Audit Follow-Up

Status As of
February 28, 2015

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Active Directory

(Report #1210 issued June 19, 2012)

Report #1508 **April 20, 2015**

Summary

This is the second follow up on the Audit of Active Directory (report #1210 issued June 19, 2012). Thirty-one action plan steps were established to address issues identified in the audit, with each step due for completion by September 30, 2014. As of February 28, 2015, seventeen (55%) of the 31 action plan steps have been completed. Ten of those 17 action steps were completed during this follow-up period, while seven action plan steps were completed in the previous follow-up period. Actions are on-going to complete the 14 remaining steps.

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. However, we noted risks, which if realized, have the potential to negatively impact City operations. Thirty-one action plan steps were developed to address those risks, of which 24 were due for completion during this audit follow-up period.

Ten of the 24 action plan steps were completed during this follow-up period. Those completed steps include:

- Develop a third party compliance statement to serve as acknowledgement third party users understand and comply with the City's computer and network policies, and remove third party access in a timely manner when it is no longer needed (five steps).
- Ensure inactive accounts are deactivated, when applicable and appropriate (three steps).
- Identify user accounts with password controls that have been overridden (one step).
- Identify updates and patches to the operating systems of the domain controllers that are published by Microsoft on a monthly basis (one step).

The remaining 14 steps for which actions have been initiated, but not completed relate to:

- Ensuring network authorizations are documented and can be retrieved when needed (three steps).
- Conducting a formal risk assessment of the City's network (two steps).
- Assessing risks related to systems operating outside ISS's support and control (one step).
- Identifying and eliminating shared accounts, unless there is appropriate justification documented for keeping an account as a shared account (four steps).
- Obtaining appropriate justification to keep accounts with password controls that have been overridden, otherwise set the account so appropriate password controls are followed (three steps).
- Installing updates and patches to the domain controllers in a timelier manner (one step).

We recognize ISS has completed 17 of the 31 (55%) action plan steps established to address concerns raised in the Audit of Active Directory, yet almost half of the action steps still remain unfinished nearly three years after the initial audit report was released. Because many of the remaining steps are time consuming and reliant upon other City departments responding to requests from ISS, we encourage ISS management to contact

department directors and/or other leadership members for those departments and/or commit additional resources, if necessary, to resolve the remaining 14 steps in the near future.

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 and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our follow-up audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our follow-up audit objectives.

Original Report #1210

The overall objective of our original audit (report #1210) was to review the Active Directory 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; and (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:

- Increase policy compliance by deactivating user accounts that have not been used in the last 90 days.
- Eliminate the sharing of user accounts.
- Enforce password controls such as requiring periodic changing of passwords.
- Add a fourth domain to the City's network which should enhance productivity and security.
- Install updates on domain controllers in a timely manner to enhance security of the City's network.
- Conduct formal risk assessments to help ensure potential risks are considered and addressed.
- Ensure requests for changes in user network permissions are recorded and retained in a manner that allows their retrieval when needed.
- Generate, review, and retain logs of network activity to provide important information in the event network security is compromised.

Report #1508

This is our second follow-up on action plan steps identified in audit report #1210. The purpose of this follow-up is to report on the progress and status of efforts (as of February 28, 2015) to complete the action plan steps that were due for completion as of September 30, 2014. To determine the status of the action plan steps, we interviewed staff and reviewed relevant documentation.

Background

In order for a computer network to operate securely there must be a mechanism in place to know who should be allowed to access the network, what they are allowed to do on the network, and what computer hardware is allowed to be part of the network. Active Directory is that mechanism for the City.

Active Directory serves as a central location for the City's network administration and security. It is responsible for authenticating and authorizing all network activity by users and computers within the City's network. It assigns and enforces security policies for the network.

Active Directory is built into the Microsoft operating system that is used on servers, but is not enabled to function on all servers. When Active Directory is enabled, that server becomes what is known as a Domain Controller, which performs the above described duties (e.g., authenticating users and computers). In the City's network there are multiple domain controllers working together to manage network activity.

The operational needs, geographic dispersal, and size of an organization are important factors to be considered when choosing the design of an organizations' Active Directory. Active Directory allows an organization to organize the elements of the network (i.e., users, computers, printers, etc.) into a hierarchical structure, similar to an organizational chart.

Active Directory implementation design is a logical organization of the City's network and is not dependent on the physical aspects of the network or the managerial organization of the City.

The significant terms relating to Active Directory design and their definitions are:

Forest: The highest organizational level of an Active Directory. Each forest is a separate installation/instance of Active Directory and can stand alone as a separate network.

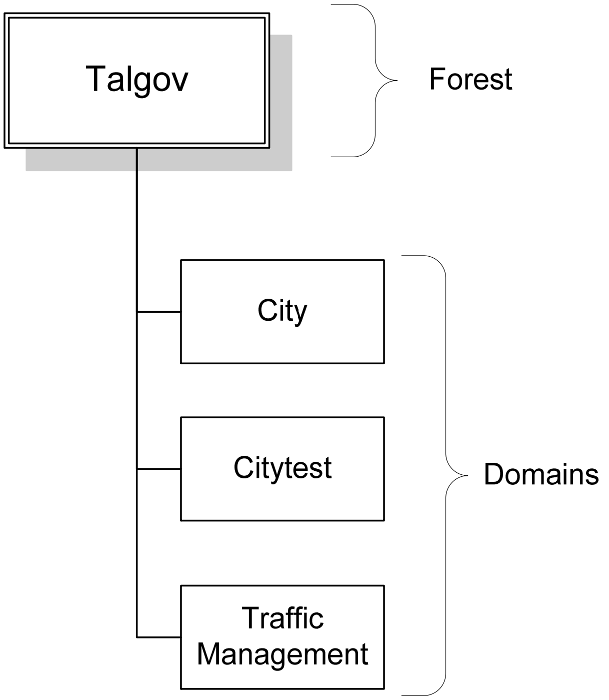
Domain: A domain is a single partition of a forest and is a central collection of objects that share a directory database. This shared database contains the user accounts, computers, servers, and other hardware that make up the domain. The domain is also the Active Directory level at which users are authenticated (logged on).

Groups: A group is a collection of users or computers. Groups allow multiple users or computers to be managed as a single unit, thereby simplifying the administration of multiple users or computers by assigning rights and permissions to the group rather than each individual user.

Users: An individual user must have an Active Directory user account to log on to the City's network. The account provides an identity for the user. Active Directory uses that identity to authenticate and grant authorization for the user to access specific networked resources (e.g., software applications and data files). User accounts are also used as service accounts for some software applications. A service account is set up in Active Directory to allow one software application to communicate through the City's network to another software application (i.e., interface).

The City has implemented Active Directory as a single forest with multiple domains. Figure 1 shows a representation of the City's Active Directory.

Figure 1: City's Active Directory



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. Seven of those action plan steps were reported as completed in our initial follow-up report (#1413 issued February 27, 2014). Regarding the remaining 24 action plan steps, as of February 28, 2015, ten were completed and actions had been initiated, but not completed, for the remaining 14 steps. Table 1 below shows the actions plan steps and their status as determined by our follow-up.

Table 1
Action Plan Steps from Audit Report #1210
Due as of September 30, 2014, and Current Status

Action Plan Steps Due as of September 30, 2014	Current Status as of February 28, 2015
A) Comply with APP 809 regarding the separation of development and testing environments.	
1. 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.	✓ Completed in a prior period.
2. Take appropriate actions based on the evaluation conducted in the preceding step and document the decisions made.	✓ Completed in a prior period.
B) Help ensure network authorizations are documented and can be retrieved when needed.	
1. A job code will be added to the BOSS system for changes in user account permissions.	♦ **In progress.** ISS is currently working on developing an electronic SharePoint form to replace the current manual form. The SharePoint form will feed the information into BOSS through a system interface and automatically create a BOSS work order ticket for ISS. The interface between SharePoint and BOSS is expected to be in place by the end of the second quarter of 2015. The completion date for this action step has been amended to September 30, 2015.
2. 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.	♦ **In progress.** As noted in Step B1 above, ISS is developing an electronic form to replace the current manual form. Once that step is complete, ISS plans to train users in the new process. The completion date for this action step has been amended to September 30, 2015.
3. 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.	♦ **In progress.** As noted in Step B1 above, ISS is developing an electronic SharePoint form to replace the current manual form. ISS stated once the revised process is in place, the SharePoint form will identify errors or omissions, and prevent requests from being submitted to ISS unless the form is completed correctly. The completion date for this action step has been amended to September 30, 2015.

C) Comply with Administrative Policy and Procedure 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.	
1. 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.	✓ **Completed.** ISS created a Third Party Connection Policy whereby any third party (non-City employee) must meet the following provisions in order to be considered for approval by ISS to access the City's network: (1) be sponsored by a City department, (2) have a legitimate and compelling business need to access the City's network, and (3) complete and sign a third party agreement which includes information such as how the third party is going to use the connection (access) and how much bandwidth the third party anticipates using. Upon receiving this information, ISS will review and approve the request if it meets established ISS criteria. If a virtual private network is needed by the third party, ISS established additional steps that must be followed. The Third Party Connection Policy stipulates all third party accounts will expire every 30 days, and any third party user who needs to continue their access after 30 days must request and be approved for an additional 30 days by ISS.
2. New user accounts for third parties will not be created without a completed compliance statement.	✓ **Completed.** ISS is in the process of applying the newly established Third Party Connection Policy. In addition to applying that policy to third parties requesting new user accounts, ISS is also identifying third parties with existing user accounts for purposes of requiring those third parties to comply with the newly established Third Party Connection Policy (i.e., by completing an appropriate agreement and obtaining approval from ISS). During our follow up, ISS provided examples of recently executed third party agreements for both new and existing user accounts. Accordingly, this step is considered completed.
D) Ensure third parties network access is removed in a timely manner when it is no longer needed.	
1. New user accounts set up for third parties will be configured such that they expire six months after the date they are established.	✓ **Completed.** ISS has received and processed completed third party connection requests from both existing third party users and a new third party user. ISS has also revised its policies and procedures to set third party account expiration at 30 days instead of the six months originally planned in the initial audit action plan steps. Accordingly, this step is considered complete.

2. All existing third party user accounts will be changed such that they expire in six months.	✓ **Completed.** As noted in Step C2 above ISS is in the process of applying the newly established Third Party Connection Policy. In addition to applying that policy to third parties requesting new user accounts, ISS is also identifying third parties with existing user accounts for purposes of requiring those third parties to comply with the newly established Third Party Connection Policy (i.e., by completing an appropriate agreement and obtaining approval from ISS). During our follow up, ISS provided examples of recently executed third party agreements for both new and existing user accounts. Additionally, ISS decided to set third party accounts to expire in 30 days instead of the six months noted in the initial audit action plan steps. Accordingly, this step is considered completed.
3. When reviews of individual third party user accounts occur, the expiration date for those accounts will be extended for no longer than six months from the date of the review.	✓ **Completed.** As noted in Step C2 above, ISS is in the process of identifying all third party accounts. As also noted in the previous steps, ISS decided to set third party accounts to expire in 30 days. Furthermore, those accounts will be extended, upon review and approval, for no longer than an additional 30 days, after which an additional review will be required before the accounts can be approved for a subsequent 30-day period. ISS has already identified some third party accounts, and those accounts are set to expire after 30 days, with expired accounts extended after review and approval for no longer than an additional 30-day period. Based on this procedure, this step is considered complete.
E) Ensure risks to the City's Active Directory and computer network are periodically and formally reviewed and evaluated.	
1. A formal documented risk assessment of the City's network, to include Active Directory, will be conducted at least annually.	♦ **In progress**. ISS stated they are working with Microsoft to identify a timeframe for Microsoft to perform a formal security risk assessment of the City's Active Directory. ISS anticipates the work will be completed and a report issued to ISS by the end of the fiscal year. Accordingly, the completion date for this action step has been amended to September 30, 2015.

2. The risk assessment will be presented to the CIO and the ISS Steering Committee.	♦ **In progress**. As noted in step E1, ISS is working with Microsoft to establish a timeframe for Microsoft to perform a formal security risk assessment of the City's Active Directory. Once Microsoft's report is complete, ISS will present the report to the ISS Steering Committee. The completion date for this action step has been amended to September 30, 2015.
F) Ensure system and application acquisitions are properly reviewed and approved; existing computer systems are periodically reviewed for effectiveness; and the purpose, goals, policies, and objective of ISS are reviewed by the ISS Steering Committee.	
1. The ISS Steering Committee will be reactivated and meet on a quarterly basis.	✓ Completed in a prior period.
2. The ISS Steering Committee will be informed of City activities which impact ISS or relate to information technology type system acquisitions.	✓ Completed in a prior period.
3. Guidance and approval will be sought from the ISS Steering Committee as needed for City information technology related activities.	✓ Completed in a prior period.
4. The ISS Steering Committee will assess risks related to systems operating outside ISS's support and control structure.	♦ **In progress.** The ISS Steering Committee has formed a Technical Advisory Group (TAG) whose operational activities are to assist the committee with prioritization of technology support and services, and to disseminate information from the committee to managers and key stakeholders throughout the City. While not specifically delineated in the TAG's charter or bylaws, ISS management stated they are proposing TAG's role include the task of performing risk assessments for systems outside ISS's support and control. Such an assessment has not yet been conducted. The completion date for this action step has been amended to September 30, 2015.
G) Help ensure user accounts that have not been used within a reasonable time period are deactivated.	
1. The inactive user accounts identified in the audit will be reviewed and considered for deactivation as applicable.	✓ **Completed.** We reviewed ten user accounts identified during the original audit as not being used within the previous 90 days. Of the ten accounts reviewed, two accounts had again become active (i.e., recently used.) The remaining eight accounts had properly been either deleted or disabled (deactivated). Accordingly, this step is considered complete.

2. 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.	✓ **Completed.** ISS has established and is using two queries to periodically identify accounts not used within the previous 90 days. Applicable accounts are disabled (deactivated) based on ISS's review of the query results. Accordingly, this step is considered complete.
3. The user accounts identified in the preceding action plan step will be reviewed and deactivated as deemed appropriate by ISS.	✓ **Completed.** ISS is reviewing query results addressed in the previous action plan step to disable (deactivate) applicable accounts.
H) Help ensure user accounts are not shared by multiple individuals.	
1. 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 progress.** At the time of our follow up in February 2015, ISS had identified approximately 440 shared accounts, for which 185 had been reviewed and eliminated. ISS was in the process of reviewing the remaining identified shared accounts to determine if there was justification for retaining or eliminating those accounts. Actions were also still in progress to determine if there were any additional shared accounts that needed to be reviewed (i.e., in addition to those already identified). ISS plans to complete those remaining actions by September 30, 2015, and the completion date for this action plan step has been amended accordingly.
2. ISS will review the user accounts identified in the previous step and obtain written justification from the applicable City departments as to the reasons these accounts should continue to be used.	♦ **In progress.** As stated in the reported status for step H1, ISS is in the process of identifying and reviewing shared accounts. Those accounts reviewed to date have either been disabled (as no longer needed) or are in the process of being justified (for continuation) by the applicable City departments. ISS plans to identify and review remaining shared accounts (and either disable or obtain justification to continue those accounts) by September 30, 2015. The completion date for this action plan step has been amended accordingly.
3. ISS will review and retain the justifications provided by the City Departments.	♦ **In progress.** As stated in the reported status for step H1, ISS is in the process of identifying and reviewing shared accounts. Those accounts reviewed to date have either been disabled (as no longer needed) or are in the process of being justified by the applicable City departments. Justification for applicable accounts will be retained by ISS. ISS plans to identify and review remaining shared accounts (and either disable or obtain justification to continue those accounts) by September 30, 2015. The completion date for

	this action plan step has been amended accordingly.
4. 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.	♦ **In progress.** For the shared accounts identified and reviewed to date, ISS has considered the purpose and justification, if provided, for continuation of the account. That consideration has been used in the ISS determination to either disable or continue the shared account. ISS plans to identify and review remaining shared accounts (and either disable or obtain justification to continue those accounts) by September 30, 2015. The completion date for this action plan step has been amended accordingly.
I) Ensure password policies are complied with and not overridden thereby increasing the risk that user accounts may be compromised.	
1. ISS will identify all user accounts that have had password controls overridden *(i.e., accounts with passwords set to never expire).*	✓ **Completed.** ISS has used a query to identify all accounts with passwords set to never expire, and is currently in the process of identifying owners of those accounts. Once the account owners are identified, ISS plans to work with account owners to either deactivate the account if no longer needed, or program the account so the password expires after a certain amount of time, in accordance with good control practices. Accordingly, this step is considered complete.
2. Written justification will be obtained from applicable departments as to why those password controls should be allowed to be overridden.	♦ **In progress.** As stated in the reported status for step I 1, ISS is in the process of identifying the owners of accounts identified as having passwords set to never expire. As they identify the owners, ISS is either deactivating the accounts if they are no longer needed, or programming the passwords to expire within a given period of time. The completion date for this action plan step has been amended to September 30, 2015.
3. ISS will review and retain the justifications provided by the City departments.	♦ **In progress.** As stated in the reported status for step I 1, ISS is in the process of identifying the owners of accounts identified as having passwords set to never expire. As they identify the owners, ISS is either deactivating the accounts if they are no longer needed, or programming the passwords to expire within a given period of time. Accounts determined by ISS to be justified in having passwords set to never expire will be documented by ISS. The completion date for this action plan step has been amended to September 30, 2015.

4. When in ISS's judgment, the justification for the overriding of password controls does not outweigh the risks posed by the password control overrides, ISS will remove the password override and ensure applicable password controls are enforced. When justification for password control overrides outweighs the associated risks, no action will be taken.	♦ **In progress.** As stated in the reported status for step I 1, ISS is in the process of identifying the owners of accounts identified as having passwords set to never expire. As they identify the owners, ISS is either deactivating the accounts if they are no longer needed, or programming the passwords to expire within a given period of time. Accounts determined by ISS to be justified in having passwords set to never expire will be documented by ISS. The completion date for this action plan step has been amended to September 30, 2015.
J) Ensure operating system updates are installed on domain controllers in a timely manner.	
1. Updates and patches to the operating systems of the domain controllers, published by Microsoft, will be identified on a monthly basis.	✓ **Completed.** ISS receives periodic alerts regarding security updates and patches released by Microsoft. ISS stated they typically review these alerts when received, but at a minimum review them on a monthly basis. In their review of the available updates, ISS indicated they determine which updates are applicable to servers and programs utilized by the City. Plans are then established to install those updates on the City's domain controllers.
2. Within one month of the release of the updates and patches by Microsoft they will be installed on the applicable domain controllers.	♦ **In progress.** Because rebooting of the server is required after updates and patches are installed, ISS said they decided to minimize potential interruptions to those departments operating 24 hours a day by installing updates quarterly instead of monthly, as originally planned. According to ISS, they do, however, immediately install security updates marked as "critical" by Microsoft instead of waiting until their next planned quarterly update. We identified 12 security updates released by Microsoft during two selected months of 2014 (April and September) that were applicable to City servers and programs. We determined if and when those updates were applied by ISS. Our review showed six of the 12 updates had been applied by ISS. Five of those six were installed within three months of their respective release dates and the remaining update was installed eight months after it was released by Microsoft. The other six updates had not been installed as of February 2015. While none of the 12 updates were marked as "critical" by Microsoft, they should have been timely installed.

	In response to our inquiry on this matter, ISS indicated they are planning to have the outstanding updates applied by the end of March 2015. Accordingly, this step has not been completed, and the completion date has been amended to April 30, 2015. We recommend ISS continue efforts to ensure security updates are timely installed. **Audit comment:** While we acknowledge ISS's intention of minimizing interruptions to departments operating 24 hours a day, we believe the redundancy available through multiple domain controllers would allow for interruptions to have a minimal impact. Also, delaying the installation of security updates only increases the risks to which those departments are exposed. Security updates are released because Microsoft has identified a vulnerability that needs to be addressed. We recommend ISS reconsider their plans to apply updates quarterly, and revert back to the original plan to install security updates no later than a month from the date of their release by Microsoft. Subsequent to discussions with ISS staff regarding the timing of applying updates to the domain controllers, ISS revised their policy so updates and patches will be applied to the domain controllers at least on a monthly basis.
K) Ensure activity logs are generated, reviewed and retained as appropriate.	
1. Evaluate and consider the risks posed by not generating or retaining logs of the activity in Active Directory.	✓ Completed in a prior period.
2. Take appropriate actions based on the evaluation conducted pursuant to the previous step and document the decisions made.	✓ Completed in a prior period.

Table Legend:

✓ Issue addressed and resolved. ♦ Actions initiated but not yet completed.

Conclusion

Table 1 above shows ISS successfully completed and resolved ten of the 24 action plan steps established to address issues identified in audit report #1210 that were due during this follow-up period. Completed action plans steps include:

- Develop a third party compliance statement to serve as acknowledgement third party users understand and comply with the City's computer and network policies, and remove third party access in a timely manner when it is no longer needed (five steps).

- Ensure inactive accounts are deactivated, when applicable and appropriate (three steps).
- Identify user accounts with password controls that have been overridden (one step).
- Identify updates and patches to the operating systems of the domain controllers that are published by Microsoft on a monthly basis (one step).

Additionally, Table 1 shows the 14 action plan steps due for completion this follow-up period for which actions have been initiated, but not completed. Those action plan steps relate to the following:

- Ensuring network authorizations are documented and can be retrieved when needed (three steps).
- Conducting a formal risk assessment of the City's network (two steps).
- Assessing risks related to systems operating outside ISS's support and control (one step).
- Identifying and eliminating shared accounts, unless there is appropriate justification documented for keeping an account as a shared account (four steps).
- Obtaining appropriate justification to keep accounts with password controls that have been overridden, otherwise set the account so appropriate password controls are followed (three steps).
- Installing updates and patches to the domain controllers in a timelier manner (one step).

We recognize ISS has completed 17 of the 31 (55%) action plan steps established to address concerns raised in the Audit of Active Directory, yet almost half of the action steps still remain unfinished nearly three years after the initial audit report was released. Because many of the remaining steps are time consuming and reliant upon other City departments responding to requests from ISS, we encourage ISS management to contact department directors or other leadership members for those departments and/or commit additional resources, if necessary, to resolve the remaining 14 steps in the near future.

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

Appointed Official's Response

City Manager:

I am pleased to see that the second follow-up on the Audit of Active Directory indicates that 17 out of the 31 steps have been completed and actions steps are on-going to complete the 14 remaining steps. Ten of those 17 steps were completed during this follow-up period, while seven steps were completed in the previous follow-up period. Additionally, I am extremely pleased that the overall scope of the audit indicated that the policies, implementation, and management of Active Directory, as a whole, were appropriate and provided adequate security relating to the City's network. I would like to thank the City Auditor's Office as well as all of the departments for their work and follow-up on this audit.

Copies of this audit follow-up #1508 or audit report #1210 may be obtained from the City Auditor's website (http://www.talgov.com/auditing/auditing-auditreports.aspx) 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:
Patrick A. Cowen, CPA, CISA, Sr. IT Auditor
T. Bert Fletcher, CPA, CGMA, City Auditor