SECOND FOLLOW-UP OF

MANAGEMENT AUDIT

PERSONAL COMPUTER LICENSING

CITYWIDE

REPORT NO. 10-04-107F2

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

June 30, 2010

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

Follow-Up: Personal Computer Licensing - Citywide
10-04-107F2

FINAL

INTRODUCTION

The Office of Internal Audit and Investigations (OIAI) performed a second follow-up of Audit Report No. 04-107, Personal Computer (PC) Licensing, which was issued March 29, 2006. OIAI issued the first follow-up report on September 24, 2008.

The initial audit had seven recommendations. The first follow-up determined that:

- Three recommendations were partially implemented by the Chief Administrative Officer (CAO) and the Department of Finance and Administrative Services' Information Systems Division (DFAS/ISD).
- Three recommendations had not been implemented by the CAO and/or DFAS/ISD.
- One recommendation was partially implemented by the Transit Department (Transit).

In March 2009, the CAO and the DFAS Director provided a status report of progress made on the recommendations in the first follow-up.

The purpose of the second follow-up is to report on the progress made by the City in addressing our findings and recommendations.

Background Information of Audit No. 04-107

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.

Additional background information has been omitted due to its sensitive nature.

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 PC Licensing. We limited our scope to actions taken to address our audit recommendations from the date of our first follow-up report, September 24, 2008 through May 24, 2010.

RECOMMENDATIONS NO. 1, NO. 2, and NO. 5

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.

DFAS/ISD stated that they had not updated the policies and guidelines because:

- 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.
- They did not know that the policies and guidelines existed until OIAI brought the issue of software licensing to their attention.

OIAI tested the software applications on the desktop computers of 89 user names and identified several significant issues.

OIAI recommended the CAO ensure that:

- The Software Code of Ethics is included in the Personnel Rules and Regulations or the IT Policies and Procedures, as determined to be most appropriate.
- All employees are aware of and follow the City's Software Licensing Policies and Guidelines.
- All employees understand the seriousness of the consequences if the polices are violated.
- Disciplinary consequences for violations are included in the Software Code of Ethics.

OIAI recommended the DFAS/ISD ensure that:

- Software Licensing Policies and Guidelines are reviewed and updated regularly and departments are aware of the changes and updates.

ACTION TAKEN

The audit recommendations were partially implemented. Employees attending New Employee Orientation (NEO) were informed about the City's Software Licensing Policies and Guidelines, Software Code of Ethics and the consequences if violated. All new employees were required to attend NEO.

The draft of a new Software Licenses Information Technology (IT) policy was approved by the City's Technology Review Committee (TRC) in August 2008, and requires that City employees or personnel working on the City's behalf:

- May use software only in accordance with vendor license agreements.
- Must not knowingly violate license agreements and/or requirements (e.g., City employees must follow the vendor requirements when using software during the evaluation stage).

However, DFAS/ISD informed OIAI that the draft has not been finalized, because it has not yet been approved by the ISC. According to DFAS/ISD:

- The ISC's review and approval of policies was suspended by the previous administration.
- The policy is expected to be reviewed by the ISC as soon as new committee members are appointed by the Mayor and a meeting is held.

RECOMMENDATION

DFAS/ISD should ensure the new Software Licenses IT policy is submitted to the ISC for final approval.

RESPONSE FROM DFAS

"DFAS/ISD agrees with this recommendation, and the new policy will be scheduled for ISC review at the July 2010 meeting."

RECOMMENDATION NO. 3

OIAI conducted interviews with 29 departments/divisions using a questionnaire, and identified several significant issues regarding control environment, software acquisition, installation and management, and performance measures.

OIAI recommended the CAO:

- Include a representative from DFAS/ISD in the NEO process. The representative could discuss important IT issues, such as software licensing and the use of City computers.
- 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.

ACTION TAKEN

The recommendation has been partially implemented.

The NEO curriculum included a discussion of the Software Code of Ethics; however, it was covered in approximately one minute. No other information regarding the City's IT policies were incorporated. A representative from DFAS/ISD was not involved in the NEO.

DFAS/ISD stated that it had implemented a process to ensure all active City employees are scheduled for annual IT security certification.

OIAI requested DFAS/ISD to provide a list of all active City employees and their most recent IT Security Certification dates. The list provided on March 3, 2010 indicated 562 employees were overdue on their annual IT Security Certifications because they were approximately three months past the test due date. As of March 10, 2010 none of these employees' access to City IT assets had been revoked. DFAS/ISD management informed OIAI that prior to revoking access, the employees are sent a courtesy e-mail, informing them that their access will be revoked. This is a manual process, and the responsible DFAS/ISD employee is behind in sending out the e-mails. The Chief Information Officer (CIO), consequently, had not received a report showing the employees who were past due in renewing their credentials. According to the City's Employee IT Security Certification policy:

- An employee who does not complete initial certification or subsequent annual renewal within the specified time period shall have his/her credentials to access City IT assets revoked.
- The revocation will be done by the CIO or his designee, in accordance with the City's Access Revocation Policy, until such time as the employee successfully completes the certification or renewal process.

As of May 4, 2010, DFAS/ISD informed OIAI that:

- 112 employees had overdue IT Security Certifications.
- 23 employees' access to City IT assets had been revoked.

OIAI met with DFAS/ISD to gain an understanding of the IT Security Certification process and determined the following:

- Employees take a ten question security test to determine if they are familiar with security policies and guidelines.

- Due to staffing shortages, one DFAS/ISD employee monitors City employee compliance with the IT Security Certification process.
- The monitoring process is manual and includes maintaining records and individually contacting employees who are out of compliance.
- The employee is currently spending approximately 50% of her time on the process, but it is currently not up-to-date.
- The City is required to have an IT Security Certification process by the Payment Card Industry Data Security Standards (PCI/DSS), which mandate that stored credit card data is protected by encryption. The PCI/DSS, a set of comprehensive requirements for enhancing payment account data security, was developed to help facilitate the broad adoption of consistent data security measures on a global basis.
- DFAS/ISD has not surveyed other entities to identify what IT Security Certification processes they have in place.

RECOMMENDATION

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

DFAS/ISD should consider surveying other entities, and determine if revisions to City's IT Employee Security Certification Policy are appropriate.

RESPONSE FROM DFAS

"DFAS/ISD agrees that the entire certification policy and process needs to be reviewed. The current method of ensuring City employees are aware of IT policies uses valuable technical resources to accomplish clerical tasks. Consequently, starting in the next two months, DFAS/ISD will perform an analysis of the training requirements, document alternative methods of achieving the necessary training goals, identify appropriate parties responsible for the training and identify the changes needed to current policies."

RECOMMENDATION NO. 4

The Citywide Software Licensing Coordinator position was eliminated during the budget cycle in fiscal year (FY) 99. The policy at that time stated that DFAS/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 protection from viruses may have decreased.

OIAI recommended that DFAS/ISD 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.

During the first follow-up, OIAI noted two employees at Transit who had personal software installed on their City issued computers. OIAI recommended that Transit ensure that personal software is removed from City computers.

ACTION TAKEN

A. DFAS/ISD

The recommendation to DFAS/ISD has been partially implemented. DFAS/ISD has taken the approach that it is each department's responsibility to ensure its employees are following City policies, as well as state and federal laws relating to software licensing. DFAS/ISD dedicated an employee for a seven month period beginning in October 2008 to train representatives from each department to collect software inventories from each PC. Each representative was provided and taught how to use the free software (freeware) to collect the software inventory. Upon completing this process, each department was required to provide a letter to DFAS/ISD stating the inventories were successfully completed. DFAS/ISD provided OIAI letters from five departments that successfully completed the software inventory collection process.

OIAI selected a sample of seven departments, including one of the five mentioned above, to determine if the departments had performed a software inventory of their PCs, and concluded that:

- Four departments (57%) did not perform a software inventory.
- Three departments (43%) performed a software inventory.

The DFAS/ISD records indicated that the most recent status regarding these four departments that did not complete the software inventory projects was that they were "in progress". According to the management of one of the departments, the DFAS/ISD representative contacted one of their employees by telephone, but never met with the employee to provide the freeware.

An employee of another department said that the DFAS/ISD representative had met with her and provided her with the freeware. She had contacted the DFAS/ISD representative and explained that she had not been able to run the freeware on a PC. She subsequently received an e-mail from the DFAS/ISD representative in which he stated that there was no hurry, because the full software inventory had been finished.

According to management of the third department, they did not complete the software inventory since the previous director believed that it was not his staff's responsibility to monitor software.

The fourth department said that they do not have enough personnel to regularly audit the software on their desktops.

The DFAS/ISD representative who was dedicated to this project is no longer employed by the City.

B. Transit

The recommendation has been fully implemented. Transit implemented the following process to ensure that personal software is removed from City computers:

- All users were instructed to remove personal software from their computers.
- Most computers in Transit are configured for the specific user, with user rights limited to disallow installation of any software program on the PC without the Administrative username and password known only to IT staff.
- Without Administrative access, Transit users are unable to install software on their computers.
- Only the IT staff can install software, and it is the policy of the Transit IT Division to install only that software which has been approved for City use and licensed to that user.

OIAI selected a sample of five Transit PCs and used the DFAS/ISD supplied freeware to obtain a listing of all software loaded on these PCs. None of the five PCs tested contained personal software.

RECOMMENDATION

The CAO should:

- Ensure that departments are aware that it is their responsibility to track their software inventory, and ensure that the software on their PCs is licensed.
- Determine the status of each department's software inventory.

Based on the status of the departments' software inventory, DFAS/ISD should consider communicating the software inventory process to the department representatives at a TRC meeting. This could help ensure that everyone is aware of the process and the deadlines and be instructed on how to use the freeware application.

RESPONSE FROM DFAS

"The CAO agrees with this recommendation and will make it clear in writing by the end of July 2010 to departments that it is their responsibility to ensure all IT policies and standards are followed. Additionally, departments will be instructed to conduct a PC software inventory as a means of ensuring that all software installed on City computers is properly licensed. DFAS will track whether or not departments have completed their PC software inventories.

"Based on the status of the department's software inventory, DFAS/ISD should consider communicating the software inventory process to the department representatives at a TRC meeting. This could help ensure that everyone is aware of the process and the deadlines and be instructed on how to use the freeware application."

"By the end of July 2010, DFAS/ISD will develop a new procedure that will provide instructions on how to produce a PC software inventory using a freeware application. This procedure will be provided on the City's employee website. ISD will make a presentation to the TRC members concerning the inventory process and where to find the new procedure."

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 FY 2007 Priority Objectives that reflected the City's commitment to fully comply with all software licensing provisions.

ACTION TAKEN

The recommendation to the CAO regarding performance measures is resolved. Performance measures provide information regarding an entity's efficiency and effectiveness. It does not appear to be appropriate to implement performance measures that specifically address software licensing at the department level, unless this area is significant to its operations.

The recommendation to DFAS/ISD regarding software licensing is discussed in Recommendation No. 4.

RECOMMENDATION NO. 7

Five workstations were identified that contained remote access software, during OIAI's review of software licenses at Transit. This software was used by Transit personnel to access the department's computer systems from a remote site. The Transit IT representative was not aware of the City's IT Network Access/Connectivity policy. This policy stated no remote connectivity software (i.e. PC Anywhere, Procomm, etc.) would be used to connect to the City's network in any way unless approved in advance and then registered with the TRC.

OIAI recommended that Transit comply with the IT Network Access/Connectivity policy, and consider using a Virtual Private Network (VPN) connection as an alternative for remote access connectivity.

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

ACTION TAKEN

The recommendation has been partially implemented. Transit informed OIAI that it had implemented the following procedures relating to the granting, reviewing and terminating VPN access:

- A request for VPN access must be filed with the Transit IT Division (Transit IT). That request must be initiated by the division manager or the director, and specify the justification for VPN access.
- Transit IT records the request on a spreadsheet, and notifies DFAS/ISD's Networking Section that a VPN account needs to be established.
- Once the VPN account is established, Transit IT installs the VPN software on the user's computer.

- Upon termination of the employee or expiration of the justification, Transit IT notifies DFAS/ISD's Networking Division to terminate the VPN account.
- Transit IT reviews VPN access accounts with the division managers annually to ensure that all justifications for access are still valid. Those that are not, are terminated.

As of April 30, 2010, Transit had 11 employees with VPN access and one whose access had been terminated. OIAI requested that Transit provide documentation to show that it was complying with its procedures for granting, reviewing and terminating VPN access. Transit did not maintain documentation for:

- Eleven of 11 employees (100%), to show that the Transit IT Division reviewed the VPN access account with the division managers during the last 12 months.
- Six of 11 employees (55%), who were granted VPN access.
- The one employee whose access was terminated.

RECOMMENDATION

Transit should document adherence to its procedures relating to the granting, reviewing and terminating VPN access.

RESPONSE FROM TRANSIT

"The Transit Department agrees that it will document its adherence to procedures relating to the granting, reviewing, and terminating of VPN access. It will do so in the following manner:

"1. The Transit Department procedures listing in the "ACTION TAKEN" section will be formalized as a "Department Instruction". This will occur no later than June 30, 2010.

"2. The documentation forms will be developed and put in use no later than July 16, 2010."

"3. "The documentation forms will be reviewed by Transit Department staff on a semi-annual basis."

CONCLUSION

Six of seven recommendations noted in the first follow-up audit report have been partially implemented. A portion of one of these recommendations to Transit was fully implemented. One of seven recommendations was resolved. DFAS/ISD and the CAO should strengthen the controls over software licensing by implementing the recommendations noted above. Transit should adhere to its procedures relating to VPN access.

We appreciate the assistance and cooperation of City personnel during the follow-up.

_____
Principal Auditor/Investigator

REVIEWED:

_____ _____
Senior Information Systems Auditor Internal Auditor

APPROVED: APPROVED FOR PUBLICATION**:**

_____ _____
Carmen Kavelman, CPA, CISA, CGAP Chairperson, Accountability in Government
Director Oversight Committee
Office of Internal Audit & Investigations