Final Audit Follow Up

As of May 14, 2003

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

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

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

(Report #0106, Issued December 18, 2000)

Report #0320 ***June 16, 2003***

Summary

This is the final follow up on the Audit of the Physical Security of the City's Local Area Network (#0106). While almost all of the issues have been resolved, three outstanding action plan tasks remain partially completed.

The outstanding tasks include:

1. Training of employees on the City's new information security policies;
2. Strengthening the physical security controls at locations housing computer local area network (LAN) equipment; and
3. Completing the procedures for restoring City mainframe/servers after a disaster (also referred to as Disaster Recovery Planning).

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

Scope, Objectives, and Methodology

Report #0106

The scope of report #0106 was to evaluate the physical security controls protecting the City's local area network (LAN) resources during the period of March through September 2000. The primary objectives of the audit were to:

- obtain a general understanding of the network operations and the physical location of all network servers and other LAN infrastructure equipment;
- evaluate the physical control environment of the network servers and other LAN infrastructure equipment; and
- evaluate the physical control environment of purchased LAN equipment waiting to be installed.

Report #0320

The purpose of this final audit follow up is to report on the status of management's efforts to implement the recommended action plan steps included in the audit report and subsequent follow up reports.

To obtain information, we interviewed ISS management, obtained and reviewed relevant documentation, observed an off-site disaster recovery test, and visited selected locations. This follow up report was conducted in accordance with Generally Accepted Government Auditing Standards and Standards for the Professional Practice of Internal Auditing, as applicable.

Previous Conditions and Current Status

In report #0106, the action plan identified four main areas, each with specific action steps (14 total) that needed to be addressed. These included:

- Information security, including designating an information security manager and developing written information security policies and procedures;
- Backups, including developing and implementing written backup policies and procedures, determining responsibility, and educating staff;
- Physical security, including determining responsibility, strengthening physical security controls, and implementing written policies and procedures; and
- Computer inventory, including strengthening inventory controls by developing and implementing written procedures.

As a result of the March 2002 follow up audit procedures, two additional action steps were added to: 1) determine a risk-based approach to identify City systems that would need to be immediately restored in the event of a disaster; and 2) implement a process to regularly identify terminated employees and remove their access to computer rooms.

As of this final follow up report, all 16 action plan tasks identified in the original audit report (14) and during the follow up periods (2) were due to be completed. Table 1 shows the status of these tasks.

Table 1

Summary of Tasks as of September 30, 2002		
# Tasks Due	# Tasks Completed	# Tasks Behind Schedule
16	13 (81%)	3

Table 2 provides a summary of each action plan step and the status by main area.

Table 2
Previous Conditions Identified in Report #0106 and Current Status

Previous Conditions	Current Status
Information Security	
• Obtain approval for an information security manager position and fill position.	√ Completed during prior period.
• Develop information security policies and procedures that address physical security of LAN equipment throughout the City.	√ Completed during prior period.
• Obtain management approval of the policies and procedures, including: ISS, executive team, and the City Manager.	√ Completed during prior period.
• Identify and obtain funding to implement security requirements per the approved information security policy.	√ Funding was identified in the Network Upgrade Project to fund ISS information security needs.
• Implement approved policies and procedures within ISS and affected departments, including policy distribution and training.	★ **Partially completed.** The security policy has been written, approved, and made available on the City's Intranet, but training still needs to be conducted. ISS Management indicates that they are scheduling the training to take place in Fall 2003.
Backups	
• Develop written ISS policies and procedures and timelines for backing up mainframe/servers under the responsibility of ISS. This will also involve the application system development team.	√ Completed during prior period.
• Identify resources, including funding and personnel, to implement approved backup policies and procedures.	√ Completed during prior period.
• Educate staff, including computer operators, on their responsibilities regarding the backup procedures.	√ Completed during prior period.
• Determine responsibility for ensuring that the backup policies and procedures are performed by proper personnel and staff.	√ Completed during prior period.

• Implement a risk-based process to determine what City systems should be included in the ISS disaster recovery plan. [*This additional step added after March 31, 2002, Follow up.*]	√ The Director of ISS worked with City management and the ISS Steering Committee to establish a priority of applications to be restored.
• Develop written ISS policies and procedures and timelines for restoring identified mainframe/servers at the off-site location. [*Since the original audit, all mainframes have been replaced by servers.*]	★ **Partially completed**. Staff has developed a draft of written procedures for what is to be backed up and how the critical systems are to be restored. [In addition, see Remaining Outstanding Issues below this table.]
Physical Security	
• Determine who controls the equipment rooms at the locations housing LAN equipment outside City Hall.	√ Completed during prior period.
• Determine who is responsible for strengthening the physical security at the locations housing LAN equipment outside City Hall.	√ Completed during prior period.
• Identify resources, including funding and personnel, to bring the locations up to approved policies and procedures.	★ **Partially completed**. Funding has been identified and personnel have been assigned, but the work has not yet been completed. Estimated completion date has been amended to Fall 2003.
• Implement a process to regularly identify terminated employees and remove their access to computer rooms. [*This additional step added after March 31, 2002, Follow up.*]	√ Completed during prior period.
Computer Inventory	
• Develop and implement procedures for inventory controls over purchased computer equipment. Such procedures addressed: maintaining a perpetual inventory; segregating job responsibilities; conducting physical counts and reconciling records to equipment; maintaining a chain of custody of equipment; and monitoring the length of time the equipment is stored by ISS to provide for timely installation of equipment.	√ Completed during prior period.

Table Legend:

- • Issue identified.
- √ Issue has been addressed and resolved.
- ★ Partially completed. Management's responsibility to complete.

Remaining Outstanding Issues

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

1. Training of employees on the City's new information security policies;
2. Strengthening the physical security controls at locations housing computer local area network (LAN) equipment; and
3. Completing the procedures for restoring City mainframe/servers after a disaster (Disaster Recovery Planning).

We conducted some additional audit testing during this final follow up period to determine the adequacy of the ISS Disaster Recovery Planning. ISS is in the process of finalizing their disaster recovery plan procedures. ISS contracts with an out-of-town vendor to provide an emergency facility with a pre-defined computing environment (hardware and operating systems) for testing purposes and to be available for the City when a disaster is declared. ISS staff has been assigned disaster recovery responsibilities and is involved in the bi-annual testing procedures.

We observed the May 2003 disaster recovery test that took place at the vendor's emergency facility outside of Tallahassee. We noted that the ISS staff were able to restore two of the three mission critical applications; the third application was not able to be restored due to the lack of some necessary files that had been inadvertently left off the recovery backup tapes.

Regarding the testing, the following issues and recommendations were identified:

1. The equipment provided by the vendor did not include all the equipment stated per the contract. We recommend that prior to arrival at the emergency facility, ISS staff verify with the vendor that all expected equipment will be provided and set up as needed.
2. Not all executable files needed could be restored from the backup tapes. Subsequent to the disaster recovery test, ISS staff corrected the backup process to include all needed files.
3. Application test procedures were not defined to ensure that the restored application and data were working appropriately. We recommend that functional business experts be involved in the disaster recovery testing process in order to test the applications adequately. ISS plans to include users in the next disaster recovery test scheduled for September 2003.
4. While some draft procedures had been developed and were utilized, these procedures are not completed. We recommend that staff continue to develop the disaster recovery plan procedures until they are complete and can assist the recovery efforts in the most efficient and effective manner. However, we also acknowledge that these procedures, once completed, will need to be periodically revised based on technology and staffing changes.

We have worked closely with ISS during the follow up period for this audit and would like to express appreciation for the professional assistance provided by ISS management and staff.

Appointed Official Response

City Manager Response:

The ability to ensure that the City's physical 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 the City Auditor's Office and the Department of Management and Administration/ Information Systems Services for their work in this effort.

Copies of this Final Audit Follow Up or audit report #0106 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 (dooleym@talgov.com).

Audit Follow Up conducted by:
Beth Breier, CPA, CISA, Senior IT Auditor
Sam M. McCall, CPA, CIA, CGFM, City Auditor