Audit Follow-Up

Actions Due As of September 30, 2013

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Active Directory

(Report #1210 issued June 19, 2012)

Report #1413 **February 27, 2014**

Summary

Information Systems Services (ISS) completed seven of the 20 action plan steps established to address issues identified in our audit of Active Directory that were due for completion as of September 30, 2013.

In audit report #1210, we noted current City policies governing the City's Active Directory were adequate and, for the most part, password controls were in place. We however noted risks, which if realized, have the potential to negatively impact City operations. Thirty–one action plan steps were developed to address those risks.

During this follow-up period 20 of those 31 action plan steps addressing the following areas of concern were due for completion.

- Compliance with Administrative Policy/Procedure 809 "Information Systems Security." Specifically:
  - The separation of development and testing activities (two steps).
  - Ensuring that third parties accessing the City's computer network acknowledge they must comply with applicable City policies to be granted access to the City's computer network (two steps).
- The ability to retrieve network authorization documentation when needed (three steps).
- Ensuring system and application acquisitions are properly reviewed and approved; existing computer systems are periodically reviewed for effectiveness; and the purpose, goals, policies, and objectives of ISS are reviewed by the ISS Steering Committee (four steps).
- Ensuring inactive user accounts are deactivated in a timely manner (three steps).
- Ensuring user accounts are not shared by multiple individuals when practical (four steps).
- Ensuring activity logs are generated, reviewed, and retained as appropriate (two steps).

Of those 20 action plan steps, management completed seven and amended the completion date for the remaining 13. Actions completed during this follow-up period include:

- Evaluating and accepting the risks associated with testing and development activities being conducted in the same computer network domain (two steps).
- Reactivation of the ISS Steering Committee and its involvement in IT decisions that impact the City (three steps).
- Generating logs of Active Directory activity for monitoring purposes (two steps).

The 13 action plan steps that were due but not completed and for which the completion dates were amended related to:

- Helping ensure network access authorization documentation can be retrieved when needed (three steps).

- Helping ensure third parties accessing the City's network comply with applicable City policies and procedures (two steps).
- Assessing risks related to systems operating outside ISS's support and control structure (one step).
- Helping ensure user accounts that have not been used within a reasonable time period are deactivated (three steps).
- Helping ensure user accounts are not shared by multiple individuals when practicable (four steps).

We appreciate the cooperation and assistance provided by staff in Information System Services during this audit follow-up.

Scope, Objectives, and Methodology

We conducted this audit follow-up in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. Those standards require we plan and perform the audit follow-up to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit follow-up objectives.

Original Report #1210

The overall objective of our original audit (report #1210) was to review the Active Directory that is used to manage the City's network. Specific objectives included addressing the following questions: (1) are there adequate policies and procedures in place to effectively manage and secure the City's Active Directory, and do those policies and procedures incorporate industry best practices; (2) are the policies and procedures in place being followed; (3) is the design of the City's Active Directory implementation reasonable from a security and administrative perspective; (4) are Active Directory user accounts adequately managed; (5) are domain controllers that run Active Directory managed properly; (6) are computer generated activity logs of network activity involving Active Directory generated, reviewed and retained?

Overall, we concluded the policies, implementation and management of Active Directory, as a whole, were appropriate and provided adequate security relating to the City's network. We did however identify areas, which if addressed, would increase the security of the City's network. Those areas included:

- Increasing policy compliance by deactivating user accounts that have not been used in the last 90 days.
- Eliminating the sharing of user accounts.
- Enforcing password controls such as requiring periodic changing of passwords.
- Ensuring that requests for changes in user network permissions are recorded and retained in a manner that allows their retrieval when needed.
- Adding a fourth domain to the City's network which should enhance productivity and security.
- Installing updates on domain controllers in a timely manner to enhance security of the City's network.
- Generating, reviewing, and retaining logs of network activity to provide important information in the event network security is compromised.

Previous Conditions and Current Status

In report #1210, we provided recommendations to management regarding areas that need to be addressed in ISS relating to the City's Active Directory. Management's Action Plan consisted of 31 action plan steps, with 20 being due as of September 30, 2013. Of the 20 steps due this period, seven steps were completed and 13 were not completed. Table 1 below shows the 20 steps due for completion and their status as determined by our follow-up.

Table 1
Action Plan Steps from Audit Report #1210
Due as of September 30, 2013, and Current Status

Action Plan Steps Due as of September 30, 2013	Current Status
To comply with APP 809 regarding the separation of development and testing environments	
• Evaluate the importance of establishing a fourth domain in the City's Active Directory taking cost into consideration as well as the risks posed by the current combining of the testing and development activities in the same domain and the non-compliance with APP 809.	✓ Management considered the risks associated with having testing and development activities occurring in the same network domain, as well as the costs associated with setting up a new domain to allow for the separation of testing and development activities. Management determined that the costs associated with setting up a new domain outweighed the risks associated with combining development and testing activities. Accordingly, management has accepted the following risks: – Disruption of development activities due to testing of updates/patches occurring in the same network domain as development activities. – Updates and/or patches not installed in a timely manner (due to delays in testing of updates/patches) potentially leading to a disruption of the City's network.
• Take appropriate actions based on the evaluation conducted in the preceding step above and document the decisions made.	✓ No action is required as management decided to not establish another domain to allow for the separation of testing and development activities (see previous action plan step).
To help ensure network authorizations documented and can be retrieved when needed	
• A job code will be added to the BOSS system for changes in user account permissions.	○ Management changed the approach to address the issue of not being able to retrieve support for changes in network authorizations. The new plan is to use the City's SharePoint application as the mechanism for requesting and documenting changes to user network access authorization rather than the BOSS system. The completion date for this action plan step has been amended to 9/30/2014.
• Training on how changes to user account access permissions will be provided to BOSS users for the new code established in the previous action plan step above.	○ Management indicated users will be trained on the use of SharePoint for making and documenting network access requests once the SharePoint system has been developed. As with the previous action plan step, the completion date has been amended to 9/30/2014.

• When requests for changes to user account permissions are not completed properly in the BOSS system, they will either be corrected by ISS personnel or sent back to the requestor for correction prior to the implementation of the user account permission changes.	○ Due to the change in the approach to address the issue of not being able to retrieve network authorization change documentation (as described in the first action plan step in this section), this step has not yet been implemented. As with the previous action plan steps, the completion date has been amended to 9/30/2014.
To comply with APP 809 and help ensure third parties granted access to the City's network understand and comply with City policies and procedures related to computers and networks	
• A third party compliance statement will be developed. That statement will be developed such that it will serve as acknowledgement, by the party completing it, that they understand and will comply with City computer and network policies.	○ Management has made plans for implementing a new procedure that will require third parties to sign a statement attesting to the fact they agree to follow all applicable City policies and procedures prior to being allowed to access the City's computer network. Management has amended the completion date for this action plan step to 3/31/2014.
• New user accounts for third parties will not be created without a completed compliance statement.	○ As noted in the preceding action plan step, management has developed plans for requiring statements of compliance from third parties; however, those plans have not yet been completed. Management has amended the completion date for this action plan step to 3/31/2014.
To ensure system and application acquisitions are properly reviewed and approved; existing computer systems are periodically reviewed for effectiveness; the purpose, goals, policies, and objective of ISS are reviewed by the ISS Steering Committee	
• The ISS Steering Committee will be reactivated and meet on a quarterly basis.	✓ The ISS Steering Committee has been reactivated and has met several times since the initial audit report was issued (i.e., in December 2012, May 2013, October 2013, and November 2013). Those meetings were scheduled and held as needed to address pertinent information technology issues. This step is considered complete.
• The ISS Steering Committee will be informed of City activities which impact ISS or relate to information technology type system acquisitions.	✓ In the meetings noted in the previous action plan step, the ISS Steering Committee (committee) has been informed of and discussed multiple activities impacting information technology within the City. The committee has also been updated on the status and progress of ongoing information technology projects. This step is considered complete.
• Guidance and approval will be sought from the ISS Steering Committee as needed for City information technology related activities.	✓ In the meetings and communications noted above, the ISS Steering Committee has provided direction and approval in several areas, including for example: – Acquisition and implementation of a new citywide time and attendance application. – Implementation of a virtual private network to

	further secure the City's network. – Upgrade to the City's document imaging and retention system. Accordingly, this step is considered complete. *(Note: The ISS Steering Committee has also recommended establishment of a technical subcommittee to assist in review and making recommendations in regard to specific information technology issues and applications. To date, neither the subcommittee nor its roles have been established. Recommendation: We recommend necessary actions be taken to finalize decisions regarding establishment of a technical subcommittee to assist the ISS Steering Committee in its overall role.)*
• The ISS Steering Committee will assess risks related to systems operating outside ISS's support and control structure.	♦ ISS management indicated that, to date, no new systems or applications have been identified that are operating outside ISS's support and structure. However, ISS staff have determined one City department (Underground Utilities) is in the early phases of implementing an application as a pilot project that potentially could be of interest to and/or used by other City departments. Prior to the acquisition of the application for full implementation by Underground Utilities, the matter should be brought before the ISS Steering Committee for consideration of citywide usage and, if applicable, acquisition of the application with an enterprise license rather than individual user licenses. Until resolution of this item, this action plan step will be considered in progress.
To help ensure user accounts that have not been used within a reasonable time period are deactivated	
• The inactive user accounts identified in the audit will be reviewed and considered for deactivation as applicable.	○ Subsequent to the initial audit, ISS management determined the expiration of passwords every 45 days serves as a compensating control that effectively disables user accounts after 45 days if the account has not had any activity. Accordingly, ISS management did not deactivate the identified inactive user accounts. We concur with management's assertion that password expiration serves a compensating control to help ensure inactive user accounts are not accessed by unauthorized individuals. However, there are ways in which that compensating control can be circumvented. Therefore, it is still important that inactive user accounts be disabled within Active Directory. In our discussions during the follow-up engagement, ISS management

	acknowledged these circumstances. As a result ISS management amended the completion date for this action plan step to 3/31/2014.
• Quarterly a query will be made of all Active Directory user accounts which will identify all accounts that have not been utilized in the last 90 days.	○ To date quarterly queries intended to identify inactive user accounts have not been generated. This lack of action was attributed to management's subsequent determination that password expiration served as an adequate compensating control to ensure inactive accounts are not improperly accessed. However, as described in the previous action plan step, this issue is again under consideration. Accordingly, the completion date for this action plan step has been amended to 3/31/2014.
• The user accounts identified in the preceding action plan step will be reviewed and deactivated as deemed appropriate by ISS.	○ For the reasons stated in the two previous action plan steps, no action has been taken. As with the two previous action plan steps, the completion date for this action plan step has been amended to 3/31/2014.
To help ensure user accounts are not shared by multiple individuals	
• User accounts in Active Directory will be reviewed for the purpose of identifying shared accounts. Shared accounts are those not assigned to a specific individual or computer service (i.e., "service accounts").	♦ In connection with another issue, ISS management reviewed all user accounts and identified those accounts with passwords set to never expire. Many of the identified accounts represented "shared accounts." (Shared accounts established by the City generally have their passwords set to never expire.) ISS management sent out an e-mail in September 2013, to key technology staff within the various City departments and offices, that listed those identified accounts. In that e-mail, the key technology staff was requested to provide information on those accounts. Among other things, that information was to be used to determine if the applicable accounts should be continued as shared accounts. ISS indicated that as of the end of our follow-up fieldwork in January 2014, no usable information has been received in response to that e-mail request and no follow-up efforts have been made. Also, ISS indicated that efforts have not been made to identify any other shared accounts (i.e., those with passwords set to never expire). ISS management acknowledged that further efforts and follow up are needed. This action plan step is considered in progress and the completion date for this action plan step has been amended to 9/30/2014.
• ISS will review the user accounts identified in the previous step and obtain written justification from the applicable City departments as to the reasons	♦ As noted above in the previous action plan step, ISS has made some efforts to obtain information as to the justification for existing shared accounts. However, those efforts are not comprehensive or

these accounts should continue to be used.	complete. As such we will consider this action plan step in progress with an amended completion date of 9/30/2014.
• ISS will review and retain the justifications provided by the City departments.	♦ As noted in the two previous action plan steps, justifications for sharing of accounts have not yet been obtained. This action plan step will be considered in progress with an amended completion date of 9/30/2014.
• When, in ISS's judgment, the justification for the sharing of user accounts does not outweigh the risks posed by the sharing of accounts ISS will disable the shared account. When the justification for sharing the user account does outweigh the associated risks no action will be taken.	♦ As noted in the previous action plan step, justifications for sharing of accounts have not been obtained. Accordingly, information has not yet been obtained to allow ISS to complete this action plan step. This action plan step will be considered in progress with an amended completion date of 9/30/2014.
To ensure activity logs are generated, reviewed and retained as appropriate	
• Evaluate and consider the risks posed by not generating or retaining logs of the activity in Active Directory.	✓ ISS management reviewed the risks associated with not generating and retaining logs of computer network activity. This action plan step is considered complete.
• Take appropriate actions based on the evaluation conducted pursuant to the previous step and document the decisions made.	✓ After reviewing the risks associated with not generating and retaining logs of computer network activity, management began a process of generating and retaining application, security, and system logs to the extent that City resources allow (i.e., the logs are overwritten on a periodic basis as resources are used up). While not monitored on a periodic basis, those logs are available to allow ISS management the opportunity to review historical activity as needed (i.e., until overwritten). This action plan step is considered complete.

Table Legend:

- • Issue to be addressed from the original audit.
- ♦ Actions initiated but not yet completed.
- ✓ Issue addressed and resolved.
- ○ Issue remains under consideration and not yet completed, completion date amended.

Conclusion

Table 1 above shows ISS successfully completed and resolved seven of the 20 action plan steps established to address issues identified in audit report #1210. Completed actions involved:

- Evaluating and accepting the risks associated with testing and development activities being conducted in the same computer network domain (two steps).
- Reactivation of the ISS Steering Committee and its involvement in IT decisions that impact the City (three steps).
- Generating and retaining logs of computer active directory activity for review and analysis on an as needed basis (two steps).

Additionally, Table 1 shows the 13 action plan steps due for completion this follow-up period that have not been completed. Those action plan steps include:

- Helping ensure network access authorization documentation can be retrieved when needed (three steps).
- Helping ensure third parties accessing the City's network comply with applicable City policies and procedures (two steps).
- Assessing risks related to systems operating outside ISS's support and control structure (one step).
- Helping ensure user accounts that have not been used within a reasonable time period are deactivated (three steps).
- Helping ensure user accounts are not shared by multiple individuals when practical (four steps).

Remaining actions due to be completed in future periods include:

- Removing network access from third parties in a timely manner when it is no longer needed (three steps).
- Helping ensure risks relating to the City Active Directory and network are periodically and formally evaluated (two steps).
- Helping ensure password policies are not overridden so as to reduce the risk that user accounts are compromised (four steps).
- Helping ensure operating system updates are installed on domain controllers in a timely manner (two steps).

We appreciate the cooperation and assistance provided by staff in ISS during this audit follow-up.

Appointed Official's Response

City Manager:

I appreciate the work done by the City Auditor on the Active Directory follow-up report. Staff continues to make progress toward completing the action item steps and evaluating the recommendations contained in the original audit. I am confident that all action items and recommendations will be addressed by their respective follow-up date. I would like to thank the City Auditor and DMA/ISS for their efforts in this audit.

Copies of this audit follow-up #1413 or audit report #1210 may be obtained from the City Auditor's website (http://talgov.com/auditing) or via request by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (Office of the City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

Audit follow-up conducted by:
Dennis R. Sutton, CPA, CIA, Sr. IT Auditor
T. Bert Fletcher, CPA, CGMA, City Auditor