



CITY OF ORLANDO

Office of Audit Services and Management Support

MEMORANDUM

To: Conrad C. Cross, Chief Information Officer

From: J. T. Sirak, CPA, Director
Office of Audit Services and Management Support

Re: Follow-Up Review of the Audit of Information Systems General Controls
(Report No. 09-06)

Date: May 22, 2009

Attached is a summary of the status of recommendations as determined from our follow-up review of the Audit of Information Systems General Controls (*Report No. 08-10*), issued May 23, 2008. Our review procedures consisted of a review of the status of the recommendations provided by the Technology Management Division, inquiries of management, and examination of certain documents.

Our follow-up was made in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

The Technology Management Division did not concur with three of the original twenty-six recommendations; of the remaining twenty-three recommendations, ten have been implemented, ten have been partially implemented and three are planned for implementation. Five of the partially implemented recommendations concern updating procedures that are expected to be implemented by September 2009 and four recommendations involve software acquisition and/or installation which are being impacted by costs and timing; the remaining recommendation, concerning documentation for the computer environment, is being addressed but not yet completed. The three recommendations planned for implementation are designed to enhance security and are presently pending funding approval.

We would like to thank the officials and personnel of Technology Management affected by these recommendations for their cooperation during this follow-up review.

Attachment

c: Honorable Buddy Dyer, Mayor
Byron W. Brooks, Chief Administrative Officer
Mayanne Downs, City Attorney
Rebecca W. Sutton, Chief Financial Officer
Jody M. Litchford, Deputy City Attorney
Raymond M. Elwell, Deputy CFO

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|----|---|--------------------------|-----------------------|---------------------|--|
| | The Technology Management Division (TMD) should: | | | | |
| 1. | Evaluate the exceptions noted from the audit of the <i>proposed</i> Information Technology Security policies and improve the policies as appropriate. (LOW) | Concur | Partially Implemented | September 30, 2009 | Updated Information Security policies have been delivered to the Executive Management for approval. |
| 2. | Evaluate the exceptions noted regarding the <i>existing</i> City Policies and Procedures for the division and improve policies as noted in the report. (MEDIUM) | Concur with Reservations | Partially Implemented | September 30, 2009 | Updated Technology management Division policies have been delivered to the Executive Management for approval. |
| 3. | Develop and implement a Security Incident Response Policy to govern all actions in the event of a suspicion of a security incident, not only on confirmed cases of successful attacks by malicious users. (MEDIUM) | Partially Concur | Partially Implemented | September 30, 2009 | Internal procedures were updated. All Internal policies and procedures will be posted on an internal site accessible by Division personnel. |
| 4. | Develop and implement an Employee Termination Notification Policy to: define appropriate notification procedures in the event of different circumstances that can surround an employee's dismissal; and emphasize the need to timely notify appropriate Security Administrators to make sure employees privileges on the City's network are terminated no later than the last day of employment. (HIGH) | Concur with Reservations | Implemented | November 2008 | Complete procedures were developed, documented, and implemented. Process was reviewed and approved by the Human Resources and the City Legal team. |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|----|--|--------------------------|-----------------------|------------------------------|--|
| 5. | Develop Information Security policies that explicitly govern or define appropriate uses of portable electronics (PDAs, Blackberries, etc.). (MEDIUM) | Concur with Reservations | Partially Implemented | September 30, 2009 | Updated Information Security policies have been delivered to the Executive Management for approval. |
| 6. | Implement a policy restricting connecting any wireless access points to the network without direct involvement and approval from TMD and enforce this policy by conducting periodic wireless site surveys, and identifying and disconnecting any rogue wireless access points that are connected to the City's network. (MEDIUM) | Concur | Implemented | August 2008 | Current Policy 754.9 addresses IT Controls recommendation. Regular periodic wireless site survey processes to identifying and disconnecting any rogue wireless access points have been implemented. Additional wireless tools are being reviewed |
| 7. | Implement a policy requiring all vendors with privileged access to any part of the City's computer system or sensitive data to undergo and present the results of a SAS-70 Audit. (LOW) | Do Not Concur | | | TM has engaged the Purchasing Division and made the recommendation to include SAS-70 requirements in the purchasing process. |
| 8. | Improve security over the City's Wireless Local Area Network (WLAN) through the following actions: <ul style="list-style-type: none"> • Create a portal to notify users of the effective Internet use policy and require users to indicate acknowledgement and acceptance before being allowed access. | Concur with Reservations | Partially Implemented | August 2008 – September 2009 | This is Staged, and will be implemented pending Legal approval of the proposed notification. Quotes for VPN equivalent |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|----|---|----------|----------------|---------------------|---|
| | <ul style="list-style-type: none"> • Implement an additional access control such as a Virtual Private Network if access is required to any of the systems on the inside of City's trusted network. • Implement a practice of performing wireless site testing to gather and test configurations of each access point, and compare the data with the list of known wireless access points and expected configuration settings. • Disable the broadcasting of the employee-only network's unique identifier (service set identifier or SSID) on all wireless access points. (MEDIUM) | | | | <p>access have been received and currently being reviewed.</p> <p>Schedule wireless site survey audit and monitoring to identifying and disconnecting any rogue wireless access points have been implemented.</p> <p>At this time, SSID will not be disabled due to business requirements</p> |
| 9. | <p>Increase the overall security of the City's network devices through the following actions:</p> <ul style="list-style-type: none"> • Restrict access to network device's management interface to only authorized users. | Concur | Implemented | August 2008 | <p>As of August 2008 restricted access issues have been addressed. The remaining equipment will be addressed with the implementation of new equipment that supports the function.</p> |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|--|--------------------------|-----------------------|---------------------|---|
| | <ul style="list-style-type: none"> • Change all vendor configured usernames and passwords, and where possible, create individual usernames for each employee who is authorized to change network configurations. • Discontinue using unencrypted network protocols for configuring network devices and use more secure protocols. (HIGH) | | | | <p>Individual usernames for each employee has been created. All vendor usernames and passwords have been changed.</p> <p>SSH access has been enabled on all but a few routers. Routers not currently configured will be addressed by retiring the routers and implementing new supported routers.</p> |
| 10. | Establish a policy and a technology to require and implement mandatory Hard Disk Drive (HDD) encryption for all laptops. (MEDIUM) | Concur with Reservations | Partially Implemented | September 30, 2009 | Technology Management has received HDD encryption quotes and is reviewing cost and the potential impact to business operations. Specific Department policies dictate no compliance data be maintained on the hard drive therefore no encryption is necessary. Further investigation is required. |
| 11. | Strengthen network printer security by reconfiguring the network access controls to restrict access to printer network interfaces to print servers and TMD personnel only. (LOW) | Do Not Concur | | | <p>This has been tested and identified as a negative impact on normal business.</p> <p>To meet compliance issues parts of the network are being redesigned so specific printers</p> |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|---|------------------|-----------------------|---|---|
| | | | | | are physically located in a secure environment and only a specific AD group will be able to print to the printer(s). The implementation plan will strengthen network printer security. |
| 12. | Expedite the current project of developing additional documentation of the computing environment and include updated documentation as a requirement of the formal Change Management Process. (HIGH) | Concur | Partially Implemented | August 2008 – implemented additional procedure for network documentation along with other areas | Currently working to improve documentation process. Recent computer environment documentation specific to CJIS and PCI compliance audits have been created and provided. |
| 13. | Configure all logs for every device across the City’s infrastructure to forward all system, application, and security logs to the centralized logging system and configure the logging level to allow capturing all security incidents as well as any system configuration changes. (MEDIUM) | Partially Concur | Implemented | August 2008 | All Windows Servers and Router syslogs have been setup to forward to a centralized logging system called Eventtraker. AS400 does not create or use syslog log files so no logs files from the AS400 will be centralized |
| 14. | Develop a formalized Systems Development Life Cycle (SDLC) methodology and require that the methodology be used on all projects. The methodology should assure: <ul style="list-style-type: none"> • Consideration of the security impact on the project during its initiation phase and | Partially Concur | Partially Implemented | August 2008 –September 30, 2009. | Created a SDLC Policy for management review and approval, expected September 30, 2009. Application development is following policy until management states otherwise |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|---|------------------|-----------------------|---------------------|--|
| | <p>through the end of the life cycle.</p> <ul style="list-style-type: none"> • Security components receive adequate testing during the implementation phase of the project. • Change orders are reviewed and properly authorized prior to their insertion into the development of systems. • Controls are in place to identify rogue or unauthorized changes. (MEDIUM) | | | | |
| 15. | Enforce existing security policies across all of the security access repositories that force passwords to expire and be changed on a regular time interval. (HIGH) | Partially Concur | Implemented | April 2009 | Windows password complexity along with AS400, Unix and other applications have been increased to meet compliance |
| 16. | Enable password complexity requirements on all operating environments, forcing users to comply with mandated policies, and implement a practice of performing a password strength assessment on a regular basis. (HIGH) | Do Not Concur | | | Windows password complexity along with AS400, Unix and other applications have been increased to meet compliance |
| 17. | Acquire and implement an automated account password management system for system administrators to better control privileged account management practices. (HIGH) | Partially Concur | Partially Implemented | April 2009 | Password Manager Pro by Adventnet was purchased and is currently being piloted for deployment in May 2009 |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|---|--------------------------|----------------------------|-----------------------|--|
| 18. | Implement a multiple-layer security approach that includes a firewall, an intrusion detection system, and/or an intrusion prevention system. (MEDIUM) | Concur with Reservations | Planned for Implementation | Unknown at this time. | IDS/IPS project has been planned for implementation pending funding approval. |
| 19. | As a part of the IDS implementation, detect potential security breaches by assigning staff to perform the regular reviews of the data. (MEDIUM) | Concur with Reservations | Planned for Implementation | Unknown at this time. | IDS/IPS project has been planned for implementation pending funding approval. |
| 20. | As part of the IDS implementation, develop and implement incident response procedures to facilitate timely and appropriate responses to a security attack or breach. (MEDIUM) | Concur with Reservations | Planned for Implementation | Unknown at this time. | IDS/IPS project has been planned for implementation pending funding approval. |
| 21. | Implement a policy requiring periodic vulnerability testing of the external and internal components of the computing infrastructure. (HIGH) | Concur with Reservations | Implemented | November 2008 | Implemented weekly external and internal scans for Vulnerability. Procedure implemented for addressing results from scans. |
| 22. | Conduct a risk assessment of all City publicly-accessible web applications and perform application level security testing on the high risk applications. (HIGH) | Concur with Reservations | Partially Implemented | Ongoing | Finance has been provided a quote from Qualysguard and has requested additional alternatives due to cost. TM will speak with Cenxic.com to see what options they can provide. Product selected must meet PCI requirements. Implementation pending funding. |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|---|----------|----------------|---------------------|---|
| 23. | Develop written policies and procedures for backup processing and offsite storage and rotation. (MEDIUM) | Concur | Implemented | April 2009 | <p>Relocated all servers to City Hall or OOC and writing to backup tapes at OPH thus eliminating the need to transport tapes. AS/400 tape rotation has been documented and changed to a weekly procedure. Tape tracking log has been implemented. Online checklist of daily responsibilities has been implemented.</p> <p>TM procedure written regarding the following processes: backups, off-site storage and rotation schedule</p> |
| 24. | <p>Investigate the use of an off-site storage service for all of the backup media generated by the City and consider the following:</p> <ul style="list-style-type: none"> • Encrypt all backup tapes in the event a backup tape is lost or stolen. • Implement a backup media log to record the movement of all backup media. • Transport the backup media in secure containers that are safe from fire, water, and dust. | Concur | Implemented | April 2009 | <p>TM has addressed the encryption backup request by addressing the tape backup process for the majority of the systems except for the AS400 which is required not to be for business reasons.</p> <p>TM has implemented online backups of servers at our OOC location. As new space is required for new online backups data is moved to a system located at OPH which</p> |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|---|--------------------------|----------------|---------------------|---|
| | <ul style="list-style-type: none"> Assure that the storage locations of backup media are clearly labeled and environmentally secure. (MEDIUM) | | | | <p>produces tapes which are maintained in a secure computer room within the Orlando Police Department. Tapes are maintained in a secure environment 24X7.</p> <p>Networker backup software maintains logs of backups to tape. Currently no tape media is transported.</p> <p>Storage racks at OPH are clearly marked/labeled and maintained in a secured computer environment within Orlando Police Headquarters.</p> <p>The few AS400 tapes transferred weekly are maintained in a locked metal box secured by a lock. AS400 backup tape activity is logged.</p> |
| 25. | <p>Enhance the existing Disaster Recovery Plan to include a Maintenance Log, glossary of terms, Status Reporting procedures for each Recovery Team, Communications Plan, and Recovery Time Objectives and Recovery Point Objectives for each system. (HIGH)</p> | Concur with Reservations | Implemented | May 2009 | <p>New procedures have been created to assure better contact access and improved SLA delivery with additional enhancements to follow.</p> |

**REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW INFORMATION SYSTEMS GENERAL CONTROLS AUDIT**

| # | RECOMMENDATIONS | RESPONSE | CURRENT STATUS | IMPLEMENTATION DATE | AUDITEE COMMENTS |
|-----|---|----------|----------------|---------------------|--|
| 26. | Mitigate the single points of failure in the network such as Core Switch/Router, Internet Service Provider, and the Metro-Ethernet Uplink. (HIGH) | Concur | Implemented | April 2009 | Secondary Core switch integrated at OOC April 2009 |