Final Audit Follow Up

As of March 31, 2007

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

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

"Inquiry into the February 2005 Network Computer Virus"

(Report #0523, Issued June 3, 2005)

Report #0715 **May 22, 2007**

Summary

This is the final follow up on the previously issued audit report #0523, Inquiry into The February 2005 Network Computer Virus. In that report we identified issues that indicated a need to better prepare for and protect the City's computer systems from computer viruses. Those issues related to staffing levels for emergencies, communication methods when e-mail is unavailable, segmentation of the City's computer network, installation of security updates, and citywide knowledge and awareness of computer security. We made specific recommendations to address those issues.

The City's Information System Services (ISS) has completed all but one of the six action plan steps developed to address our recommendations. The steps completed include:

- Identification of City employees, outside ISS, with skills that can be utilized to augment ISS staff during emergencies;
- Development of an alternative means of disseminating information to employees when e-mail is unavailable;
- Development and implementation of a plan to test security updates prior to installation;
- Installation of security updates in a timely manner, after testing; and
- Development and implementation of plans to increase the awareness of the importance of personal computer (PC) security.

The one outstanding item, relating to the segmentation of the City's computer network, is substantially complete. The necessary network infrastructure has been acquired and installed. The final steps in segmenting the network relate to resolving computer configuration issues and conducting the "changeover" to the segmented network. Management expects to complete the network segmentation prior to September 30, 2007. As this is the final follow up, the completion of this action plan step has been turned over to management for final resolution.

Scope, Objectives, and Methodology

The original audit and this subsequent follow up were conducted in accordance with Generally Accepted Government Auditing Standards and Standards for the Professional Practice of Internal Auditing, as appropriate. This follow up audit was for the period June 5, 2005, through March 31, 2007.

Report #0523

On February 14, 2005, the City noted that its computer network was not functioning properly. What was first believed to be a network hardware malfunction was subsequently determined to be a computer virus that had infected the City network.

The scope of report #0523 included a review of activities performed by ISS during the period February 14, 2005, through March 31, 2005, and other departments during the period February 14 - 25, 2005, to address the virus infection. The objective of the report was to answer the following questions:

1. How was the virus detected, identified, and eradicated?
2. What were the impacts of the virus to the City (i.e., financial, customer service, data integrity)?
3. How was the City infected with the virus?
4. Was the infection preventable?
5. What are the lessons learned from this experience?

The audit concluded that virus infections are common occurrences for everyone and every business that has computers, networks, and Internet connectivity. The key is to have preventative measures in place to minimize the impact of an infection and have adequate plans in place to reestablish business operations quickly.

City departments learned many lessons during the virus infection. ISS management identified areas that needed to be addressed. Additionally, recommendations were made toward reducing the impact of future virus infections and expediting departments' reestablishment of business operations.

Report #0715

This is our second and final follow up on action plan steps identified in audit report #0523. In our first follow up we reported on progress and efforts to implement action plan steps due as of March 31, 2006. The purpose of this final follow up is to report on the progress and status of efforts to complete action plan steps due for completion through March 31, 2007. To obtain information we conducted interviews with key staff, made observations, and reviewed relevant documentation.

Previous Conditions and Current Status

In report #0523, ISS management and City Auditor staff identified several areas that if addressed, would decrease (but not eliminate) the likelihood of future virus infections and reduce the impact of infections when they do occur. The areas identified included:

- Increasing the number and expertise of ISS staff;
- Improving communication;
- Implementing network segmentation;
- Installing operating system updates in a timely manner;
- Implementing automated virus scanning;
- Providing computer security training for users and ISS staff; and
- Improving business continuity planning throughout all City departments.

A total of six action plan steps were developed to address the areas identified. Of those six steps, five have been completed and one has been substantially completed and is being turned over to management for final resolution. Table 1 provides a summary of all action steps and their current status.

Table 1
Information System Services Action Plan Steps from Report #0523 due as of March 31, 2007, and Current Status

Action Plan Steps	Current Status
To ensure adequate staffing during times of emergencies	
• Identify employees in departments other than ISS, from across the City, with strong computer skills, knowledge, and abilities that can be called upon to augment ISS staff in times of emergencies.	✓ A list of employees with strong computer skills, knowledge, and abilities and their contact information has been developed to assist ISS in contacting and recruiting additional staff when needed to address emergency-type situations. This step was completed in a prior period.
To develop an alternative means of communicating and disseminating information when e-mail is unavailable	
• Identify or develop an alternative means of communicating important information throughout the City for use when e-mail is no longer available.	✓ The City's telephone system has been identified as the alternative method of disseminating information when e-mail is unavailable. The recent upgrade to the City's telephone system allows voice mail messages to be transmitted to multiple extensions at one time. This step was completed in a prior period.
To complete the segmentation of the City's computer network	
• Continue and complete the process of segmenting the City's computer network.	✳ This step has been substantially completed. The hardware needed to support the segmentation of the network has been acquired and installed. When the first segment of the network was activated, issues with the configuration of the involved computers arose and the project was suspended until those issues could be resolved. ISS believes those issues have been resolved and anticipates completing the segmentation of the computer network by September 30, 2007. This step has been turned over to management for final resolution.
To ensure that operating system and application updates are installed and do not impact critical applications	
• Develop and implement a plan to test operating system and application security updates prior to installation.	✓ A plan to identify, obtain, and test system and application security updates has been developed and implemented.
• Install operating and application security updates within a reasonable time frame after completion of testing.	✓ The process in place for the installation of security updates is such that most updates are to be identified and installed on a monthly basis, with critical updates being installed more frequently (on an as needed basis).

To improve computer security knowledge and awareness for both ISS staff and other computer users throughout the City	
• Complete development and implementation of plans to increase the awareness of the importance of PC level security.	✓ An on-line course to inform and educate City employee computer users about PC security was developed. The City's Chief Information Officer is in the process of briefing the City's department directors as to the course and asking the directors to ensure all their employees take the on-line training. This step was completed in a prior period.
Table Legend:	
• Issue addressed in the original audit.	✓ Issue addressed and resolved.
	✳ This step is substantially complete and is being turned over to management for final resolution.

Conclusion

ISS has completed five of the six action plan steps developed in response to the recommendations made in audit report #0523. The sixth action plan step is substantially complete and is being turned over to management for final resolution.

We commend ISS for their efforts and results in addressing the issues and completing the action plan steps that arose from the initial audit.

Appointed Official's Response

City Manager:
The ability to ensure that the City's network is safe and secure from virus attack is certainly a priority and I appreciate the follow up by Auditing staff. I am pleased that most of the action plans are completed. I would like to thank Auditing and DMA/ISS for their work in this effort.

Copies of this final audit follow up #0715 or audit report #0523 may be obtained from the City Auditor's website (http://talgov.com/auditing/index.cfm) via request by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

Final audit follow up conducted by:
Dennis Sutton, CPA, CIA, Senior IT Auditor
Sam M. McCall, CPA, CGFM, CIA, CGAP, City Auditor