District could make unnecessary overtime payments to employees or even pay for work that was not authorized or performed.

Procurement of Information Technology Services

Professional services generally include services rendered by accountants, attorneys, engineers, information technology (IT) specialists and others requiring specialized skill, training and expertise, use of professional judgment or discretion, and/or a high degree of creativity. The Board is responsible for establishing procurement

[1] Of the $1.4 million in overtime paid in 2010, up to $389,922 was attributed to mandatory overtime.

[2] A holdover occurs when a member is required to work after his specified shift ends.

policies and procedures that ensure that the District receives quality services at reasonable prices. It is important that the Board require detailed contracts be executed with all professional service providers that fully define the nature and extent of the services that they will provide and the methods by which District officials can confirm the quality of the services performed. District officials must oversee vendor activities to ensure that the District receives quality services in compliance with contractual provisions.

The District contracts with a consultant to provide IT support and maintenance. In 2004, the District entered into a service agreement with a consultant who provided support during the majority of our audit period. Per the service agreement, this consultant was to provide ongoing daily support for workstations, servers and the network infrastructure, and recommend steps to improve their service and reliability. The agreement contained a warranty that all services performed under the agreement would be performed consistent with generally prevailing professional or industry standards. However, the agreement did not address the method by which District officials would confirm the quality of the services performed. During the audit period, the District paid this consultant $147,480 for professional IT services: $74,455 in 2009 and $73,025 in 2010.[3]

The Board did not exercise sufficient oversight over services received by the contracted IT consultant to ensure that the District was receiving quality services. We found numerous deficiencies in the District's IT system that the consultant did not correct,[4] and found that the consultant did not employ basic security practices. For example, there were significant weaknesses with the configuration of the District's network that increased the risk that sensitive data stored on District servers could be accessed by unauthorized individuals. A number of vulnerable services were running on District servers, which could have caused a variety of problems from a denial of service to a compromise of systems and data integrity. Further, the web server operating system (OS) was 11 years old at the time of our audit and support for this OS ended in July 2010. In addition, we found a multitude of other security vulnerabilities which we have separately communicated to District officials.

We reviewed the service detail of 14 payments made to the previous consultant totaling $61,730[5] and tracked the 521 specified activities

[3] In November 2010, the District contracted with a new IT consultant when the former consultant relocated out of the area.

[4] These deficiencies are in addition to the deficiencies discussed in the Information Technology section.

[5] We judgmentally selected all payments from the eight months during the audit period in which the largest payments were made to this vendor and for which the vendor submitted detailed activity reports to the District.

to identify unresolved recurring issues with the District's IT system.[6] We found 15 recurrences of service for unresolved issues related to email and 12 recurrences of service for unresolved issues related to remote access and connectivity over a 14-month time period. We also found numerous recurring instances of unspecified generic services: 30 recurrences of service for user administration and 24 recurrences of service for website maintenance over an 18-month period, and 13 recurrences of service for server monitoring over a three-month period. When issues are not corrected, the District repeatedly pays for the same service, and may expend more than necessary. Without details of the service provided, the District cannot be certain that it received the services for which it paid, and cannot properly monitor the quality of services received.

Fuel

The Board is responsible for ensuring that controls over fuel consumption are in place to ensure appropriate use of District resources. The Board should adopt policies that require limiting access to fuel stores, maintaining perpetual inventory records, and conducting periodic inventories to reconcile inventory records to physical inventory levels. In addition, the Board should adopt a comprehensive policy for gas purchase cards, which describes how the cards can be used and by whom, the documentation needed to support purchase card claims, and the District's recourse in the event of improper card use. The policy also should establish custody of the cards when not in use, require proper documentation for all transactions, and establish a means to recoup any unauthorized expenditures.

The District did not have written policies and procedures for controlling vehicle fuel inventories and the use of District gas purchase cards. As a result, controls over fuel tank inventories were weak, records of fuel inventory use were not complete, and information was not always submitted to determine the legitimacy of District gas purchase card use.

<u>Fuel Inventories</u> − Complete fuel inventory and usage records help District officials account for all purchases made, inventories on hand, and the use of these consumable assets. The periodic reconciliation of fuel inventory readings with recorded usage is an important control to help reduce the risk of errors and/or irregularities occurring and not being corrected.

[6] The 14 payments were for 1,139 service hours provided in 43 out of 85 weeks invoiced over the 18-month period. An average of 25 hours per week was invoiced in the 24 weeks reviewed in 2009, and an average of 28 hours per week was invoiced in the 19 weeks reviewed in 2010.

The District has two above-ground fuel tanks located at one of its remote fire stations: one 3,000 gallon tank for diesel fuel and one 1,000 gallon tank for regular unleaded gas. The District purchased 30,154 gallons of diesel fuel totaling $65,813, and 20,283 gallons of unleaded gasoline totaling $40,702 for the District fuel tanks during our audit period. Controls over access to District fuel inventories were not sufficient to adequately safeguard District fuel assets, and available records were not sufficient to determine the legitimate use of fuel inventories. We found that:

- The District did not have written policies and procedures for controlling vehicle fuel inventories.

- Neither the fuel tanks nor the switches to operate fuel tank pumps are enclosed or locked, and the switches remain turned on throughout the day.

- Not all fuel pumped from District tanks is recorded in daily fuel logs. Fuel pumped from the above-ground fuel tank into the District fuel truck tanks used to fill equipment at other District stations was not recorded in the log used to maintain electronic vehicle fuel usage records. Additionally, fuel can be easily removed from the fuel truck tanks when the truck is unlocked.

- District officials did not conduct fuel inventories and maintain fuel inventory records, which did not allow for the reconciliation of fuel usage with deliveries and inventories.

The failure to restrict access to District fuel tanks and to ensure that District personnel maintained adequate fuel purchase and delivery records, recorded periodic inventory, and reconciled inventory with usage readings places the District at a significant risk of unauthorized use or theft of the District's fuel supplies.

<u>Gas Purchase Cards</u> − The Board is responsible for ensuring that all transactions on the District’s gas purchase card billing statements are reviewed to verify that charges are supported by adequate documentation and are legitimate. It is essential that the person who performed each transaction and the vehicle fueled is identified to provide accountability for expenditures charged to District purchase cards. The vehicle mileage at fueling also should be required to facilitate analysis of vehicle fuel usage to detect non-District fuel purchases.

The District purchased $10,401 of gasoline using purchase cards issued through a direct account with a fuel vendor from January 2009 through June 2010, and $8,755 from June 2010 through October 2010 using cards issued through a sub-account of the Town of Poughkeepsie with the same vendor. District officials issued 10 cards under the District's direct account, six were distributed to the Deputy Chief and captains, and the four remaining cards were used as needed for other District vehicles. District officials subsequently issued 35 gas purchase cards under the sub-account, which were distributed and assigned to specific District vehicles.[7]

The Board did not develop policies and procedures establishing controls over gasoline purchase cards. Consequently, records for fuel purchases using District gas cards did not provide sufficient, reliable information to determine legitimate use of the cards. Billing statements for the direct account did not identify the vehicle being fueled, and the submitted purchase receipts did not always identify the vehicle being fueled, the purpose for the purchase, or the vehicle mileage. We reviewed 33 purchase card transactions[8] totaling $2,108 and found that 17 did not have sufficient available data, such as identification of the vehicle, to support the use of the gas card for a legitimate purpose. In addition, 19 transactions did not have sufficient available data, such as identification of the vehicle, vehicle mileage at fueling, and the previous vehicle mileage, to calculate vehicle miles per gallon and determine the reasonableness of vehicle miles per gallon.

When the District made purchases under the Town's sub-account, gas purchase cards were not always used in a manner to provide reliable data for a proper analysis of card use. We reviewed seven months of statements and found four instances in which vehicle odometer readings provided on the statement were inconsistent with the previous transaction reading for the same vehicle. The Deputy Chief told us that this was due to the purchase of gas for vehicles other than the ones to which the cards were assigned. When odometer readings provided on the statement were inconsistent with the previous reading for that vehicle, the purchase was not entered into electronic vehicle fuel usage records, resulting in incomplete vehicle fuel usage records. District officials' failure to implement adequate internal controls regarding the use of gasoline purchase cards could result in the District incurring unauthorized and/or inappropriate charges.

[7] When the District changed to the Town's sub-account, purchase cards were used as the primary means to purchase gasoline for District vehicles, and the District discontinued routinely filling District vehicles from the District's unleaded gasoline fuel inventories.

[8] We judgmentally selected three months from the first 18 months of our audit period when the District had a direct account with the vendor, and tested all gas card purchase transactions on the voucher invoices.

Fleet Management

It is important that an effective fleet management program for any local government establish guidelines for the acquisition, utilization, maintenance and repairs, and replacement and disposal of vehicles. To ensure that taxpayers only absorb the costs of services from which they will derive a benefit, the fleet management policy should require that a needs assessment be completed before any new vehicles are added to the fleet. It is important that the needs assessment specifies the proposed use of the vehicle and the estimated number of miles per year the vehicle is expected to be driven. The policy also should require that the vehicle utilization be reviewed annually and other alternatives to purchasing vehicles be considered.

The District's Apparatus Purchase Plan includes four to five year replacement and/or reassignment plans for staff vehicles. However, the Board did not formally adopt policies and procedures for the management of the District's fleet. Consequently, the District acquired more vehicles than needed, and certain vehicles are under-utilized.

The District purchased three sport utility vehicles for $108,060 in August 2009. However, District officials did not complete a needs assessment for these vehicles prior to purchase. While the vehicles were initially purchased to support the reassignment of two staff vehicles and add an emergency medical vehicle to the existing fleet, District officials subsequently decided to use two vehicles for emergency medical purposes and the other to support the reassignment of a front-line command vehicle.

These three vehicles had not yet been put into service 20 months after purchase. In April 2011, 20 months after purchase, the vehicles had been individually driven 1,411, 359, and 972 miles. While District officials told us that it took time to customize these vehicles prior to their use, we question the need for these vehicles given that they were not in service almost two years after purchase. When vehicles are purchased unnecessarily, funds are no longer available for essential purchases, and taxpayers are absorbing the cost for future services from which they may not benefit.

Recommendations

1. The Board should adopt an overtime policy and develop written procedures to implement the policy. These policies should provide clear guidance regarding overtime and require approval in advance before an employee is permitted to work overtime.

2. District officials should ensure that all written agreements for IT services clearly define expected services, provide a means for monitoring quality and price, and provide the District and the service provider with a clearly defined and mutually agreed upon basis for determining service quality and cost.

3. District officials should develop written, comprehensive internal control policies and procedures for the District's fuel inventories that address the safeguarding of fuel and the maintenance of accurate and timely inventory records.

4. The Board should develop and implement written policies governing the use and control of fuel purchase cards.

5. District officials should maintain fuel consumption records and perform analytical reviews to ensure that miles per gallon per vehicle are consistent between fueling, recorded fueling does not exceed the vehicle's tank capacity, and the dates and times of fueling are reasonable.

6. The Board should establish and adopt comprehensive written policies and procedures relating to the key aspects of the District's fleet management operations, including the acquisition, utilization, maintenance, replacement and disposal of all District-owned vehicles.

7. Once adopted, the Board should periodically review its fleet management policies and procedures for adequacy and to ensure compliance.

8. The Board should ensure that each vehicle purchased is supported by an accurate needs assessment.

Length of Service Award Program

The District sponsors and funds a defined benefit length of service award program (LOSAP). The purpose of a LOSAP is to facilitate recruitment and retention of volunteer firefighters by providing them with a monthly pension-like benefit based upon their years of qualified service to the community. To receive yearly service credit, each member must accumulate at least 50 points, which are earned by participating in activities defined by General Municipal Law (GML) and the District's service award program point system. In general, upon reaching entitlement age, program participants will receive a benefit of up to $20 a month for each qualified year of service, with a maximum benefit payable of $800 a month. The District's contribution for the 2010 service award program year was $92,001. As of December 31, 2010, program assets totaled $2.1 million.

The Board and District officials did not establish sufficient controls over the District's LOSAP. District officials have not implemented procedures and controls to ensure that qualified service award credit is being accurately reported for its volunteer members. We found that six of 12 volunteer members reviewed were improperly reported to the program administrator as having attained the points necessary to receive service award credit for the 2010 plan year. Not all service award points given were supported by records or source documents, and the service award point system did not provide clear guidance for the calculation of service award points for some categories of activities. In the absence of controls to ensure that qualified service award credit for its volunteer members is being accurately reported, there is an increased risk that the District will pay benefits that were not legitimately earned.

Documenting and Monitoring − To ensure that only those volunteers who earned 50 points or more are given service credit, District officials must establish standards and procedures for the administration of the LOSAP that, among other things, outline the fire companies' documentation of volunteer activities for which the volunteers may earn service credit. Additionally, to ensure proper internal controls, computerized application systems should only allow authorized users access to electronic records used to determine annual service award points. Various officers,[9] as defined by each company, are responsible for maintaining activity records that are used to determine service award points. The District's Service Award Program Point System delegates the responsibility for maintaining point system records to the volunteer fire companies. The point system requires that volunteers

[9] Service Award Administrators, Captains, Lieutenants, Recording Secretary

strictly comply with sign-in procedures for verifying attendance at activities, and that attendance sign-in sheets be produced upon demand if the Service Award Program's records are audited.

District officials have not implemented procedures and controls to ensure that qualified service award credit is being accurately reported for the District's volunteer members. District officials did not verify annual service award points reported by the volunteer fire companies. They also did not sufficiently monitor the LOSAP program to ensure that volunteer fire companies retained original documentation to support LOSAP points given. In fact, two of the District's four volunteer fire companies could not provide any sign-in sheets to support participation in activities from which LOSAP points were earned in the 2009 and 2010 years, and one of the two remaining companies could only provide sign-in sheets for one full month in 2010. As a result, 10 of the 12 volunteers included in our sample did not have sign-in sheets on file to support the points credited to them for participation in incident responses.

We also found that District officials did not establish procedures to ensure that access to electronic records used to determine annual service award points was restricted to officers responsible for maintaining such activity records. We reviewed user accounts for 18 of 44 volunteers[10] who had permissions to add and edit staff activities in the electronic application and found that only three were designated officers. The other 15 users were volunteer firefighters, emergency medical service volunteers, or volunteer fire police, and included two who were on leave. When access to records is granted to unauthorized individuals, the risk is increased that they could enter service award points that were not earned.

Without procedures and controls to ensure that qualified service award credit for its volunteer members is being accurately recorded and reported, the District may pay for benefits that have not been legitimately earned.

<u>Service Award Program and Point System</u> − GML[11] allows a service award sponsor to adopt its own point system that must adhere to statutory requirements. The District established a service award program point system that consists of eight categories of activities for which firefighters can earn points. This system establishes the number of points granted for the performance of each activity and the maximum number of points that can be earned for each category

[10] We judgmentally selected 18 from a total of 44 users in the Volunteer Member Level2 users group. The Volunteer Member Level2 users group has permissions to add and edit electronic activity records.

[11] GML Article 11-a, section 217

of activity. Volunteers can earn service credits for training courses, attendance at drills, holding a specific elected or appointed position, attendance at meetings, participation in department responses, miscellaneous activities, military leave, and line of duty disability. The entire maximum number of points for participation in department responses[12] is awarded once the member participates in the required percentage of calls during a calendar year, which is determined by the total number of calls a fire company as a whole responds to during the year. To be eligible to earn one year of service credit, an individual must be considered an active member of any one of the District's four volunteer fire companies, and earn at least 50 points under the service award program point system during that calendar year.

Each volunteer company has a service award administrator who is responsible for calculating annual service award credits earned for their company's volunteer members. Each year, the service award administrators submit a notarized list of all active members and their points earned to the Board for review and approval. However, the Board does not verify points submitted by the service award administrators. A Board Commissioner forwards this information to the firm that administers the District's service award program to determine the annual funding requirements of the program, the eligibility of the persons to be paid service award cash benefits, and the amount of benefits to be paid to such persons.

We selected 12 volunteer members who received service award credit for the 2010 program year for review.[13] We identified six members who were improperly reported to the program administrator as having attained the points necessary to receive service award credit, as follows:

- Fifty-six and 54 points were reported for two members who earned only 31 and 26 points, respectively. These volunteers, from the same company, were inappropriately awarded points for participation in departmental responses that were not calculated in accordance with the service award program point system.

- Fifty points were reported for three members who earned only 32, 31, and 27 points each. These volunteers were given points that were not supported by electronic records or sign-in sheets

[12] A maximum of 50 points can be earned for participation in department responses. A maximum of 25 points can be earned for response to fire calls, and a maximum of 25 points for emergency medical service calls.

[13] Our sample was judgmentally selected from participants reported to the program administrator as having earned less than 60 points in 2010, and also included all participants in the program who served as service award administrators for their respective fire companies in 2010.

for attendance at drills, company meetings and miscellaneous activities.

- Fifty points were reported for one member who earned only 37.5 points. This volunteer was inappropriately listed as having been on military leave because District records showed this member returned to active status in October 2009.

We also found discrepancies between the electronic records of activity and the sign-in sheets provided for these activities. For example, the electronic records for two volunteers indicated that they participated in 19 and 36 fire call responses and, therefore, met the requirement for participating in 16 fire calls to receive 25 points of service credit for incident participation. However, the source documents indicated that they responded to 15 and nine fire calls, respectively.[14] Electronic records are used to calculate service award credits earned. To ensure that members earn the correct credits, it is essential that the electronic records are accurate and supported by the source documents.

Further, although the District's service award program point system awards a maximum of 25 points per year for attending training and 20 points for drills, it does not provide a definition for either training courses or drills. Therefore, there is an inconsistency in the determination of service award point allocation for training and drills by the service award administrators for each volunteer company. One company administrator awarded training points for training received outside of the District, while another awarded training points only for training that was assigned and provided by the District. Further, one company administrator awarded points for drills for skills practice provided only by the company, while another awarded points for drills for any training event scheduled by either the District or the company.

Because the Board did not provide clear guidelines for determining points that could be earned, and did not verify points awarded by the service administrators, errors and irregularities occurred without detection and correction. As a result, members were awarded, and provided benefits for, service points that they did not earn.

Recommendations

9. District officials should develop procedures to ensure that qualified service award credit is being accurately recorded and reported for the District's volunteer members. The Board also should provide clear guidance regarding the distinction between training

[14] The service award administrator for their volunteer fire company did not award points for incident participation to these two participants.

and drills so that associated service points are appropriately and consistently awarded by the companies between these activities.

10. The Board should require its volunteer companies to maintain all required documentation including attendance sheets for verification of LOSAP service credits.

11. The Board should establish procedures to ensure that access to electronic records used to document and calculate eligibility for annual service award credit is restricted to authorized users in designated positions.

12. The Board should review and verify LOSAP points reported by the volunteer companies before submitting the annual report to the third-party administrator. The Board also should ensure that appropriate documentation is maintained, and strictly enforce the point system.

Information Technology

Computerized data is a valuable resource that District officials rely on to make financial decisions and report to State agencies. If computers on which this data is stored fail, or the data is lost or altered, either intentionally or unintentionally, the results could range from inconvenient to catastrophic. Even small disruptions can require extensive time and effort to evaluate and repair. For this reason, it is important that District officials control and monitor computer system access and usage, establish a formal disaster recovery plan, and ensure that computerized data and assets are physically secured. The Board is responsible for adopting policies and procedures and developing controls to safeguard computerized data and assets.

District officials have not established adequate internal controls to effectively safeguard computer systems and data. District officials have not established procedures for the backup of critical electronic data and the verification of the data's integrity, and have not developed a disaster recovery plan. Controls over electronic data were not sufficient to protect sensitive and confidential data stored on District servers, and the District does not have policies and procedures for the transmission of sensitive data on portable drives. Non-technology District personnel have domain and computer operating system administrative rights, user permissions for the District's financial software were not assigned to restrict access to necessary routines and to adequately segregate incompatible duties, and District computers were used in violation of District policy. As a result of these control weaknesses, the District's IT assets are at an increased risk of possible theft and of compromise by intentional or unintentional manipulation, loss or corruption. The District is also at risk of a potentially costly disruption to its critical operations.

Data Backup and Disaster Recovery – An effective IT internal control system includes a formal disaster recovery plan with policies and procedures to minimize the loss of essential data and to maintain or quickly resume critical operations if a disruption occurs. Data stored on computers and servers also must be backed up (a duplicate copy of information made) on a routine basis and stored remotely in a secure environment. Periodically, IT personnel need to verify the integrity of the backup data and test the effectiveness of the restoration process by restoring the data from the backup copy. To enhance security, backups also can be encrypted to render data unusable by unauthorized individuals. Establishing a detailed written agreement between the District and any outside service agency that performs these critical functions provides both parties with a clear understanding of the services expected of the outside agency.

The District does not have a disaster recovery plan, and District officials have not established procedures for the backup of critical electronic data and the verification of the data's integrity. The District's service agreement with its current IT consulting firm does not adequately define responsibilities in relation to backups, and does not specify the required frequency of the backups. The service agreement with the District's former IT consultant did not specify backups as part of the provided service. The former consultant did not provide a record of backup activities. Therefore, the District does not know if all expected files were backed up successfully. Further, neither the District nor the current consultant could ascertain the last successful restore of backup data, which would verify the effectiveness of the restoration process and integrity of backup data. Backups are not stored off-site; they are stored on external hard drives located in the server room at District headquarters. Though the server room is locked, it is accessed unsupervised by the District's communications vendor technicians and is not protected from fire and water. Additionally, backups of sensitive data are not encrypted to render data unusable by unauthorized individuals should a breach of security occur.

As a result of these control weaknesses, the District's IT assets are at an increased risk of loss and/or damage and potentially costly disruptions to the District's critical operations. The lack of a detailed written agreement deprives the District of protection in the event that an IT consultant defaults on its obligations, and there is no clear understanding of the extent of services that are to be provided.

Data Storage − District officials should establish internal controls over storing and securing data based on the potential harm that could result to individuals and/or the District if the information were to be inappropriately accessed, used or disclosed. Encryption can render data, for which a breach of security or improper disclosure could potentially cause great harm, unusable by unauthorized individuals. New York State Technology Law (Law) requires local governments to establish an information breach notification policy. The policy details how employers would notify New York State residents whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. The disclosure must be made in the most expedient time possible, 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 District has not established sufficient controls to protect sensitive and confidential data stored on District servers. Although access to confidential and sensitive information is controlled by a user account, the data is not encrypted for protection in the event that access controls are circumvented. Further, the Board has not established an information breach notification policy as required by Law. An individual's personal information, along with confidential business information, could be severely impacted if security is breached or data is improperly disclosed. Without an information breach notification policy, in the event that personal information is compromised, officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.

Data Transport – Universal Serial Bus (USB) drives are compact, portable data storage devices that plug into a computer's external port. Such drives offer a cost-effective, convenient method of storing, transporting, and downloading electronic data. However, these devices enable electronic data, including potentially confidential records, to be removed from District premises and subsequently accessed by an unauthorized individual with little difficulty. Therefore, data stored on USB drives should always be encrypted. It is essential for the District to have a security management program that includes policies and procedures for the secure storage and transport of sensitive information on these storage devices.

The District did not have controls in place for the transmission of sensitive data on portable drives. Therefore, users were allowed to connect non-encrypted, personally owned portable drives to networked District computers. Although the District's technology use policy prohibits revealing personal information about others, the District did not have procedures to prevent the removal of this sensitive information from the District's system. Without adequate controls over the use of these storage devices, the District is at an increased risk of the retrieval and misuse of sensitive information by unauthorized individuals.

User Account Management − Network access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. Access controls provide reasonable assurance that computer resources are protected from unauthorized use or modification. Generally, access controls should be based on the principle of least privilege, which maintains that users should have the most limited access rights possible to complete their authorized duties. A system should provide a process to identify and differentiate users to control electronic access. User IDs enable the system to recognize specific user accounts, grant the appropriately-authorized access rights, and provide user accountability for computer transactions. Each individual on the network should be assigned a unique user ID. Under no circumstances should user accounts and passwords be shared, as this would compromise all the other associated controls. An employee's unique user account and user access should be disabled when the individual is on extended leave, or when employment has been terminated.

District officials did not develop or enforce formal procedures for network user account management. Group accounts were established for generic use by more than one individual. Of the four group user accounts we identified on the domain controller, one account, though enabled, appears to never have logged onto the system. We also examined all 19 domain user accounts identified as those of retirees and found that all remained enabled for up to 24 years after retirement. Further, the network user account assigned to the District's attorney was enabled but not actively being used. This account last logged into the network 338 days prior to our test date.

When inactive user accounts remain enabled, a user or attacker could gain access to data and transactions for which they are not authorized, resulting in the manipulation and/or loss of data.

Administrative Rights – Domain and administrative rights give users full authority to create, delete and modify files, folders or settings on a computer. If an unauthorized user were to gain access to an account with domain or administrative rights, that person would have the ability to install programs, download or destroy data, and change log files to cover such actions. Even if an unauthorized user did not have malicious intent, mistakes and accidents could occur, such as unintentional deletions and modifications that could be detrimental. Therefore, it is important that the number of users having administrative rights be limited to the IT coordinator and a designated back-up person. Furthermore, even those designated individuals must only use the administrator accounts when absolutely necessary.

Non-technology District personnel have domain and computer operating-system administrative rights. We identified 10 accounts as global administrator accounts, authorized to administer – or control through configurations, additions, deletions, installations, and modifications – every object[15] on the domain. Of the 10 global administrator accounts, seven belonged to users with no need for administrative access: the part-time bookkeeper; the part-time Business Manager; the secretary; a Career Captain; the Assistant Director of Emergency Medical Services; the Director of Emergency Medical Services; and a scanner. These users do not fulfill an IT job function and do not require domain level administrator privileges. Additionally, 76 accounts have local administrator access for network

[15] Objects can include user and computer accounts, software packages, group policies, security templates, email distribution groups, and more.

devices, which means that they have the capability to install, delete and modify programs and settings on any device they are logged into.

Our review of the groups and users on seven District computers[16] found 10 user accounts assigned to the computer local administrators group. Local administrative rights on three of the computers were assigned to one shared account that can be used by anyone in the District. Local administrative rights on the other four computers were assigned to nine users who did not have administrative IT responsibilities (the assistant director of emergency medical services, four captains, three lieutenants, and the part-time business manager).

Administrative rights appear to have been indiscriminately and unnecessarily assigned on the domain and individual District computers. Indiscriminate assignment of administrative user rights exposes the District's systems and data to an increased risk of loss, corruption or misuse.

User Access Rights – To ensure proper segregation of duties and internal controls, the computerized application systems should allow user access to only those computer functions necessary to fulfill job responsibilities. Having access controls in place provides for proper segregation of duties so that users are not involved in multiple aspects of transactions. When it is not possible to adequately segregate duties, District officials should establish compensating controls, such as requiring someone who is independent of the process to review the employee's work. Generally, a system administrator is able to control and use all aspects of the software, such as giving users complete access to create, delete, and modify files, folders, or settings on a computer. A good system of controls requires that this position be separate from the Business Office function.

Controls over access to software applications used by District employees are not adequately designed. The District does not have a formal process to add, delete or modify user access to applications. As a result, user access to the District's financial software[17] was not assigned based on job duties and to adequately segregate incompatible duties. Of the four financial software user accounts,[18] permissions for three users were not assigned to adequately segregate accounts payable duties. The bookkeeper, Treasurer and Business Manager

[16] We judgmentally selected seven out of 18 computers at the District's headquarters building. Our sample selection was based on the location of the computer and the number of potential users of the computer.

[17] The District's financial software is used for processing payables, reconciling bank accounts, budgeting and financial reporting.

[18] We reviewed all four of the financial software user accounts: those of the Treasurer, Business Manager, Secretary, and the administrator account used by the bookkeeper.

have the ability to add new vendors, enter disbursements, and print checks. User access to these functions could not be individually assigned because the software groups several functions in one "Area," which is the level at which user access can be assigned.

We also found that the Business Manager was given full access rights to an area that gives users the ability to write, void, and print checks. These functions are not relevant to the Business Manager's responsibilities. Further, the bookkeeper does not have her own user account; she uses the administrator account when accessing the application. Using the administrator account, the bookkeeper has access to all areas in the application, including changing and deleting transactions. We also observed the Treasurer using the administrator account to access the application on the bookkeeper's computer.

Ineffective controls over the assignment of a user's access to the financial software system could result in unauthorized access, manipulation, and the loss of financial data, which may not be detected and corrected in a timely manner. Additionally, by using the administrator account, the bookkeeper has access to all areas of the financial software and could manipulate data to conceal inappropriate transactions.

Computer Usage – A good system of IT controls starts with policies to define appropriate user behavior, and the tools and procedures necessary to protect information systems. Such policies should include procedures governing the acceptable use of computers and the internet, and hold users accountable for the proper use and protection of District resources. Prohibiting the installation of unauthorized software by system users is crucial in preventing potentially harmful software from infecting District computers. Unauthorized programs could transfer personal or sensitive information to outside networks, potentially slow down the network, or cause system crashes and loss of data.

To help protect the District's computing environment, the Board adopted a technology use policy that requires that all employees use District technology resources only to enhance fire or emergency medical service to the public. Users are required to sign a technology user agreement form acknowledging that they have read and understand the technology use policy, and agree to abide by its provisions. The policy identifies prohibited activities which include, but are not limited to, any personal use that interrupts District business and keeps an employee from performing his/her work, downloading or copying music for non-District purposes onto District equipment, downloading or installing software onto District equipment without permission from the IT Operations Manager, non-District related streaming media, and using, accessing, or transmitting pornographic or sexually-explicit materials.

We reviewed seven computers at the District's headquarter building[19] and found 21 installations of software on six of the computers that were either in violation of District policy, posed security threats, or did not appear to serve a valid District purpose. For example,

- Eleven software installations indicated use in violation with the District's technology use policy. For example, one software installation contained a program that helps facilitate and organize the download of new music.

- Two software installations had security threats, including a process that allows users to win sweepstakes every time they make an online purchase. This process installs adware – possibly spyware – and a toolbar that are difficult to remove.

- Six installations did not appear to serve a valid District purpose; for example, a browser plug-in for music that allows the user to play different instruments, transpose music, and save or print out musical scores on the internet.

We also found internet use that was in violation of the District's technology use policy. We reviewed cookie[20] files of 11 user accounts on three District computers for internet activity[21] and found prohibited internet access on one computer. Nine websites visited by this computer during evening hours on two different days contained pornographic material. This computer was able to access prohibited sites because the District did not have internet content filtering in place during that time.[22] Further, although two of these nine websites do not host malware, they may contain embedded links to sites which do host malicious content.

These violations occurred because District officials did not establish procedures to enforce the technology use policy. Without measures

[19] We judgmentally selected seven out of 18 computers at the District's headquarters building. Our sample selection was based on the location of the computer and the number of potential users of the computer.

[20] A cookie is a small file or part of a file stored on an internet user's computer, created and subsequently read by a web site server, containing personal information such as a record of pages visited.

[21] For our sample, we selected one computer that is shared among all career firefighters and two computers that are in isolated office areas. We judgmentally selected users based on the existence of cookies during the audit period.

[22] At the time of our audit, the District's current IT consultant was in the process of installing routers on which internet filtering would occur and identifying websites that are not necessary for District operations.

to enforce the policy, District resources may be improperly used or expended. Further, the unauthorized download and installation of software exposes the District's network to potential damage from malicious software that may not be properly screened for current technological threats. Malicious software could infiltrate the network, thereby potentially destroying, manipulating, or stealing data. In addition to using District resources for non-District business, inappropriate internet use puts the District's network at risk due to potential exposure to sites which host malicious content.

Recommendations

13. District officials should develop a formal disaster recovery plan that addresses the range of threats to the District's IT system, distribute the plan to all responsible parties, and ensure that it is periodically tested and updated as needed.

14. District officials should establish policies and procedures to address the backup and restoration of critical electronic data. District officials also should establish a process that requires District personnel to periodically test backups to ensure data integrity.

15. The Board should establish policies and procedures for the secure storage and transport of sensitive information residing on computer hard drives, portable media, and peripherals.

16. District officials should discontinue the practice of using group user accounts and require that only individual user accounts are used to access the District's information technology system.

17. District officials should examine all network accounts to determine if they are still being used, when they were last accessed, and if the passwords are being changed. All old, unused, or otherwise defunct accounts should be disabled and deleted after examination.

18. District officials should reduce the number of domain and computer operating system administrators to those who have a valid business need for this capability.

19. District officials should ensure that user access rights to District software are appropriately restricted to correspond with employees' job functions or member needs.

20. District officials should establish procedures to monitor and enforce the District's technology use policy. This includes implementing the use of a content filter in accordance with their policy and monitoring internet use for inappropriate use.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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

Arlington Fire District

11 Burnett Boulevard
Poughkeepsie, NY 12603
www.afd.org

Business: (845) 486-6300
Fax: (845) 486-6322

For Emergencies
DIAL 911

"Safeguarding Our Community"

April 25, 2012

Mr. Christopher J. Ellis
Chief Examiner of Local Government
and School Accountability
Office of the State Comptroller
33 Airport Drive, Suite 103
New Windsor, NY 12553

Re: Arlington Fire District
Draft Report Internal Controls over Selected
Financial Activities and Information Technology
Report of Examination 2011M-244
Response to Draft Report

Dear Mr. Ellis:

This letter will confirm that the Board of Commissioners is in receipt of your preliminary draft findings ("Draft") and hereby submits its comments on the Draft following the exit conference. The Board has carefully reviewed the Draft and while this response sets forth some concerns relating to it the Board will prepare a Corrective Action Plan dealing with the issues raised therein, which will be submitted in accordance with the time lines established for that response. The Board views the Draft as an opportunity to review and improve upon our practices and procedures and we certainly intend to utilize this opportunity as such.

The following are our comments with reference to the findings in the Draft:

BOARD OVERSIGHT

Overtime

The Draft recommends that the Board adopt written procedures for the implementation and processing of overtime. Currently overtime is calculated by the overtime chairman of the union. This calculation is reviewed and approved by the District bookkeeper, the Chief and the secretary to confirm that the purpose for the overtime was to meet the minimum manning requirements of the collective bargaining agreement (CBA).

See
Note 1
Page 32

The overtime procedures utilized by the Arlington Fire District as confirmed in the CBA are a result of an arbitration awarding to the union the right to control over time. The Board of Fire Commissioners has delegated to the Chief the obligation to control overtime based upon the daily operational concerns of the District. The Board will review this matter further with the understanding that any determinations or policy directives must be consistent with the decision.

Procurement of Information Technology Services

The Board is in general agreement with the findings and recommendations recognizing that the switch to the new IT vendor was promoted by many of the issues raised in this Draft. The Board believes that its new IT vendor has addressed most, if not all, of the issues raised in the Draft.

Fuel

The Board has reviewed the findings and recommendations and while it does not disagree that the procedures in the perfect world would account for each individual card being associated with an individual vehicle and an individual District member; District operations, however, often require that individual users take or be assigned to different District vehicles thereby making the reconciliation of mileage to individual cards impractical. Additionally it has been determined that when the District fuel truck is utilized to fuel fire fighting equipment there are times when excess fuel on the vehicle is also used to "top off" other District vehicles rather than returning the fuel to the sub station. Because of these operational issues the reconciliation of miles per gallon per vehicle cannot be performed on a specific basis although the District does generally monitor the fuel usage of each vehicle. In any event even if the District were to be able to alter its record keeping methods only a limited number of vehicles would be able to be monitored for mileage records as fire fighting equipment in service is left running at the scene and would therefore never be able to produce accurate data based upon the recommendations in the Draft.

See
Note 2
Page 32

With regard to the comments relating to the security of the fuel storage facility the Board will review the recommendations but believes that currently the security measures adequately protect the District. Although the tank is not locked fuel cannot be accessed from either the storage tank at the sub station or from the fuel truck without the pumping equipment functioning. The fuel tank at the substation is always manned and the fuel tanks are within full view of the substation personnel. Gasoline cannot be siphoned from the tanks due to screening in place in each tank.

Although the Board believes it adequately protects all fuel storage and monitors usage the Board will review these recommendations further prior to issuing a Corrective Action Plan.

Fleet Management

The Board is aware of the issues raised by the Draft and after a review has determined that the original plan for the purchase of the vehicles was undertaken at a time when staffing issues were being addressed to provide for a Battalion system within the District which, due to budgetary constraints, never was implemented. The Board agrees that all equipment must be purchased and utilized to best achieve the most economical use of taxpayer funds and notes now that all vehicles are in service and the District holds no excess equipment.

LENGTH OF SERVICE AWARD PROGRAM

The Board has carefully reviewed the findings and recommendations and is in general agreement with those recommendations. Since the individual companies had maintained and transmitted reports to the District the verification of the source records was in fact lacking. The Board is in the process of evaluating improvements to allow input to the firehouse software to maintain up to date records and is mandating that source documents be provided to the District on a quarterly basis to verify that input. The Board is reviewing the recommendations and will finalize a full response in its Corrective Action Plan.

INFORMATION TECHNOLOGY

The Board has carefully reviewed the findings and recommendations and generally concurs with those recommendations. The Board is having its new IT consultant review in detail each of the recommendations and believes that these have been, or will be, addressed and will further detail those items in its Corrective Action Plan. The Board was especially concerned with the Draft statement regarding unauthorized content on one District computer. The initial review by our IT consultant has not confirmed that finding and the Board will be reviewing that further prior to issuing its Corrective Action Plan.

See
Note 3
Page 32

Very truly yours,

ARLINGTON FIRE DISTRICT
BOARD OF FIRE COMMISSIONERS

Richard C. Dore

Richard Dore, Chairman

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

During our audit period, and at the time of our audit, the District did not have procedures in place to ensure that overtime assigned by the union overtime chairman actually maintained minimum staffing per the collective bargaining agreement with the firefighters union.

Note 2

Controls over access to District fuel inventories are not sufficient to adequately safeguard District fuel assets. Neither the fuel tanks nor the switches to operate fuel tank pumps are enclosed or locked, and the switches remain turned on throughout the day. Fuel can be easily removed from the fuel truck tanks when the truck is unlocked; the pumping equipment is operated by a simple switch. Therefore, it is important that District officials periodically reconcile fuel inventory readings with recorded usage to identify and address shortages.

Note 3

Our review of District computer use uncovered internet access that was prohibited by the District's technology use policy. On two different days, during evening hours, one of the District-owned computers was used to access or visit nine websites that contained pornographic material. We provided the details of our findings to District management so that they could take necessary action.

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 oversight, cash receipts and disbursements, purchasing, payroll and personal services, capital assets and inventories, the length of service award program and information technology.

During the initial assessment, we interviewed appropriate District officials, performed limited tests of transactions and reviewed pertinent documents, such as District policies and procedures, 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. We also reviewed the District's internal controls and procedures over computerized 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. We then decided on the reported objectives and scope by selecting for audit those areas most at risk, and evaluated those weaknesses for the risk of potential fraud, theft and professional misconduct. We selected expenditures, the length of service award program and information technology for further audit testing.

- We reviewed bargaining agreements, District policies, purchase plans, and length of service award program documents, and interviewed District officials and employees to gain an understanding of procedures used to control, record and monitor expenditures related to overtime, professional information technology services, fuel consumption, management of the District fleet, the administration of the LOSAP, and to obtain an understanding of internal controls over the information technology system.

- We obtained total overtime expenditures from annual financial reports. To determine the amount attributed to mandatory overtime, we used beginning of year and end of year hourly rates for each overtime-eligible firefighter, the overtime rate of pay, and the number of weeks for which career firefighters were paid for mandatory overtime in a year.

- We interviewed appropriate District employees to gain an understanding of informal procedures related to overtime scheduling, approval, and monitoring to determine if overtime was effectively managed.

- We compared required manning levels of the Arlington Professional Firefighters Agreement to actual staffing levels to determine if overtime was assigned when minimum staffing levels were met. We judgmentally selected overtime assignments and obtained pertinent information from weekly overtime reports, daily work schedule reports, personnel reports and payroll records.

- We obtained total expenditures for professional information technology services from electronic disbursement data and payment vouchers.

- We reviewed agreements with professional information technology vendors to gain an understanding of the services to be provided. We reviewed computer settings and configuration information obtained from District servers and judgmentally selected District computers to identify deficiencies in the information technology system as maintained by the primary vendor. We also examined service activity details contained in judgmentally selected vendor invoices to identify unresolved recurring issues with the District IT system.

- We obtained total fuel expenditures from electronic disbursement data and payment vouchers.

- We interviewed District employees, examined District fuel tanks, and reviewed daily fuel logs and electronic records to gain an understanding of controls over fuel inventories.

- We reviewed payment vouchers, electronic vehicle fuel usage records and fuel tracking sheets to determine if gas purchase cards were used for legitimate District purposes. We judgmentally selected three months during which the District had a direct account with the vendor and tested all gas card purchase transactions on invoices contained in the corresponding vouchers. We reviewed statements for all seven months of our audit period during which the purchases were made under the Town sub-account.

- We reviewed the Board resolution authorizing the acquisition of three sport utility vehicles and the District Apparatus Purchase Plan. We also interviewed District employees to determine the intended purpose of the purchase. To determine vehicle use, we obtained mileage of the vehicles at the time of purchase from vendor invoices and physically examined the vehicles' odometer readings for subsequent mileage. We obtained mileage of District vehicles currently being used for similar purposes from electronic vehicle records and compared it to the odometer readings of the newly purchased vehicles.

- We obtained the annual 2010 LOSAP contribution from the annual report prepared by the program administrator.

- We compared the District's Service Award Program Point System to the requirements of a service award program set forth in GML Section 217 to determine compliance with GML.

- We reviewed the District's service award point system and other LOSAP documents to ascertain the process used by the District for tracking and reporting annual service award credit. We also made inquiries to the service award administrators of the District's volunteer fire companies and to the Commissioner of the Board who serves on the District Service Award Committee for the same purpose.

- We obtained volunteer company worksheets that summarized annual service award points earned by each volunteer from various activities in the program year from certified 2010 service award program packets, and verified agreement with the 2010 annual LOSAP report prepared by the program administrator.

- We judgmentally selected volunteers who earned 50 to 60 service award points for the 2010 program year. We traced the number of points earned for each category of activity on company summary worksheets to appropriate electronic records (training, incident participation and non-incident activities) and available source documents (sign-in sheets) to verify whether points were awarded properly. We reviewed GML Section 219-a: Chapter 602 of the Laws of New York and subsequent legislation to gain an understanding of the audit requirements for Length of Service Award Programs.

- We reviewed the Arlington Fire District Control Book – IT Reference Manual prepared by the District's contracted information technology consultant to identify all District networks (both wireless and internal) and determine their locations.

- We ran scans on the District's internal and wireless network to determine their attributes. We connected to wireless access points and scanned the wireless subnet to determine protocols being run on access points and any connected devices. We ran port scans on the internal network to identify server services and protocols, along with any other services on the network. We also scanned the District's firewall on the internal and external devices. We identified vulnerable services and specific vulnerabilities using the standards set forth by the National Institute of Standards and Technology in their National Vulnerability Database.

- We interviewed appropriate District employees to obtain an understanding of internal controls over the District's financial, scheduling, personnel, operations and inventory computerized systems, and further reviewed select user privileges for each.

- We obtained computer settings and configuration information from judgmentally selected District computers and reviewed security information, groups and users, and installed software.

- We obtained computer settings and configuration information from critical District servers, and reviewed details of the operating systems, security information, groups and users, and installed services.

- We logged onto three judgmentally-selected District computers as a local administrator and examined the cookie files of users for internet activity that violated District policy. We judgmentally selected the users based on the existence of cookies during the audit period. We conducted further examination of judgmentally-selected websites visited by these users.

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

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

Steven J. Hancox, 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
Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

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

Serving: 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 AND REGIONAL PROJECTS
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