Audit Follow Up

As of March 31, 2002

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 #0222 *June 10, 2002*

Summary

Information Systems Services (ISS) has completed 8 of the 13 (62%) action plan tasks due as of March 31, 2002. The outstanding tasks are contingent upon obtaining management's approval of the information security policies, completing the backup software implementation, and obtaining funding to strengthen 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.

While we were conducting our follow-up procedures, we noted two additional related issues that were not discussed in the original audit report (#0106). First, there were three terminated employees that still had physical access to ISS computer rooms. Upon notification, ISS immediately removed their access and implemented a process to regularly identify terminated employees and remove their access to computer rooms. Second, related to backup and recovery, we noted that there was not a documented risk-based process to determine what City systems were included in the ISS disaster recovery plan. The ISS Director has indicated that he will address this issue during the next ISS Steering Committee meeting.

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 #0222

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 March 31, 2002. To obtain information, we conducted interviews with key department staff, inquired regarding the status

and/or visited 30 of the identified 38 locations housing computer LAN equipment, 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 (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;
- 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 of March 31, 2002, all action plan tasks identified in the original audit report were due to be completed. Table 1 shows the status of these tasks.

Table 1

Summary of Tasks as of March 31, 2002		
# Tasks Due	# Tasks Completed	# Tasks Behind Schedule
13	8 (62%)	5

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 approach has alleviated the need for a position.
• 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. Audit Comment: The proposed draft addresses physical access to the location housing computer and telecommunications equipment but does not provide suggested controls or minimum guidelines. In addition, the physical security section does not address environmental conditions, such as fire/smoke/water detection, air cooling, dust and dirt, etc.
• Obtain management approval of the policies and procedures, including: ISS, executive team, and the City Manager.	♦ As of March 31, 2002, the draft policies had been provided to ISS, the Executive Team and Leadership Team for feedback. The policies have not yet been approved or implemented.
• Identify and obtain funding to implement security requirements per the approved information security policy.	ISS has identified criteria and processes that will take funding to implement. ISS will have to wait for the security policies to be approved.

• Implement approved policies and procedures within ISS and affected departments, including policy distribution and training.	♦ Partially completed. The security policy has been written and reviewed and implemented in ISS. The Executive Team has reviewed and approved the policies and procedures in concept. The implementation to other departments, training, and distribution depend on approval date of policies.
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.	♦ Partially completed. ISS currently has backup procedures in place, but these procedure are changing due to new implementation of Veritas software. ISS is currently in the final debugging stage on Veritas implementation. Application overview and run documentation will be prepared and application will be "operational" once debugging is complete. Veritas replaces all other server backup applications.
• Identify resources, including funding and personnel, to implement approved backup policy and procedures.	√ ISS has purchased new backup software and designated the staff in ISS responsible for determining what is backed up, how often, and by whom.
• 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.	√ ISS has determined who is responsible for ensuring that backups are completed for each operational area.
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 policy and procedures.	♦ Partially completed. Our inquiries of the status of 30 of the 38 locations housing LAN equipment indicated that 50% of the locations had made some improvement, and 50% had not made any improvement since September 2001. Therefore, there are not adequate physical controls at many of the locations housing LAN equipment. Funding for improvements was designated to come from ISS Network upgrade projects; but per management, there are other higher priority projects that need to be funded before the physical security upgrades.

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 ♦ In progress

Summary of Action Plan Steps

As noted in Table 1 above, ISS has completed 8 of the 13 (62%) due action plan tasks. The outstanding tasks are contingent upon obtaining management's approval of the information security policies, completing the backup software implementation, and obtaining funding to strengthen the physical security controls at locations housing computer LAN equipment.

Other Related Issues

While conducting our follow-up audit procedures, we reviewed security access listing reports to identify who was allowed access into the ISS computer rooms. We noted that three terminated employees still had physical access into computer rooms (two into the main computer room, and one into the ISS training facility). Upon notification, ISS immediately removed their access and implemented a process to regularly identify terminated employees and remove their access to computer rooms.

Also, we inquired about the backup processes and disaster recovery planning. We noted ISS disaster recovery procedures address only three City systems, Financials, Human Resources, and Customer Information System. There does not appear to be a documented risk assessment to determine what City systems are critical and should be included in the City's disaster recovery planning. The ISS Director has indicated that he will address this issue during the next ISS Steering Committee meeting.

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

Appointed Official Response

City Manager Response:

The tragic events of September 11, 2001 have certainly heightened our awareness to protect and secure the physical and logical data assets of the City of Tallahassee. The protection from cyber terrorism will save the City time, money, and resources. There has been tremendous progress made in addressing some of the initial action plans and plans are in place to complete all of the action plans documented. I would like to thank Auditing and DMA/ISS for their work in this effort.

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