# Audit Follow Up

**As of March 31, 2002**

CITY OF TALLAHASSEE

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

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

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

***Report #0223*** ***June 10, 2002***

## Summary

***City management has completed nine of the thirteen due action plan tasks and four tasks are behind schedule, two 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) and no penetration testing (to obtain unauthorized access); and 2) did not include detailed database security testing.

### *Report #0223*

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, 2002. To obtain information, we conducted interviews with key department staff, attended meetings, reviewed relevant documentation, and visited selected sites to observe

any improvements implemented. 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 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 March 31, 2002, nine of the thirteen due action steps were completed (69%) and four tasks are behind schedule, two of which have been partially completed. Table 1 provides a summary (by main area) of each action plan step and the status.

**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. | √ Draft policies were distributed and management input requested and received. |
| • 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. | √ Draft policies were distributed and management input requested and received. |
| **Management and Monitoring** | |
| • 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. | √ First assessment was conducted during Fall 2001. |
| **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, it will include periodic monitoring procedures to ensure that the controls are in place. | ♦ Partially complete. ISS has implemented operating processes to add, change, and transfer user access to the network, but these have not been developed into written procedures. Estimated completion date has been revised to August 31, 2002. |

| | |
|---|---|
| • 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. | o Not completed. Estimated completion date has been amended to November 30, 2002. |
| **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. | √ The Police Technical Services Division has implemented processes to ensure the removal of all terminated employees from their data systems in a timely manner. |
| • Police Department should examine the use of shared passwords and determine a way to adequately protect their data. | √ The Police Technical Services Division has completed an initial review of shared user IDs and passwords and is implementing procedures to limit their use and implement compensating controls to reduce the associated risks. Such controls include: ensuring that the locations where shared user IDs and passwords are used are physically secure; limiting the user ID to a specific workstation; and limiting the network resources that can be accessed from that workstation. |
| • Fire Department is to develop and implement procedures to inform the CAD/RMS security administrator when employees terminate from the Fire Department. | √ The Fire Department implemented a process to notify the Police Technical Services Division and ISS when an employee leaves the department and have their access removed in a timely manner. |
| • 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. | √ The Retirement Division, Treasurer-Clerk's Office, identified and marked all retirees in the HRMS system that should be exempt from public records and provided training to all staff. |
| • 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. | o Not completed. Estimated completion date has been amended to December 31, 2002.<br>The CIS exemption from public records request targets City staff that qualify for the exemption along with other eligible utility customers (non-City employees) who request an exemption. City employees who are flagged in HRMS/Payroll as protected have been notified in an effort to identify those who utilize COT utilities. An Excel database has been created, and is being maintained, of all eligible customers who have responded. The database is being used to filter them from any public records request. After CIS goes into production, an alert will be created to identify accounts with protected status.<br>Audit Comment: There are associated risks with the use of the Alert field which could result in improper disclosure of customer information that is exempt from public records. The risks have been communicated to the CIS project team and steering committee. |

| | |
|---|---|
| • Energy Loan Database – Energy Services management is to explore options and implement a process to identify which records are exempt from public records in the database to minimize the risk that personal information for exempt employees is improperly disclosed. | √ Energy Services implemented a procedure to identify records as exempt from public records and informed staff and other users about the indicator and its purpose. |
| • 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 complete. ISS has researched and identified the encryption software they intend to use for both server files and e-mail. There is no existing funding available. The estimated completion date has been revised to December 31, 2002. |

**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 nine of the thirteen due action plan tasks, and four tasks are behind schedule, two of which are partially completed.

Other actions have been implemented to further protect confidential information defined as exempt from public records per Chapter 119, Florida Statutes, including: Human Resources has made forms available to employees on their internal web site; and Fire Department has joined the Police Department in providing their staff information and forms regarding the information that can be protected on the Leon County Property Appraiser's web site.

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 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 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 #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