Audit Follow Up

As of March 31, 2001

CITY OF TALLAHASSEE

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 #0121 ***May 22, 2001***

Summary

Information Systems Services (ISS) has implemented one of the four scheduled action plan steps and amended three completion dates identified in our previously issued report #0106, Physical Security of the City's Local Area Network Audit Report. In audit report #0106, issued December 18, 2000, we identified some 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 Local Area Network (LAN).

As the City evolves from a centralized computing environment to a more decentralized computing environment, the physical security needs to increase as the number of locations housing information technology resources increase. 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.

Our report identified general issues and recommendations noted during the audit. 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 #0121

The purpose of this audit follow up is to report on the progress and/or status of the efforts to implement the recommended action plan steps due as of March 31, 2001. To obtain information, we conducted interviews with key department staff and reviewed relevant documentation.

The audit and this subsequent follow up were conducted in accordance with Generally Accepted Government Auditing Standards.

Previous Conditions and Current Status

In report #0106, the action plan identified four main areas, each with specific action steps (13 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;
- Strengthening physical security weaknesses, including determining responsibility, implementing written policies and procedures; and
- Safeguarding computer inventory, including developing and implementing written procedures.

As of March 31, 2001, there were four action steps due to be completed. Of those, ISS has completed one (25%) and amended the completion date of the other three. Table 1 provides a summary of the report action steps due and the status by main area.

Table 1
Previous Conditions Identified in Report #0106 and Current Status

Previous Conditions	Current Status
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.	o Behind schedule; completion date has been amended to October 1, 2001.
• Determine responsibility for ensuring that the backup policies and procedures are performed by proper personnel and staff.	o Behind schedule; completion date has been amended to October 1, 2001.
Strengthening Physical Security Weaknesses	
• Determine who controls the equipment rooms at the locations housing LAN equipment outside City Hall.	o Behind schedule; completion date has been amended to May 30, 2001.
Safeguarding Computer Inventory	
• Develop and implement procedures for inventory controls over purchased computer equipment. Such procedures will address: ⇒ Maintaining a perpetual inventory ⇒ Segregating job responsibilities ⇒ Conducting physical counts and reconciling records to equipment ⇒ Maintaining a chain of custody of equipment ⇒ Monitoring the length of time the equipment is stored by ISS to provide for timely installation of equipment	√ Completed. Interim manual procedures have been developed and implemented to provide controls over the computer inventory until the implementation of the new PeopleSoft Financials system. At that point, the ISS Lockup Room (where the computer inventory is stored) will be identified as a warehouse location in the Financials system. This will provide a fully functional on-line inventory control system. We will review this on-line functionality during the next follow-up review period.

Table Legend:
- • Issue addressed in the original audit
- ⇒ Issue sub-components
- ✓ Issue has been addressed and resolved
- o Behind schedule, completion date has been amended
- ✗ Issue not resolved

Significant Outstanding Issues

As noted in Table 1 above, ISS has amended the completion date of three of the four action plan tasks that were due as of March 31, 2001.

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

Appointed Official Response

City Manager Response: Security of the City's information technology infrastructure is of utmost importance, particularly as we continue to decentralize our technology resources. Inventory control procedures have been developed and implemented for the interim period until the inventory module in the PeopleSoft financials system is in place. In the interim, ISS staff will continue their focus on the development of additional procedures necessary to protect our technology environment. I appreciate the assistance of the Auditing staff and ISS in their comprehensive review of our technology resources.

Copies of this Audit Follow Up or audit report #0106 may be obtained 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