FOLLOW-UP OF

PERSONAL COMPUTER LICENSING

REPORT NO. 08-04-107F

City of Albuquerque
Office of Internal Audit and Investigations

City of Albuquerque

Office of Internal Audit and Investigations
P.O. BOX 1293 ALBUQUERQUE, NEW MEXICO 87103

September 24, 2008

Accountability in Government Oversight Committee
City of Albuquerque
Albuquerque, New Mexico

Follow-Up: Personal Computer Licensing
08-04-107F

FINAL

INTRODUCTION

The Office of Internal Audit and Investigations performed a follow-up of 04-107, Personal Computer Licensing, issued March 29, 2006. The purpose of our follow-up is to report on the progress made by the Chief Administrative Office (CAO), Department of Finance and Administrative Services (DFAS), and ABQ Ride's management in addressing our findings and recommendations.

Software is one of the most valuable technology assets to any business. Software is used every day by businesses, governments, schools, and consumers and many organizations that do not properly manage their software. Poor software management can cost an entity not only in terms of legal and financial risk but also in lost efficiency and productivity. When software is purchased, the buyer does not become the owner of the copyright. Instead, the buyer purchases the right to use the software under certain restrictions imposed by the licensing agreement.

Computer software is protected by U.S. copyright laws, U.S. code Title 17 and 18. The City could be held liable under both civil and criminal law for the misuse of the software agreement. A civil action could include the software owner immediately preventing the City from using the software and monetary damages. The software owner can choose between actual and statutory damages. Actual damages include the amount lost due to the infringement as well as any profits attributable to the infringement. Statutory damages can be as high as $150,000 per case. In addition, the government could criminally prosecute the City for copyright infringement. For software with a value of $2,500 and greater the conviction could include an additional fine up to $250,000 or five years in jail, or both.

SCOPE, OBJECTIVES, AND METHODOLOGY

Our follow-up procedures consist of interviews of City personnel and review and verification of applicable documentation to assess the status of our audit recommendations. Our follow-up is substantially less in scope than an audit. Our objective is to ensure management has taken meaningful and effective corrective action in regards to our findings and recommendations.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

The scope of the follow-up did not include an examination of all the functions and activities related to the CAO, DFAS, and ABQ Ride's personal computer licensing. We limited our scope to actions taken to address our audit recommendations from the date of our final report, March 29, 2006, through the end of fieldwork, August 12, 2008.

RECOMMENDATION NO. 1:

The Software Licensing Polices and Software Licensing Review Process and Guidelines (Software Licensing Policies and Guidelines) were written and published in July 1993. They had never been revised/reissued. The Software Code of Ethics was no longer included as part of the City's Code of Ethics.

OIAI tested the software applications on the desktop computers of 89 user names and determined the following:

- Seventy-six (85%) contained software that was not licensed.
- Eight (9%) had non-City approved instant messaging software.
- Eight (9%) had the same application loaded, but only one license was purchased.
- Six (7%) were accessed using a generic user id.
- Five (6%) contained personally owned software.
- Three (3%) had dial-up access via modems.
- Two (2%) had transferred applications that were not removed from the desktops in which they were initially loaded.
- One (1%) contained two remote access applications.

During the review of the software licensing logs the following items were noted:

- Five desktop computers had the same application loaded, but only one license was purchased.
- A software application loaded on 17 separate desktop computers, but only three licenses were located.

The City's Information Technology (IT) policy did not include consequences for employees who violated Software Licensing agreements.

OIAI recommended the CAO ensure that:

- All employees are aware of the City's policies.
- All employees should understand the seriousness of the consequences if the polices are violated.
- Disciplinary consequences for violations were included in the Software Code of Ethics.

The CAO agreed that the use of unlicensed software represented a risk to the City. The City had expended significant resources to bring the software licensing into compliance. However, the CAO respectfully disagreed with some of the specific findings noted:

- Of the 76 computers found to contain software that was not licensed, 53 of them had software that was not required to be licensed if it had been installed for use for 30-days or less. This particular software was not often needed by City users so the 30-day installation option is often used when needed. Because the test period for the audit was the month of June 2004, it seemed more likely than not that this finding of non-compliance was overstated.

  OIAI commented that the software license stated that one copy of the software could be used on one computer or workstation, for evaluation purposes without charge for a period of 21 days. The CAO should instruct City users to track their time when using the application in question.

- Of the six computers found to be accessible using a generic user id, all six were located in either a security environment or a 24/7 operation. Use of a generic id was permitted under these circumstances with approval from the Information Systems Committee (ISC) or the Technical Review Committee (TRC).

OIAI commented that according to the TRC no exceptions had been granted at that time.

- The use of dial-up modems was permitted with ISC and/or TRC approval for specific instances involving law enforcement or public safety application where it is desirable that the user not be identified as the City.

  OIAI commented that the dial-up modem in question was not approved by the ISC and/or the TRC. The modems were not involved with law enforcement or public safety applications.

The CAO noted that many of the findings were based on two documents, Software Licensing Policies and Guidelines, published in 1993. It appeared that these two documents were provided to OIAI by a long-term employee of DFAS' Information Systems Division (ISD) even though they had been out of circulation and common use for many years. In many cases the policies and guidelines promulgated in those documents were outdated, no longer best practices, or had been superseded by polices, standards and guidelines issued by the ISC. OIAI asked ISD and researched the IT Policies and Standards and did not find any policies, standards or guidelines that superseded either document.

In July 2005, the ISC adopted an Employee IT Security Certification Policy. This policy was to ensure that every employee who uses City IT assets was regularly informed of expectations concerning the safe and secure use of those assets. DFAS/ISD anticipated that initiation of the annual certification process would be completed by June 2006.

The CAO requested that the Human Resources Department (HRD) modify the New Employee Orientation (NEO) curriculum to include a section about the proper use of City IT assets, including software licensing compliance.

ACTION TAKEN

The audit recommendation has been partially implemented. New employees attending NEO are informed about the City's Software Licensing Policies and Guidelines, Software Code of Ethics and the consequences if violated. All new employees are required to attend NEO.

The CAO stated nothing has been implemented regarding the tracking of employees time spent using trial software during the evaluation stage.

RECOMMENDATION

The CAO should instruct City users to track their time when using a software program, during the evaluation stage, to ensure compliance with the licensing agreement.

RESPONSE FROM CAO

"The CAO concurs with recommendation. The new Software Licenses IT policy once approved by the Information Services Committee (ISC), will direct City employees to abide by all federal, state and local laws to ensure compliance with software licensing agreements."

RECOMMENDATION NO. 2:

The Software Licensing Policies and Guidelines had not been updated since July 1993. DFAS/ISD stated that they had not been updated because:

- They did not know that the Software Licensing Policies and Guidelines existed until OIAI brought it to their attention.
- There was a change in management in the mid 1990's.
- Other issues such as Y2K and Enterprise Resource Planning were considered a higher priority.

OIAI recommended that:

- The CAO ensure departments follow the Software Licensing Policies and Guidelines.
- DFAS/ISD review and update Software Licensing Policies and Guidelines regularly.
- DFAS/ISD make departments aware of changes and updates to the Software Licensing Policies and Guidelines.

The CAO and DFAS/ISD responded that it was the responsibility of the ISC to ensure that policies, standards, guidelines and procedures regarding the acquisition, implementation and use of all City IT assets are current and reflect best practices. DFAS/ISD was to hold monthly IT Users Group (ITUG) meetings. These meetings were to make departmental IT liaisons aware of changes in policies, standards, guidelines and procedures. DFAS/ISD was to post new or revised policies, standards, guidelines and procedures to the employee intranet by July 2006.

ACTION TAKEN

The audit recommendations have been partially implemented. DFAS stated that no specific policies pertaining to software licensing have been submitted to or approved by the ISC. The ITUG meetings were replaced in September 2006 with the monthly TRC meetings. Documentation of the TRC minutes are available for review on the City's website, which is available to everyone.

RECOMMENDATION

The CAO and DFAS/ISD should implement a Software Licensing Policy and Guideline which is updated regularly.

RESPONSE FROM CAO AND DFAS/ISD

"The CAO and DFAS/ISD concurs with recommendation. The Technical Review Committee (TRC) recently approved the new Software Licenses IT policy mentioned in the response to Recommendation No. 1. The new Software Licenses IT policy is pending approval from the ISC."

RECOMMENDATION NO. 3:

OIAI conducted interviews with 29 departments/divisions using a questionnaire to review:

- Control environment
- Software acquisition procedures
- Software installation and management
- Performance measures for software licensing

The interviews revealed the following:

- Twenty-four (83%) did not maintain a separate register listing of all software within the department/division.
- Twenty-two (76%) did not explain the City's Software Licensing Policies and Guidelines to new hires or transfers.
- Eighteen (62%) did not regularly educate their employees about software copyright compliance.
- Thirteen (45%) did not store software centrally within the department/division.

- Eight (28%) did not register software after the initial purchase.
- Six (21%) did not retain and file software license agreements.
- Six (21%) did not have a software manager.
- Four (14%) did not authorize or purchase software centrally within the department/division.
- Two (7%) did not analyze software licenses based on the expected use of the software.

OIAI recommended the CAO:

- Include a representative from ISD in the NEO process. The representative could discuss important IT issues, such as software licensing and the use of City computers.
- Develop a new Software Code of Ethics and set up an electronic annual certification process that employees are required to complete. New employees should be required to complete the electronic annual certification process prior to receiving access to City computer systems.

The CAO requested HRD modify the NEO curriculum to include a component on the proper use of City IT assets. DFAS/ISD anticipated implementation of an electronic annual certification process by June 2006.

ACTION TAKEN

The audit recommendation has been partially implemented.

NEO

The NEO curriculum contains the Software Code of Ethics; however, it is covered in approximately one minute. No other information regarding the City's IT policies are incorporated. A representative from ISD is not involved in the NEO.

Electronic Certification

DFAS/ISD stated that the annual electronic certification process was implemented in August 2006. There have been 5,114 certification tests taken as of June 19, 2008. A review of this list indicated that it was incomplete. DFAS/ISD stated that the query they run nightly is not capturing the full list of employees.

Since the list was incomplete, OIAI performed alternative sampling procedures. Test work was performed as of July 31, 2008 on OIAI's eight full time staff members.

Three employees (38%) had certifications that were expired. The IT Policy for Access Revocation states that when an employee is not in compliance with the City's Employee IT Security Certification Policy the individual's access shall be revoked until he/she successfully completes the certification or renewal process. None of the employees' access were revoked.

Two employees (25%) have been employed by the City for less than one year. DFAS/ISD interpretation of the Employee IT Security Certification policy was that new employees were not required to complete their first certification until one year from their hire date. However, the policy states that each City employee who applies for *new* or modified access shall complete the certification process within 30 days of the access request, and then annually within 30 days of the employee's anniversary date. DFAS/ISD has not required any new employees to complete the certification within the 30 day requirement.

One employee's (13%) name changed and was not included on the nightly update. The employee's certification was current but not included on the current list of certified employees.

Two employees (25%) were correctly included on the list as certified.

RECOMMENDATION

DFAS/ISD should ensure all employees are certified as required by the City's IT Security Certification Policy.

RESPONSE FROM DFAS

"DFAS concurs with recommendation. The City's IT Security Certification program has been functioning since its implementation in August 2006, except for a four month period when we were experiencing severe email problems. As a result of the inaccurate employee data extract discovered by Internal Audit, ISD is working to correct the Security Certification employee capture program that runs against the Empath system. These corrections are expected to be completed by October 2008 to ensure that all City employees are required to be annually certified."

RECOMMENDATION NO. 4:

The City-wide Software Licensing Coordinator position was eliminated during the budget cycle in Fiscal Year 1999. The Software Licensing Guidelines stated that ISD would assign a coordinator to provide guidance to departments when required. Without proper guidance, departments might have been less likely to follow and enforce software licensing guidelines. The risk of copyright infringement might have been greater and controls in place to protect the integrity of the City's computer environment from viruses may have decreased. OIAI recommended that DFAS reinstate the Software Licensing Coordinator position.

DFAS/ISD responded that rather than add another position, they were exploring different ways to exercise more control over the software licensing issue in the City. When computer equipment was replaced, ZenWorks was installed on each machine. This automated monitoring tool could be very effective in a non-centralized environment.

DFAS/ISD stated the City contracted the deployment of new computers to an outside vendor. This vendor:

- Accepted shipment of the computers
- Installed the software specified for each computer
- Delivered them to the departments, along with the applicable software license(s)

The vendor provided the City with a list of the equipment received and deployed. DFAS/ISD was to discuss alternative methods of controlling the software licenses and computer hardware delivered to the departments with the vendor.

ACTION TAKEN

The audit recommendation has not been implemented.

Control Over Software Licensing

In 2007, DFAS/ISD began the process to establish a Technical Support team, whose function would have been to help departments control the software used by City employees via ZenWorks and Microsoft's Active Directory. DFAS/ISD has not had the resources to set up and implement configuration settings that would help departments control software licensing.

ZenWorks

In 2004 DFAS/ISD began installing ZenWorks on all City personal computers. In 2007, DFAS/ISD was going to set up the ZenWorks configuration settings by having the Technical Support team track the software used by City employees and report licensing violations to the departments. Due to a lack of resources, DFAS/ISD could not set up and implement configuration settings that would help departments control software licensing.

ZenWorks provides an inventory of the software that is installed on computers under its control. This product does not track licenses. It was intended to be used as a reporting tool for departments to verify they had licenses for all the software found on their computers. It can prevent employees from installing software on ZenWorks-controlled machines, if the City decided to have DFAS/ISD implement that restriction. For example, while conducting test work for another finding, OIAI noted two employees at ABQ Ride who had personal software installed on their City issued computers. If this option in ZenWorks was enabled, the employees would have been prevented from installing the personal software.

Currently DFAS/ISD has not found an alternative solution to provide this support to the ZenWorks configuration settings implementation. Documentation is not available to address the effectiveness of the ZenWorks program for monitoring software.

Outside Vendor

DFAS stated that as of March 2008, the vendor that had been deploying new computers ceased operation in New Mexico. The DFAS Purchasing Division is currently working on establishing several contracts with vendors for the purchase, set up and repair of City personal computers.

DFAS/ISD discussed alternative methods of controlling software licenses and delivery of computer hardware with several vendors. DFAS/ISD stated the departments can purchase software using the purchasing card and do not have to go through one specific software vendor. DFAS/ISD stated that the responsibility to ensure licenses for all software should remain at the department level.

RECOMMENDATION

DFAS/ISD should create a process for departments to follow that will ensure compliance with software licenses. DFAS should consider updating ZenWorks so it can provide a listing to departments of software installed on City computers.

ABQ Ride should ensure that personal software is removed from City computers.

RESPONSE FROM DFAS

"DFAS/ISD concurs with recommendation. ISD is working with Internal Audit to develop a process for departments to track software license to ensure compliance. ISD will dedicate a person to work with the departments to implement the process. The target date for completion of the process and deployment of resource to work with department is November 2008. In addition to the tracking process, DFAS will explore the cost and capabilities of ZenWorks, as it relates to providing software licensing information at the department level.

"ISD will work with Transit IT staff to ensure personal software is removed from ABQ Ride City computers."

RECOMMENDATION NO. 5:

The Software Code of Ethics was no longer part of the Personnel Rules and Regulations (PRR). OIAI recommended the CAO ensure the Software Code of Ethics be included in the PRR.

The CAO responded that they would consult with the Director of HRD about the feasibility of amending Parts 301.15 *Automated Systems* and 902.1 *Reasons for Disciplinary Actions* of the PRR. The amendment would address software licensing compliance, with reference to the on-line policies, and possible disciplinary actions for violations.

ACTION TAKEN

The audit recommendation has not been implemented. The CAO stated that they did not amend the PRR to incorporate the Software Code of Ethics.

RECOMMENDATION

The CAO should ensure that the Software Code of Ethics is included in the PRR or the IT Policies and Procedures, as determined to be most appropriate.

RESPONSE FROM CAO

"The CAO concurs with recommendation. Ethical use of computers is addressed in PRR 301.15 and in combination with the IT policies and standards approved by the ISC, and will act as the "Software Code of Ethics."

RECOMMENDATION NO. 6:

The City did not have performance measures for monitoring software licensing. OIAI recommended:

- The CAO ensure that department management implement performance measures for monitoring software licensing.
- DFAS consider centralizing the monitoring of software licensing by placing DFAS/ISD in charge of the process.

The CAO responded that the issue of software licensing compliance was a City-wide issue, not a specific department issue. The CAO would attempt to include a performance measure in Fiscal Year 2007 Priority Objectives that reflected the City's commitment to fully comply with all software licensing provisions.

DFAS/ISD responded that they were installing ZenWorks on all new and replacement computers. This program would help control the installation of unauthorized software by users. Because the IT replacement schedule is directly impacted by available funding, DFAS/ISD was unable to project a date when all City IT equipment would be equipped.

ACTION TAKEN

The audit recommendations have not been implemented. The CAO did not implement performance measures that specifically address software licensing. ZenWorks has been installed on 2,175 out of approximately 5,300 (41%) computers. DFAS stated that ZenWorks can not be installed on any computers that are assigned to the Enterprise Funds due to

network constraints. There are approximately 500 computers assigned to the Enterprise Funds.

DFAS/ISD stated that they were not responsible for all City licenses, nor would they be able to track licenses due to the way software is purchased throughout the City. DFAS/ISD stated they could provide regular reports to departments that detail what software was loaded on the computers under the control of ZenWorks. However, the reports are not currently utilized.

RECOMMENDATION

The CAO should implement performance measures that specifically address software licensing.

DFAS/ISD should develop a process for departments to track software licenses installed on City computers.

RESPONSE FROM CAO

"The CAO does not concur with recommendations. In order to have an effective performance measure you must have data about the process that tracks software licenses. When this process is in place, we will be able to report generally about exceptions to the process and the timeframe to correct the exceptions. Until this process in is place performance measurement is not possible."

RESPONSE FROM DFAS/ISD

"DFAS/ISD concurs with recommendation. ISD is working with Internal Audit to develop a process for departments to track software licenses installed on City computers. ISD will then dedicate a person to work with the departments to implement this process."

RECOMMENDATION NO. 7:

Five workstations at ABQ Ride were identified that contained remote access software. This software was used to access the Department's computer systems from a remote site. OIAI recommended that ABQ Ride comply with the Network Access/Connectivity policy and consider using a Virtual Private Network (VPN) connection as an alternative for remote access connectivity.

ABQ Ride responded that they would work with DFAS/ISD to convert all remote access to VPN by April 30, 2006.

ACTION TAKEN

The audit recommendation has been partially implemented. ABQ Ride currently has 14 employees who have been authorized to have VPN access. Six of 14 (43%) employees did not have the VPN software program loaded on their computer. None of the 14 computers had the remote access software previously identified.

RECOMMENDATION

ABQ Ride should review employees VPN accounts to determine if access is still required.

RESPONSE FROM ABQ RIDE

"Transit concurs with recommendation. The security of the City's assets and computing environment is not taken lightly. To rectify the situation, ABQ-Ride's I.T. Manager, will contact the six employees that currently have VPN access, but have not installed/activated the software to determine if the access is still needed. This action shall be done by close of business September 15, 2008. A listing of all employees with VPN access will be reviewed with Senior Management at least annually.

"In the future, all VPN access requests and justification is to go through the IT Manager or designee. Records of each request will be maintained. In addition, we will require a justification from employees currently using VPN to be on record."

CONCLUSION

The CAO, DFAS/ISD and ABQ Ride have partially implemented four of the recommendations noted in the initial audit. Three items have not been implemented. The CAO should implement Software Licensing Policies and Guidelines and ensure employees are aware of their responsibilities. DFAS should ensure all employees are up to date on their IT Security Certification.

OIAI will request a report of progress made as of November 30, 2008, from the CAO and DFAS. A second follow-up will be performed within one year.

We appreciate the assistance and cooperation of the CAO, DFAS/ISD, and ABQ Ride personnel during the audit.

Principal Auditor

REVIEWED:

Audit Manager

Internal Auditor

APPROVED:

Carmen Kavelman, CPA, CISA, CGAP
Director
Office of Internal Audit & Investigations

APPROVED FOR PUBLICATION**:**

Chairperson, Accountability in Government
Oversight Committee