Final Audit Follow Up

As of September 30, 2003

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

Sam M. McCall, CPA, CIA, CGFM
City Auditor

"Audit of the Logical Security of the City's Local Area Network"

(Report #0201, Issued October 26, 2001)

Report #0404 *December 2, 2003*

Summary

This is the final follow up on the Audit of the Logical Security of the City's Local Area Network (#0201). Eighteen of the 20 action plan steps (90%) have been completed. The two remaining steps have been partially completed and relate to:

- Implementing recommendations from the vulnerability assessment reports, and
- Implementing periodic monitoring procedures to ensure that the controls are in place related to deleting user access.

Since no additional follow ups will be conducted on this audit, these partially completed tasks become management's responsibility to complete and address as appropriate.

During our testing of user IDs and passwords, we also noticed a slight increase in user IDs with passwords set not to expire. We continue to recommend that all users comply with the Information Security Policy and periodically change their passwords to minimize the risk that users' passwords are compromised and used in an unauthorized manner. Exceptions to the policy should be justified and minimized.

Scope, Objectives, and Methodology

Audit Report #0201 and this subsequent follow up were conducted in accordance with Generally Accepted Government Auditing Standards and Standards for the Professional Practice of Internal Auditing, as applicable. We reviewed documentation, interviewed staff, and conducted selected tests of information security controls to ensure they were working effectively.

Report #0201

The scope of report #0201 was to evaluate the logical security controls protecting the City's local area network (LAN) resources. Fieldwork took place from December 2000 through June 2001.

The primary objectives of the audit were to:

- obtain a general understanding of the network operations and the logical access paths into the network;
- provide assurances regarding security controls that management believed were in place;
- evaluate the adequacy of security controls that management believed should be improved;
- determine the adequacy of policies and procedures related to unauthorized access into the City's LAN;

- ♦ determine the adequacy of the controls in place to prevent unauthorized access into the City's LAN; and
- ♦ determine the accessibility to confidential information stored on the City's LAN.

The scope of this audit was limited in that our audit procedures: 1) included basic, but not extensive, vulnerability assessment activities (to identify potential access weaknesses) and no penetration testing was performed (to obtain unauthorized access); and 2) did not include detailed database security testing.

Report #0404

The purpose of this final audit follow up is to report on the progress and/or status of efforts to implement management action plan steps provided in the audit report.

Previous Conditions and Current Status

In report #0201, the action plan identified four main areas, each with specific action steps (20 steps in total) that need to be addressed. These included:

- Policies and procedures, including developing written information security policies and procedures and providing training to City employees.
- Management and monitoring, including designating an information security group to implement and monitor security activities; and periodically contracting with outside vendors to assess the City's information security infrastructure.
- User access controls, including developing and implementing adequate user access procedures; conducting a vulnerability assessment and implementing recommendations; limiting the number of users with privileged access capabilities; identifying all modems on the network; and implementing controls so unauthorized users cannot access the network remotely.
- Protection of confidential information, including establishing processes within departments to adequately protect data defined as exempt from public records from unauthorized access and inadvertent disclosure.

As of September 30, 2003, 18 of the 20 action steps due were completed (90%) and the two remaining steps have been partially completed. Table 1 shows the status of these tasks and actions that were taken during the current follow up period. Estimated completion dates are provided when available.

Table 1
Previous Conditions Identified in Report #0201 and Current Status

Previous Conditions	Current Status
Policies and Procedures	
• Provide draft security policies to a City employee committee for review and incorporate appropriate feedback into the draft document.	√ Completed in a prior period.
Provide draft security policies to City management, including City Attorney's Office, Treasurer-Clerk's Office, Human Resources, for feedback and to ensure the proper process is followed.	√ Completed in a prior period.

• Present final draft security policies to City management, including Executive Team, Appointed Officials, and other appropriate persons as determined for feedback.	√ Completed in a prior period.
• Identify the appropriate City staff to provide training to all City employees as to the security policy detail.	√ Staff was identified in a prior period. Audit Comment: ISS is currently working with Communications to produce a training tape that can be shown to employees across the City. There is not an estimated completion date.
Management and Monitoring	
• Designate an information security group to consist of various information security related positions, such as: technology infrastructure administrator, database administrator, computer operations and customer service supervisor, and mission-critical application security administrators.	√ Completed in a prior period. This group is meeting periodically. Audit Comment: The Senior IT Auditor in the Office of the City Auditor is included as an advisory member of this committee.
• Information security group is to develop standard operating procedures for implementing security activities, such as: coordinating and conducting information security awareness training for employees; routinely monitoring security activities, such as suspected or actual security breaches; recording, tracking, and analyzing suspected and actual information security incidents; and assisting department-owners in assessing the confidentiality and security requirements of their data (also called assessing risks).	√ Completed during this period. The Information Security Committee has developed a Security Manual that includes: the committee's roles and responsibilities, the Information System Security Policy, and specific policies and procedures for databases and selected application systems. Audit Comment: We commend the committee for its work in developing this manual and recognize that it will be a work in progress as other applications and computing environments are added.
• Contract to have a vulnerability assessment of current City network infrastructure performed to identify all potential areas of weakness.	√ Completed in a prior period.
• Periodically contract with an outside vendor to assess the City's information security infrastructure.	√ Re-assessments have been conducted quarterly (most recent assessment was to be completed in November 2003).

• Implement recommendations from the vulnerability assessment results.	⋆ Partially completed. ISS is in the process of implementing some of the remaining recommendations they determined important to network operations. These are estimated to be completed by December 31, 2003.
• Perform post review after implementation of the recommendations.	√ ISS staff contracts quarterly with a vendor to conduct vulnerability assessments. With each one, the vendor assesses the status of the prior recommendations.
User Access Controls	
• Develop standard operating procedures in Information Systems Services (ISS) Distributed Network Systems for staff to understand the processes needed to be in place regarding how to add, change, transfer, and delete user access. In addition, ISS management should include periodic monitoring procedures to ensure that the controls are in place.	⋆ Partially completed in prior period. ISS developed and implemented written procedures to add, change, and transfer user access to the network. However, periodic monitoring procedures have not been performed to ensure controls are in place. Audit Comment: We tested access controls for 54 terminated employees between April 1 through October 29, 2003, to determine whether they had access on the network. We found five terminated employees (9%) that still had access to the network.
• Identify and determine the functionality of all modems operating in the City, and implement adequate controls to ensure that the network cannot be accessed without proper authentication.	√ Completed during this period. Audit Comment: Using a daily phone log, we tested to determine whether any connections were made to or from the 66 identified phone lines connected to modems. During our testing, we noted no exceptions, which indicates that modem controls are working effectively.
Protection of Confidential Information	
• Police Department security administrators need to develop and implement a process to perform periodic reviews of the user IDs in their systems.	√ Completed in a prior period.

• Police Department should examine the use of shared passwords and determine how best to adequately protect their data.	√ Completed in a prior period.
• Fire Department is to develop and implement procedures to inform the CAD/RMS security administrator when employees terminate from the Fire Department.	√ Completed in a prior period.
• In the Human Resource Management System (HRMS), a consistent use of the "public record" indicator should be implemented, and staff should be notified and trained as needed.	√ Completed in a prior period.
• Customer Information System (CIS) – 1. CIS project team should design and implement a method to identify a customer as being exempt from public records in the new CIS. 2. All exempt employees should be identified in the CIS, and staff should be notified and trained regarding how the indicator is to be utilized.	√ Completed during this period. For the appropriate customers, Customer Service Representatives have been instructed to write "***CONFIDENTIAL, Information should only be provided to the account holder.***" in the Alert field in CIS. Audit Comment: Management will need to be diligent in ensuring that the personal information in these confidential accounts is not disclosed when responding to any public records requests.
• Energy Loan Database – Energy Services management is to explore options and implement a process to identify which records in the database are exempt from public records to minimize the risk that personal information for exempt employees is improperly disclosed.	√ Completed in a prior period.
• Research to identify the best encryption software that could be used by any City employee to encrypt e-mail messages and attachments when transmitting confidential information. Roll out the use of the encryption software to those departments with the greatest need, and train staff as needed.	√ Completed during this period. ISS has implemented the encryption feature in Microsoft Outlook allowing internal e-mails to be sent encrypted. City management and users have been notified of this new feature and can request assistance from ISS to set up as needed.

• Growth Management and City/County GIS – staff needs to remove personal information for exempt employees from their Internet site and determine a method for identifying a record as exempt. Steps include: a. A subcommittee of the Permit Tracking System (PETS) inter-local steering committee is to identify options to identify records that should be exempt from public records in the PETS system. b. The PETS inter-local steering committee will evaluate and then select the most cost efficient and least work-intensive option to implement. c. PETS technical staff will design and implement the approved method and develop a process to periodically verify that the records that should be protected are identified.	√ Completed during this period. Rather than removing personal information for only those exempt employees, the PETS steering committee opted to redact all names when displaying permitting information on the Internet. Audit Comment: While this solves one issue, redacting all names may in turn cause another issue related to limited access to public records. With all changes that are considered, we recommend that protecting personal information for those exempt employees from being accessed over the Internet continue to be a priority.

Table Legend:

- Issue addressed in the original audit

✓ Issue has been resolved
★ Partially completed, completion date has been amended

Remaining Outstanding Issues

As the audit follow up period closes, two action plan tasks remain partially completed and are designated as management's responsibility to complete. As noted in Table 1, these include:

- Implementing recommendations from the vulnerability assessment reports, and
- Implementing periodic monitoring procedures to ensure that the controls are in place related to deleting user access. During our testing of active user accounts on the network, we identified five terminated employees out of the 54 terminated employees tested that had an active network user account. We notified ISS for them to remove the users' access.

In addition, we noted that there were 204 user IDs with passwords that were set not to expire. These user IDs included employees from executive management and generic user IDs utilized in various departments throughout the City. This is an increase from the 191 user IDs with passwords set not to expire identified during the prior follow-up period. We continue to recommend that all users comply with the Information System Security Policy and periodically change their passwords to minimize the risk that users' passwords are compromised and used in an unauthorized manner. Exceptions to the policy should be justified and minimized.

We appreciate the assistance provided by staff in Information Systems Services and other affected City departments during this audit follow up.

Appointed Official Response

City Manager Response:

The ability to ensure that the City's logical technology assets are safe and secure is certainly a priority and I appreciate the follow-up by Auditing staff. Plans are in place to complete all of the action items documented in this report. I would like to thank Auditing and DMA/ISS for their work in this effort.

Copies of this Final Audit Follow Up (#0404) or audit report #0201 may be obtained at the City Auditor's web site (http://talgov.com/citytlh/auditing/index.html) or via request by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail, in person (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:
Beth Breier, CPA, CISA, Senior IT Auditor
Sam M. McCall, CPA, CIA, CGFM, City Auditor