Audit Follow Up

As of September 30, 2002

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 #0304 *December 12, 2002*

Summary

Information Systems Services (ISS) has completed 12 of the 16 (75%) action plan tasks due as of September 30, 2002. Of the remaining 4 tasks, 3 have been partially completed. The outstanding tasks include implementation, distribution and training of the information security policies, completing the procedures for restoring City mainframe/servers should a disaster occur, and strengthening the physical security controls at locations housing computer local area network (LAN) equipment.

In audit report #0106, issued December 18, 2000, we identified areas in which physical security needed to be improved to adequately protect the City's information technology resources. This also included security over the inventory of equipment waiting to be installed as part of the City's LAN.

As the City evolves from a centralized computing environment to a more decentralized computing environment, physical security needs to increase as the number of locations housing information technology resources increases. Physical security controls include restricting physical access to the information systems resources, protecting these resources from environmental hazards, and having the ability to restore operations should the resources become damaged or destroyed.

Because of the sensitive nature of a physical security review, we provided broad descriptions of the physical security weaknesses in our previously issued report. In addition, we provided management with separate reports identifying the specific security weaknesses at each location housing LAN equipment.

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 #0304

The purpose of this audit follow up is to report on the progress and/or status of management's efforts to implement the recommended action plan steps due as of September 30, 2002. To obtain information, we interviewed ISS management regarding the status of the outstanding action steps, obtained and reviewed relevant documentation. 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 need 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, 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) to implement a process to regularly identify terminated employees and remove their access to computer rooms.

As of September 30, 2002, all action plan tasks (16) identified in the original audit report and during the follow-up periods were due to be completed. Estimated completion dates were amended for all outstanding steps. 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	12 (75%)	4

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.	√ In place of an information security manager, a new Security Group has been formed and is tasked with creating standard operating procedures for security issues. This group held their first meeting in October 2002. Audit Comment: The Senior IT Auditor in the Office of the City Auditor will be included as an advisory member of this committee.
• Develop information security policies and procedures that address physical security of LAN equipment throughout the City.	√ Minimal physical security requirements are included in the current draft information security policies and procedures to provide guidance to departments that house LAN equipment.
• Obtain management approval of the policies and procedures, including: ISS, Executive Team, and the City Manager.	√ As of September 30, 2002, the draft policies had been provided to ISS, the City Manager, and the Executive and Leadership Teams to obtain feedback.
• Identify and obtain funding to implement security requirements per the approved information security policy.	√ ISS will use monies from the Network Upgrade projects to fund implementation of the information security policies and procedures as needed.
• Implement approved policies and procedures within ISS and affected departments, including policy distribution and training.	★ Partially completed. The security policy has been written and approved. Implementation, distribution, and training still need to be conducted. Estimated completion date amended to March 31, 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.	√ ISS developed backup procedures for the new backup software.
• 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*].	★ Partially Completed. The Director of ISS requested and received feedback from Leadership Team members regarding critical applications they feel would need to be restored in the event of a disaster. He will now plan to work with 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.	o Completion date amended to March 31, 2003.
Physical Security	
• Determine who controls the equipment rooms at the locations housing LAN equipment outside City Hall.	√ Completed during prior period. Each department is responsible for its own equipment rooms.
• Determine who is responsible for strengthening the physical security at the locations housing LAN equipment outside City Hall.	√ Completed during prior period. The departments are responsible for strengthening the physical security at their locations with assistance available from ISS.
• Identify resources, including funding and personnel, to bring the locations up to approved policies and procedures.	★ Partially completed. ISS will use monies from the Network Upgrade projects to fund construction of nine (9) lockable cabinets to protect LAN equipment. Other solutions include: moving network equipment; or expecting departments to provide adequate protection on site. Estimated completion date amended to March 31, 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*].	√ ISS has implemented a process. Staff will need to periodically review access to ensure the process is working effectively.

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 addressed in the original audit
- √ Issue has been addressed and resolved
- ★ Partially completed
- ♦ In progress
- o Not due yet

Summary of Action Plan Steps

As noted in Table 1 above, ISS has completed 12 of the 16 (75%) due action plan tasks. Of the remaining 4 tasks, 3 have been partially completed. The outstanding tasks include implementation, distribution and training of the information security policies, completing the procedures for restoring City mainframe/servers after a disaster, and strengthening the physical security controls at locations housing computer local area network (LAN) equipment.

We appreciate the assistance provided by Information Systems Services management and staff during this audit follow up.

Appointed Official Response

City Manager Response:

The ability to ensure that the City's logical and physical data assets are safe and secure is certainly a priority and I appreciate the follow-up by Auditing staff. There has been positive progress made in addressing the initial action plans. Plans are in place to complete all of the action plans documented before the next report. I would like to thank Auditing and DMA/ISS for their work in this effort.

Copies of this Audit Follow Up (#0304) 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