Audit Follow Up

As of September 30, 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 #0208 *December 21, 2001*

Summary

Information Systems Services (ISS) has completed four of the nine due action plan tasks, partially completed three action plan tasks, and has amended the expected completion date of the remaining two tasks to be completed during the next follow-up period ending March 31, 2002.

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, 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 #0208

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 September 30, 2001. To obtain information, we conducted interviews with key department staff, attended meetings, and reviewed relevant documentation. This follow up report was 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 September 30, 2001, four of the nine due action steps were completed (44%), and three were partially completed. The completion dates for the remaining two tasks were amended to be completed during the next follow-up period ending March 31, 2002. Table 1 provides a summary of each action plan step and the status by main area.

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

Previous Conditions	Current Status
Policies and Procedures	
• Develop information security policies and procedures that address physical security of LAN equipment throughout the City.	√ ISS has completed the draft of this policy and is circulating it to various departments throughout the City requesting feedback from internal customers and executive management.
• Obtain management approval, including: Information Systems Services, executive team, and the City Manager.	o Behind schedule, completion date has been amended to March 31, 2002.
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.	♦ Interim procedures have been developed and implemented until the new backup software and equipment is implemented. These will need to be revised when the new software and equipment is implemented.
• Identify resources, including funding and personnel to implement approved policy and procedure.	o Behind schedule, completion date has been amended to March 31, 2002.
• Educate staff, including computer operators, on their responsibilities regarding the backup procedures.	♦ Computer operators were provided training regarding their responsibilities to perform backups according to the interim procedures. Additional training will be needed when the new software and equipment is implemented.

• Determine responsibility for ensuring that the backup policies and procedures are performed by proper personnel and staff.	♦ Interim procedures have been developed, implemented, and responsibilities assigned until the new backup software and equipment is implemented. These will need to be revised when the new software and equipment is implemented.
Strengthening Physical Security Weaknesses	
• Determine who controls the equipment rooms at the locations housing LAN equipment outside City Hall.	√ ISS met with representatives from departments that house equipment, and it was determined that 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.	√ The departments are responsible for strengthening the physical security at their locations. ISS is providing consulting expertise to make sure the rooms are properly secure. All but three departments sent ISS a plan of action regarding how they were going to address the physical security weaknesses.
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, and ⇒ Monitoring the length of time the equipment is stored by ISS to provide for timely installation of equipment.	√ Interim manual procedures were put in place until the PeopleSoft Financials system was put in place. A new business process was put in place when the PeopleSoft Financials system was implemented in July 2001. The ISS Lockup Room now only stores computer equipment ordered by ISS for its own use. Departments now order and receive computer equipment and are responsible for obtaining a FARR tag for capital items. Then, the department submits a request to ISS to install the computer equipment. The ISS inventory unit in PeopleSoft only contains inventory in the ISS department.

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
- ♦ In progress, partially completed

Summary

As noted in Table 1 above, ISS has completed four of the nine due action plan tasks, partially completed three action plan tasks, and has amended the expected completion date of the remaining two tasks.

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

Appointed Official Response

City Manager Response:

I appreciate the follow-up by Auditing staff on the important issue of security of the City's information technology infrastructure. I would like to commend ISS staff for the progress they have made on the action plans. Training has occurred, interim procedures developed, and new business processes put into place. I also want to thank City staff in all departments for their cooperation with Auditing staff and ISS to strengthen the physical safety of our technology resources at their locations.

Copies of this 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