Audit Follow Up

As of September 30, 2002

CITY OF TALLAHASSEE

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

# "Audit of the Logical Security of the City's Local Area Network"

### (Report #0201, Issued October 26, 2001)

Report #0305 December 12, 2002

## Summary

**City management has completed 12 of the 20 action steps due (60%) and 8 tasks are behind schedule, 5 of which have been partially completed.**

In audit report #0201, issued October 2001, we identified some areas in which logical security needed to be improved to adequately protect the City's information technology resources. This also included the protection of confidential data, as defined in Chapter 119.07, Florida Statutes.

The City relies on computers and electronic data to perform functions that are necessary to provide services to the citizens of Tallahassee. Examples of these services include: police and fire dispatching and reporting; electric, water, gas and solid waste operations; public works operations (traffic, streets and drainage); growth management and permitting; bus operations; and financial reporting.

As the City changes from a centralized mainframe environment to a distributed client/server environment, there are increased access paths into the computers and systems. Logical access into the City's local area network (LAN), and areas within, must be limited to only authorized users with legitimate business purposes. Access paths into the LAN include:

- direct login from employee workstations in City Hall;
- remote login from employee workstations at other City buildings via fiber, etc.;
- remote login via modems; and
- Internet.

There are also logical access layers that must be protected at each layer. These layers, from external to internal, are: remote, network, operating system, database, and application.

## Scope, Objectives, and Methodology

### Report #0201

The scope of report #0201 was to evaluate the logical security controls protecting the City's local area network (LAN) resources. Fieldwork took place from December 2000 through June 2001.

The primary objectives of the audit were to:

- ♦ obtain a general understanding of the network operations and the logical access paths into the network;
- ♦ provide assurances regarding security controls management believed were in place;
- ♦ evaluate the adequacy of security controls that management believed should be improved;
- ♦ determine the adequacy of policies and procedures related to unauthorized access into the City's LAN;
- ♦ determine the adequacy of the controls in place to prevent unauthorized access in the City's LAN; and

- determine the accessibility to confidential information stored on the City's LAN.

The scope of this audit was limited in that our audit procedures: 1) included basic, but not extensive, vulnerability assessment activities (to identify potential access weaknesses) but no penetration testing (to obtain unauthorized access); and 2) did not include detailed database security testing.

### *Report #0305*

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, 2002. To obtain information, we conducted interviews with key department staff, attended meetings, reviewed relevant documentation, and performed testing to ensure selected controls put in place were working effectively. This follow up report was conducted in accordance with Generally Accepted Government Auditing Standards and Standards for the Professional Practice of Internal Auditing, as appropriate.

## *Previous Conditions and Current Status*

In report #0201, the action plan identified four main areas, each with specific action steps (20 steps in total) that need to be addressed. These included:

- Policies and Procedures, including developing written information security policies and procedures and providing training to City employees.
- Management and Monitoring, including designating an information security group to implement and monitor security activities; and periodically contracting with outside vendors to assess the City's information security infrastructure.
- User access controls, including developing and implementing adequate user access procedures; conducting a vulnerability assessment and implementing recommendations; limiting the number of users with privileged access capabilities; identifying all modems on the network; and implementing controls so unauthorized users cannot access the network remotely.
- Protection of confidential information, including establishing processes within departments to adequately protect data defined as exempt from public records from unauthorized access and inadvertent disclosure.

As of September 30, 2002, 12 of the 20 action steps due were completed (60%) and 8 tasks are behind schedule, 5 of which have been partially 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 |
| 20 | 12 (60%) | 8 |

## Table 1
## Previous Conditions Identified in Report #0201 and Current Status

| Previous Conditions | Current Status |
|---|---|
| **Policies and Procedures** | |
| • Provide draft security policies to a City employee committee for review and incorporate appropriate feedback into the draft document. | √ Completed in a prior period. |
| • Provide draft security policies to City management, including City Attorney's Office, Treasurer-Clerk's Office, Human Resources, for feedback and to ensure the proper process is followed. | √ Completed in a prior period. |
| • Present final draft security policies to City management, including Executive Team, Appointed Officials, and other appropriate persons as determined for feedback. | √ A presentation was made to the City management, including the Executive Team, Appointed Officials, and the Leadership Team on July 10, 2002. No changes to the policies were requested of ISS. |
| • Identify the appropriate City staff to provide training to all City employees as to the security policy detail. | ★ Partially completed. ISS Distributed Network Services will provide training to all City staff over the next year. Use of video on Citynet (the City's Intranet) will also be used so that every employee has the opportunity to take this training. Estimated completion date amended to October 3, 2003. |
| **Management and Monitoring** | |
| • Designate an information security group to consist of various information security related positions, such as: technology infrastructure administrator, database administrator, computer operations and customer service supervisor, and mission-critical application security administrators. | √ Group was identified in February 2002, and the first meeting was held in October 2002.<br>Audit Comment: The Senior IT Auditor in the Office of the City Auditor will be included as an advisory member of this committee. |

| | |
|---|---|
| • Information security group is to develop standard operating procedures for implementing security activities, such as: coordinating and conducting information security awareness training for employees; routinely monitoring security activities, such as suspected or actual security breaches; recording, tracking, and analyzing suspected and actual information security incidents; and assisting department-owners in assessing the confidentiality and security requirements of their data (also called assessing risks). | o Director of ISS met with the above identified information security group in October 2002 to go over expectations of the security group. Estimated completion date was amended to March 31, 2003.<br>Audit Comment: As noted above, the Senior IT Auditor will be included as an advisory member of this committee. |
| • Contract to have a vulnerability assessment of current City network infrastructure performed to identify all potential areas of weakness. | √ First assessment was conducted during Fall 2001. |
| • Periodically contract with an outside vendor to assess the City's information security infrastructure. | √ There have been two re-assessments conducted since the first report. |
| • Implement recommendations from the vulnerability assessment results. | ★ Partially completed. Of the 17 recommendations, 7 have been implemented and the remaining are scheduled to be completed in 2003. |
| • Perform post review after implementation of the recommendations. | √ ISS has contracted to have two quarterly external re-assessments conducted and plans to contract for an annual internal re-assessment. |
| **User Access Controls** | |
| • Develop standard operating procedures in Information Systems Services (ISS) Distributed Network Systems for staff to understand the processes needed to be in place regarding how to add, change, transfer, and delete user access. In addition, ISS management should include periodic monitoring procedures to ensure that the controls are in place. | ★ Partially completed. ISS has developed and implemented written procedures to add, change, and transfer user access to the network. These procedures still need to be enhanced to include periodic monitoring procedures to ensure controls are in place.<br>Audit Comment: We tested 71 terminated employees to determine whether they had access on the network and found that 9 (13%) still had access. ISS management will need to conduct periodic monitoring to ensure the user access controls are working effectively. |

| | |
|---|---|
| • Identify and determine the functionality of all modems operating in the City, and implement adequate controls to ensure that the network cannot be accessed without proper authentication. | ○ Not completed. Estimated completion date has been amended to March 31, 2003. |
| **Protection of Confidential Data** | |
| • Police security administrators need to develop and implement a process to perform periodic reviews of the user IDs in their systems. | √ Completed in a prior period. |
| • Police Department should examine the use of shared passwords and determine how best to adequately protect their data. | √ Completed in a prior period. |
| • Fire Department is to develop and implement procedures to inform the CAD/RMS security administrator when employees terminate from the Fire Department. | √ Completed in a prior period. |
| • In the Human Resource Management System (HRMS), a consistent use of the "public record" indicator should be implemented, and staff should be notified and trained as needed. | √ Completed in a prior period. |
| • Customer Information System (CIS) –<br>1. CIS project team should design and implement a method to identify a customer as being exempt from public records in the new CIS.<br>2. All exempt employees should be identified in the CIS, and staff should be notified and trained regarding how the indicator is to be utilized. | ○ Not completed. Estimated completion date had been amended to December 31, 2002.<br>Currently, a manual process is in place to monitor customers that are exempt from public disclosure. The new CIS system went into production in October 2002. ISS staff are planning to work with user departments to create an alert to identify accounts with protected status.<br><u>Audit Comment</u>: There are associated risks with this manual process and the use of a text-based Alert field. The risks have been communicated to the CIS project team and executive steering committee. |
| • Energy Loan Database – Energy Services management is to explore options and implement a process to identify which records in the database are exempt from public records to minimize the risk that personal information for exempt employees is improperly disclosed. | √ Completed in a prior period. |

| | |
|---|---|
| • Research to identify the best encryption software that could be used by any City employee to encrypt e-mail messages and attachments when transmitting confidential information. Roll out the use of the encryption software to those departments with the greatest need, and train staff as needed. | ★ Partially completed. ISS has researched and identified the encryption software they intend to use for both server files and e-mail. Funding will be used from the Network Upgrade projects to procure the software. The estimated completion date has been revised to December 31, 2002. |
| • Growth Management and City/County GIS – staff need to remove personal information for exempt employees from their Internet site and determine a method for identifying a record as exempt. Steps include:<br>a. A subcommittee of the Permit Tracking System (PETS) inter-local steering committee is to identify options to identify records that should be exempt from public records in the PETS systems.<br>b. The PETS inter-local steering committee will evaluate and then select the most cost efficient and least work-intensive option to implement.<br>c. PETS technical staff will design and implement the approved method and develop a process to periodically verify that the records that should be protected are identified. | ★ Partially completed. The PETS Technical Committee has proposed a solution to the GIS Steering Committee in their November 2002 meeting, and they will examine the legal implications of the proposed solution. Estimated completion date has been amended to March 31, 2003. |

**Table Legend:**

• Issue addressed in the original audit

✓ Issue has been resolved
★ Partially completed, completion date has been amended
o Behind schedule, completion date has been amended

## Summary

As noted in Table 1 above, various City departments have completed 12 of the 20 action plan tasks due, and 8 tasks are behind schedule, 5 of which are partially completed.

Outstanding actions include: implementing solutions in two computer systems (CIS and PETS) to protect confidential information defined as exempt from public records per Chapter 119, Florida Statutes; and addressing the issue of unidentified modems connected to the City's LAN.

In addition, during our testing of user passwords, we noted that there were several user IDs that had passwords that were set not to expire. These user IDs included employees from executive management, Growth Management, Police Department, Gas Utilities, and Electric Utilities. We recommend that all users be required to periodically change their passwords to minimize the risk that users' passwords can be compromised and be used in an unauthorized manner, and exceptions should be noted and minimized as much as possible.

One of the actions that ISS is considering is to associate employee IDs with user names in the password management software. This would provide a tool for system administrators and help desk personnel to ensure that only active employees have active user IDs on the network and in their systems. We encourage ISS to implement this control.

We appreciate the assistance provided by staff in Information Systems Services and other affected City departments 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 (#0305) or audit report #0201 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