Audit Follow Up

As of September 30, 2006

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 #0709 **January 12, 2007**

Summary

This is the second follow up on audit report #0523, Inquiry into The February 2005 Network Computer Virus. In that report, we made six recommendations designed to improve the City's defenses against computer viruses and minimize recovery time when infections occur. As reported in the first follow-up, the City's Information System Services (ISS) completed three of the five action plan steps due, and amended the completion date of the two steps that were not completed. At that time, ISS also amended the completion date of the one step that was not due to coincide with the other amended completion dates. The steps completed to date include:

- identification of City employees, outside ISS, with computer skills to augment ISS staff during emergencies;
- development of an alternative means of disseminating information to employees when e-mail is unavailable; and
- development and implementation of plans to increase the awareness of the importance of personal computer (PC) security.

The steps from the audit that have not been completed relate to: (1) identification, and testing of operating system and application security updates, (2) installation of those operating and application security updates in a timely manner, and (3) segmentation of the City's network, which should help protect against the spread of infections when they occur. The completion dates for these steps was amended to March 31, 2007.

During this follow-up, the Office of the City Auditor became aware that a computer virus had again infected the City's computing environment. This virus, while not as damaging as the February 2005 infection, caused a major disruption in the City's computing environment. The final impact to the City's operations has not been determined as the effects are still being addressed. We recommend that ISS complete the outstanding action plan steps so that future infections will be minimized.

Scope, Objectives, and Methodology

The 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.

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 keys to addressing risks related to virus infections include having: (1) preventative measures in place to reduce the chances of infections and minimize the impact of an infections and (2) adequate plans in place to recover from and reestablish business operations quickly when infections occur.

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 #0709

This is the second follow up on the progress and efforts of ISS to implement the action plan steps identified in audit report #0523. It covers the period March 31, 2006, through September 30, 2006.

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, three were completed as of March 31, 2006. ISS requested that the target completion date for the remaining three action plan steps be amended to March 31, 2007. Table 1 provides a summary of all action steps and their current status. While there were no action plan steps due at this time we followed-up on this audit because of the importance of the subject and the potential impact to City operations.

Table 1
Information System Services Action Plan Steps from Report #0523 due as of September 30, 2006, 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.	✓ This step was completed in the first follow up period. A list of employees with strong computer skills, knowledge, and abilities and their contact information was developed to assist ISS in contacting and recruiting additional staff when needed to address emergency-type situations.

<table>
<tr><td colspan="2"><i>To develop an alternative means of communicating and disseminating information when e-mail is unavailable.</i></td></tr>
<tr><td>• Identify or develop an alternative means of communicating important information throughout the City for use when e-mail is no longer available.</td><td>✓ This step was completed in the first follow up period. The City’s telephone system has been identified as the alternative method of disseminating information when e-mail is unavailable. It has the ability to send voice mail messages to multiple extensions at one time. Minimal testing has been conducted to ensure this process will function as intended when needed.</td></tr>
<tr><td colspan="2"><i>To complete the segmentation of the City’s computer network</i></td></tr>
<tr><td>• Continue and complete the process of segmenting the City’s computer network.</td><td>◊ As noted in the first follow up report, ISS amended the completion date from June 30, 2006, to March 31, 2007. The completion of this step was delayed due to problems encountered in selection of and contracting with a vendor to provide equipment and resources for the upgrade of the City’s computer network infrastructure. Without adequate segmentation of the City’s computer network there is the potential that virus infections could spread throughout the City faster than ISS can react to limit the impact.</td></tr>
<tr><td colspan="2"><i>To ensure that operating system and application updates are installed and do not impact critical applications.</i></td></tr>
<tr><td>• Develop and implement a plan to test operating system and application security updates prior to installation.</td><td>◊ ISS requested that the final completion date for this action plan step be amended from September 30, 2006, to March 31, 2007. Progress has been made on the completion of this step. Plans have been established and documented for the testing of updates to applications. However, plans for testing updates to operating systems have not been finalized or implemented. Until implemented, the City’s computer network is at a greater risk of being infected and negatively impacted by computer viruses.</td></tr>
<tr><td>• Install operating and application security updates within a reasonable time frame after completion of testing.</td><td>◊ The completion of this action plan step is dependent on the completion of the previous step, relating to the development and implementation of plans for the testing of security updates prior to installation. Therefore the completion of this step has also been amended from September 30, 2006, to March 31, 2007. To test the current status of updates for desktop computers we judgmentally selected and examined a computer to determine the status of operating system updates. Our examination showed that the most recent updates were installed in January 2006 although Microsoft has released security updates every month since that time. Therefore, if every security update was deemed necessary, the City’s desktop computers would be eight months behind on security updates.</td></tr>
</table>

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.	✓ This action plan step was completed in the prior period. An on-line course to inform and educate City employee computer users about PC security was developed and implemented. All City employees are required to take and successfully complete the on-line training.

Table Legend:

● Issue addressed in the original audit	✓ Issue addressed and resolved	◊ Amended completion date

Conclusion

Of the six action plan steps identified in the audit, ISS completed three steps, and amended the completion date of the remaining three steps from June 30, and September 30, 2006, to March 31, 2007. The completion date of those steps was amended as part of the last follow up.

During this follow up, the City Auditor's Office became aware that the City had been infected with another virus. This infection, while not as destructive as the February 2005 virus, still caused disruption in the City's computer environment. The final impact of this infection has not been determined as the effects are still being identified and resolved. We recommend that ISS complete the outstanding action plan steps as soon as possible in order to minimize the impact of future virus infections.

We appreciate the cooperation and assistance of the Information Systems Services provided in this audit follow up.

Appointed Official Response

City Manager:

The ability to ensure that the City's network is safe and secure from attack is certainly a priority and I appreciate the follow up by Auditing staff. The virus certainly impacted our work processes and plans are in place to complete all of the action items documented in this report by the end of March 2007. I would like to thank Auditing and DMA/ISS for their work in this effort.

Copies of this Audit Follow Up or Audit Report #0523 may be obtained from the City Auditor's website (http://talgov.com/auditing/index.cfm), 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).

Audit Follow Up conducted by:
Dennis Sutton, CPA, CIA, Sr. IT Auditor
Sam M. McCall, CPA, CGFM, CIA, CGAP, City Auditor