CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

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

May 3, 2006

AUDIT OF

800 MHz Radio System

HIGHLIGHTS

Highlights of City Auditor Report #0614, a report to the City Commission and City management.

WHY THIS AUDIT WAS CONDUCTED

The 800 MHz radio system (800 MHz system) is the primary means of radio communications for the City of Tallahassee and Leon County governments. As of November 17, 2005, there were approximately 3,200 radios authorized to access the 800 MHz system. Those radios were used by 16 various City departments, four County agencies/departments and the three local institutions of higher learning. The Radio Control Division (RCD) is responsible for the management and operation of the radio system; the maintenance has been subcontracted to Motorola, Inc.

The focus of our audit was a review of selected computer controls as they relate to the radio system. Additionally, we reviewed the operations and performance of the 800 MHz system and the RCD.

To conduct our review, we interviewed key individuals, visited and observed various 800 MHz locations, and reviewed reports, e-mails, and maintenance records.

WHAT WE RECOMMEND

Our recommendations are intended to improve the reliability and performance of the 800 MHz system. As such, we recommend: RCD should take a more proactive role in identifying and mitigating risks to help ensure the system remains reliable and available. An emergency/disaster recovery plan should be developed and documented to help ensure an orderly, timely, and efficient recovery from adverse incidents as they may occur. Physical security and environmental controls should be improved at the 800 MHz system facilities to ensure that they are accessed only by authorized persons so that the environmental conditions are suitable for the computer equipment. System coverage and logical security controls should be addressed during any planned upgrade or replacement project that may occur.

To view the full report, go to:

http://www.talgov.com/auditing/index.cfm and select *Auditing Reports*, then *Reports Issued FY 2006*, then *Report #0614*. For more information, contact us by e-mail at auditors@talgov.com or by telephone at 850/891-8397.

Audit Conducted by: Dennis Sutton, CPA, CIA
Beth Breier, CPA, CISA

WHAT WE FOUND

Overall, we found that the 800 MHz system appeared to be very reliable with users reporting a system up-time greater than 99.9% since its inception in 1999. However, issues were identified indicating the need to better identify and mitigate risks that could lead to major interruptions in radio operations. These issues included the need for:

- Fully documented emergency plans;
- A log of system outages, their causes, and remedial actions taken;
- Notification of the FAA for mid-level tower lighting outages;
- A record of the individual components which comprise the 800 MHz system;
- Environmental sensors installed at all system locations;
- Updated standard operating procedures; and
- Timely actions to address known issues to prevent damage and system interruptions.

Due to maintenance concerns (availability of replacement parts) and technological advancements, management has begun to explore options for the future upgrade or replacement of the current 800 MHz system. We identified issues with the current system that should be addressed during any such upgrade or replacement project. Those issues include:

- Improving the coverage of the radio system so all areas of Leon County have good reception and transmission; and
- Improving the logical security in the 800 MHz system software. For example, to ensure that:
    - Each user has unique user IDs and passwords; and
    - Access within the central controller is limited such that users can only access the parts of the system needed to complete their assigned duties.

800 MHz Radio System

AUDIT REPORT #0614

May 3, 2006

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

Copies of this audit report #0614 may be obtained from the City Auditor's web site (http://talgov.com/auditing/auditreports.cfm), or 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).

Audit conducted by:
Dennis Sutton, CPA, CIA, Senior Auditor
Beth Breier, CPA, CISA, Audit Manager
Sam M. McCall, CPA, CGFM, CIA, CGAP, City Auditor

Table of Contents

800 MHz Radio System

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

Report #0614 *May 3, 2006*

Executive Summary

This audit reviewed selected computer controls of the 800 MHz radio system (800 MHz system) as well as the operation and performance of the system and the Radio Communications Division (RCD) of Information System Services (which operates the system). The computer controls that were evaluated were those controls that were in effect during the period February 2005 through September 2005.

The 800 MHz system is the primary means of radio communication for the City of Tallahassee and the Leon County Sheriff's Office. As such, it is critical to the operations of the public safety departments operating in Leon County. The system is a computer-based radio system where computers dictate the path wireless communication will take. Due to the integrated nature of computers, the locations that house the 800 MHz system infrastructure should be maintained and controlled in a manner similar to any other computer system.

Users reported that the 800 MHz system has met their needs and has been very reliable.

We noted that the 800 MHz system appears to have been very reliable and was operational in excess of 99.9% of the time. However, because RCD does not maintain a log of all system outages, we based our determination of system reliability on records maintained by user departments. Also, based upon user interviews, we concluded that the 800 MHz system met their needs.

The Radio Communication Division needs to strengthen oversight of operations and system controls of the 800 MHz system.

During the course of our observations, inspections, and inquiries we noted issues that led us to conclude that the operation and oversight of the 800 MHz system could be improved by identifying and mitigating potential risks to the operation and performance of the 800 MHz system. Specifically, those issues were in the areas of system operations, and physical and logical security controls. Accordingly, the following recommendations are made to address the issues identified:

- Emergency plans should be further developed and documented to help ensure that (1) appropriate actions are taken in a timely

manner and (2) necessary resources are available, in the event of an emergency.

- A system to track or log all 800 MHz system outages should be developed to assist management in measuring and documenting reliability, identifying recurring issues and planning future maintenance needs.
- The RCD should comply with Federal Aviation Administration regulations relating to reporting all radio tower lighting outages.
- The alarm system that monitors various aspects of the 800 MHz system and its infrastructure should be examined to ensure it is connected properly, and periodically tested to ensure it is functioning as intended.
- Annual system emergency tests should be conducted in accordance with the maintenance agreement or removed from the contract.
- While the coverage of the 800 MHz system meets contractual provisions, there are service areas in the County where radio communications are problematic. To improve radio performance in these areas, system coverage should be further addressed during the assessment of potential technological options in future upgrade or replacement projects involving the 800 MHz system.
- Subsidiary inventory records should be developed and maintained to account for and assist in the management of individual components comprising the 800 MHz system.
- The approved standard operating procedures should be updated to reflect changes in uses and management of the 800 MHz system. In addition, oversight should be improved to ensure compliance with the procedures.
- Physical access controls should be strengthened to ensure that only authorized persons are allowed to enter 800 MHz facilities.
- Environmental sensors to monitor the various 800 MHz system infrastructure locations should be periodically tested to ensure notification of appropriate personnel when environmental

conditions deteriorate to the point where system functionality may be impacted.

- Stronger logical security controls in the 800 MHz system should be considered and implemented in any future upgrade or replacement of the 800 MHz system.

During the course of our audit, efforts were initiated to evaluate future radio communication needs of the current 800 MHz users. The current system will need to either be upgraded or replaced in the near future due to technology changes and maintenance concerns. The City has contracted with a consultant to assist in the evaluation.

We would like to acknowledge the cooperation and support of the Radio Communications Division of Information Systems Services, the Police Department, the Sheriff's Office, and First Communications, Inc., (the vendor contracted for maintenance services) during this audit.

This page intentionally left blank.

Scope, Objectives, and Methodology

The scope of the audit included a review of selected computer controls (access controls and service continuity) over the 800 MHz radio system (800 MHz system) that were in place February through September 2005, and of the performance and oversight of the 800 MHz system (and the related maintenance contract) by the Radio Communications Division (RCD) within Information Systems Services (ISS).

The objectives of this audit were to evaluate whether: (1) RCD operated the 800 MHz system in an efficient and effective manner; (2) selected computer controls (physical and logical security controls and emergency planning) as they relate to the 800 MHz system were in place and functioning as intended; and (3) the 800 MHz system meets the needs of its users through an evaluation of the performance of the system.

This audit focused on general system controls, operations, and oversight of the 800 MHz system.

To evaluate efficiency and effectiveness of operations and oversight of the 800 MHz system, we: visited and observed tower sites; interviewed RCD, Tallahassee Police Department (Police Department), Leon County Sheriff's Office (Sheriff's Office), and First Communications staff; and reviewed reports, e-mails, and maintenance records.

Procedures performed included interviewing staff, reviewing maintenance reports, and site visits to various tower locations.

To evaluate selected general computer controls of the 800 MHz system, we: interviewed RCD, user departments, and First Communications (the contractor providing maintenance for the radio system) personnel; visited tower locations; and examined the features and settings within the system software and computers.

To evaluate the performance of the 800 MHz system, we interviewed personnel from the RCD, Police Department, Sheriff's Office, and First Communications. We also reviewed

documentation reporting 800 MHz system downtime from the Police Department, and monthly testing results performed by First Communications.

This audit was conducted in accordance with Generally Accepted Government Auditing Standards and Standards for the Professional Practice of Internal Auditing.

Background

This background section provides a general description of the 800 MHz system, its users, management of the system, and related maintenance contracts.

800 MHz System Description

The 800 MHz system is the primary means of wireless communications in the City and County for public safety operations.

In April 1997, the City Commission approved a contract for approximately $8.8 million with Motorola for the acquisition of an 800 MHz trunked simulcast radio system (800 MHz system). The delivered 800 MHz system was accepted by the City in November 1998, after a six-month delay to resolve coverage and coverage-testing issues.

The 800 MHz system is the primary means of voice and data wireless communication for the City of Tallahassee, and voice-only communications for the Sheriff's Office and other users (including universities, and other City and County departments).

The 800 MHz system, referred to as a trunked simulcast radio system, consists of multiple channels and features providing multiple users the ability to communicate simultaneously across the entire system, within an entire organization, or within smaller pre-defined talk groups within each organization. In the system set up, each radio is assigned to one or more talk groups. Each radio can be configured to talk within one or more talk groups at a time. There are many talk groups set up within each organization that use the 800 MHz system. For example, police officers within the various patrol districts can choose to communicate within their assigned patrol district, or across the entire police department. In addition, talk groups are configured across two or more

organizations. Users can choose which talk group is used so only users assigned to that talk group(s) will hear the broadcasted message.

As stated above, the 800 MHz system consists of multiple channels. The more channels the 800 MHz system has, the more users can simultaneously use the system. When a user attempts to communicate, the 800 MHz system will automatically select the next available channel. The City's 28 channels have provided adequate capacity to transmit voice and data for public safety as well as for public service departments and agencies.

Federal Communications Commission directives will require the City to alter the 800 MHz system in the future.

Recently, the Federal Communications Commission issued directives that will require the City to abandon certain 800 MHz frequencies and channels on which the City's radio system operates. As part of that directive, frequencies and channels will be set aside in other parts of the radio spectrum for public safety use. However, it is not yet known which frequencies and channels the City will receive, what impact those changes will have, or how much it will cost the City. RCD management has been directed to monitor the developments as they occur, in order to regularly update the Management Oversight Committee (MOC).

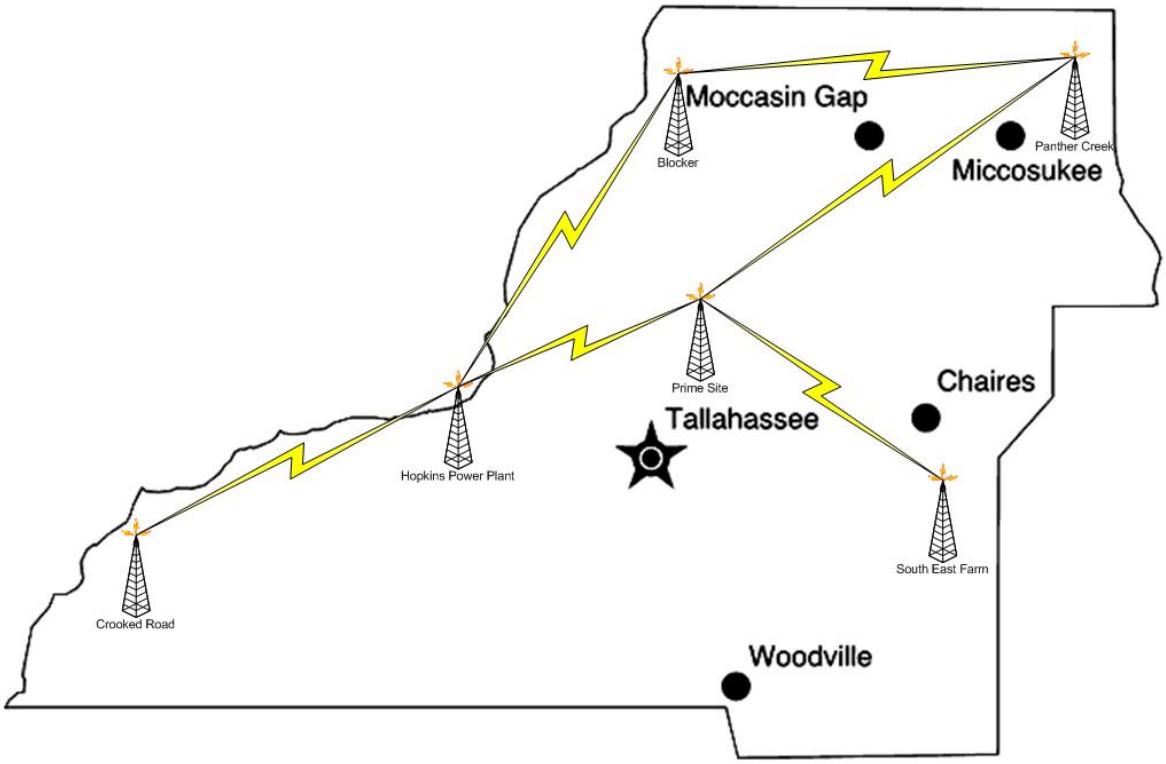
The 800 MHz system is a computer-based radio system. Computers select the channel that users talk on without human intervention and only allow pre-identified radios to communicate on the system. The 800 MHz system and its components therefore should be protected and cared for in a manner similar to any other computer and the equipment shelters should have controls in place similar to those for computer operations rooms.

The 800 MHz system is comprised of six radio towers and approximately 3,200 radios.

The City's 800 MHz system is comprised of six radio towers located throughout Leon County, with an equipment shelter at the base of each tower. The most important tower, located at the Police Department, is known as the "prime site." All communications flow through the prime site regardless of which tower initially submits a broadcasted transmission. The prime site houses the central controller, or "brains," of the 800 MHz system.

The central controller identifies authorized users and routes transmitted communications to their intended destinations. Figure 1, on the next page, shows a graphical representation of the towers, their approximate locations within Leon County, and the names commonly associated with each tower site.

Figure 1
800 MHz System Tower Locations and Connectivity in Leon County



Developed by Audit Staff

From this diagram it can be seen that not all towers have direct connectivity to and from the prime site. The reason that all towers are not directly linked to the prime site is a combination of distance and geographical features. Regardless of the intermediate relay (through another tower) in communication, all signals must reach the prime site before they can be transmitted to their final destinations.

In 1999, a Management Oversight Committee was formed to oversee the operation of the 800 MHz system.

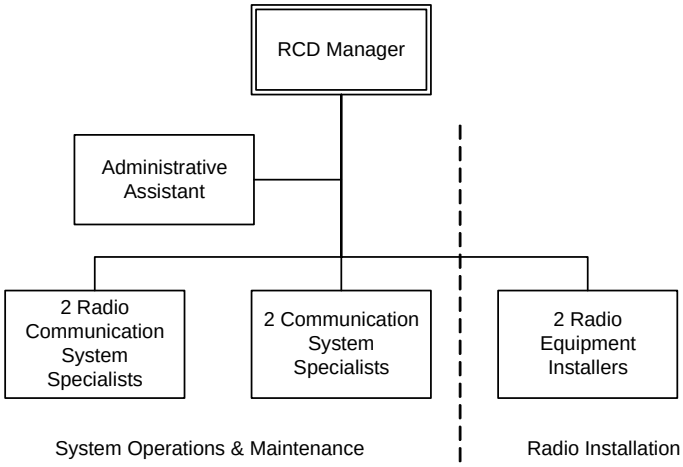
In 1999, the Sheriff's Office acquired a 25% interest in the voice side of the system. To provide the Sheriff's Office an opportunity to provide input and be involved in decision making, a 800 MHz system Voice Management Oversight Committee (MOC) was formed. The MOC is comprised of the Assistant City Manager for Public Safety and Neighborhood Services, the Police Chief, the Fire Chief, the City's Chief Information Officer, and the Sheriff. The RCD manager and staff regularly attend all MOC meetings and provide information as requested.

Operation and Oversight of the 800 MHz System

The 800 MHz system is operated by the Radio Communications Division of Information Systems Services.

The Radio Communications Division (RCD) of ISS is responsible for the operation and oversight of the 800 MHz system. The RCD is somewhat segregated into two sections. One section is involved in the operation and maintenance of the system hardware including the management of the maintenance contract(s). The second section is responsible for installation and removal of radios and other equipment from vehicles. Figure 2 illustrates the organization of the RCD.

Figure 2
Organization Chart for the Radio Communications Division



Developed by Audit Staff

Current users of the 800 MHz system include the City, County, and local universities and community college.

800 MHz System Users

Currently there are approximately 3,200 authorized radios on the 800 MHz system at the City, County, and local universities/community college, public safety, utility, and other public service departments. At one time, several state agencies also were users on the 800 MHz system. All state agencies, with the exception of the universities/community college, have since left the system and now utilize the state of Florida's Statewide Law Enforcement Radio System (SLERS). The universities will also be transitioning over to the SLERS in the near future. Table 1 shows the current agencies using the system and the number of radios registered in the system for each department or agency. (Note: For several user groups, multiple radios may be assigned to a single employee. For example, police officers have radios in their vehicles as well as portable radios they carry on their person.)

Table 1
Number of System Users by Agency and Department

Voice System Users	
DESCRIPTION	**Number of Radios**
City Users	
Police Department	620
Fire Department	224
Electric Utility	195
Public Works	175
StarMetro (bus system)	126
Water Utility	199
Solid Waste	78
Aviation	70
Parks & Recreation	69
Gas Utility	28
Neighborhood & Community Services	24
Utility Business & Customer Services	51
Fleet	17
Storm Water	7
Growth Management	5
Streets and Drainage	1
Total	**1,889**
Leon County Users	
Sheriff's Office	775
Public Works	210
Volunteer Fire Departments	75
Emergency Medical Services	115
Total	**1,175**
Other Users	
Florida A&M University	50
Florida State University	66
Tallahassee Community College	14
Total	**130**
TOTAL RADIOS	**3,194**

Source: 800 MHz system reports

Maintenance of the 800 MHz System

The maintenance of the 800 MHz system is divided into two areas of responsibility: (1) the network components and performance and (2) the supporting infrastructure.

First Communications, Inc., has been subcontracted to maintain the 800 MHz system.

For the maintenance and performance of the network components, the City has entered into an annual contract with Motorola, Inc. (Motorola). The maintenance agreement with Motorola provides for repairs of the system infrastructure and regular periodic preventative maintenance. Under the terms of the agreement, Motorola has the right to subcontract the maintenance work. Motorola has subcontracted the maintenance work of the 800 MHz system to First Communications, Inc. (First Communications). Even though Motorola has subcontracted out this work, they retain responsibility for all contract terms and requirements. RCD is responsible for managing the Motorola maintenance agreement, which involves the monitoring, oversight, and approval of the work performed by Motorola and/or First Communications, as applicable.

As Motorola's subcontractor, First Communications is responsible for the system's fixed network components, the antennas, and the mobile and portable radios (except when damage is caused by user abuse or neglect). The fixed network components include the computers and other hardware located in the radio shelters at the base of each tower.

Regular periodic maintenance includes a variety of tests and inspections conducted on a daily, monthly, semiannual, and annual basis. These tests are designed to ensure that the system is performing adequately and to identify potential performance problems before the 800 MHz system performance is negatively impacted or fails.

In addition, the City's contract with Motorola provides for timely response to recover from system outages. The contract does not provide for a guaranteed percentage of operational time, however, it does guarantee a system failure response and recovery time.

All maintenance of the supporting infrastructure of the 800 MHz system is the responsibility of the RCD. This includes maintaining the shelters at the base of each tower, the towers, and the electrical supply to the system.

Overall Summary of Issues

While users reported high reliability of the 800 MHz system, we noted issues that increased the risk the system would be damaged or disabled, and areas where oversight of the system should be improved.

In general, the performance of the 800 MHz system appears to have been very reliable. Our analysis of outages and recovery times reported by a user department showed that the system was operational in excess of 99.9% of the time. It also showed that the system recovered from every outage in less than the time guaranteed in the maintenance contract (in most instances the outage was self- corrected by the system).

Notwithstanding the apparent reliability of the system, we noted the occurrence of incidents and issues that could have potentially disabled the system. As a result, we noted where improvements could be made to strengthen the oversight and system controls of the 800 MHz system.

Issues and Recommendations

We noted several areas where the controls, operations, and oversight of the system can be improved to ensure a more reliable, secure, and better-operating system. These issues have been classified into the following two broad categories, (1) the operation and oversight of the 800 MHz system, and (2) system security controls.

Operation and Oversight of the 800 MHz System

As defined for this report, the operation of the system includes the reliability of the system by the RCD, the performance of the system, and the safeguarding of system assets by the RCD.

<u>RCD should be more proactive in addressing issues and controls relating to the 800 MHz system.</u>

RCD oversight and operation of the 800 MHz system needs improvement.

RCD's oversight of the 800 MHz system involves ensuring that: 1) the system is always up and running efficiently and effectively; 2) the contractors are providing quality services; 3) the operations and activities related to the 800 MHz system comply with applicable laws, regulations, and policies and procedures; and (4) all external and internal risks to the 800 MHz system are identified and mitigated as soon as possible.

During the course of this audit, several issues came to our attention that are directly related to the operation and oversight of the 800 MHz system and the above-noted responsibilities of RCD. Some of those issues reported in subsequent sections of this report included the need for:

- Fully documented disaster recovery plans;
- A log tracking system outages to assist in identifying recurring issues and planning future maintenance;
- Notification of appropriate authorities when incidents of mid-level tower lighting, as well as other lighting, failures occur;
- A process to review the alarm system to ensure all appropriate parts of the 800 MHz system are connected and that the alarm system is properly functioning;
- A review of the emergency testing provisions in the maintenance contract;
- Subsidiary inventory records of the individual components that make up the 800 MHz system; and
- A review of the adequacy of the environmental sensors.

Improvements in the oversight of the 800 MHz system should help ensure the system remains reliable.

Other issues that came to our attention during our review indicating the need for improved oversight of the 800 MHz system included:

- A roof leak occurred at the prime site and no remedial action (i.e., applying temporary covering as protection) was initiated for two weeks.
- A known problem with the air conditioners at the prime site was not communicated to personnel able to monitor and mitigate the situation during non-business hours. Subsequently, the air conditioners failed leading to a complete 800 MHz system failure.
- A gap in the fence at the prime site could potentially allow unauthorized persons access to the radio tower.

(*Subsequent to our audit fieldwork, a vandal accessed the prime site tower area and caused minimal damage. In response to that incident, RCD management began a project to upgrade the security at the prime site, including the fencing*).

The above issues indicate that the RCD's oversight of the controls relating to the 800 MHz system should be improved to help ensure the system remains reliable. To improve the RCD's oversight of the controls and operation of the 800 MHz system, we recommend that RCD take a more proactive role in identifying and mitigating potential risks to the operations and performance of the 800 MHz system. Such activities should include ensuring:

- appropriate and timely actions are taken to address known issues relating to the 800 MHz system;
- activities performed by RCD staff are satisfactorily completed; and
- compliance with all applicable laws, policies, operating procedures, and contracts.

An emergency or disaster recovery plan has not been fully developed or documented.

Formal emergency plans have not been fully developed or documented to help ensure appropriate, organized, and timely actions are taken when emergencies occur.

An emergency or disaster recovery plan provides for the orderly recovery of business applications in the event of an unexpected interruption in operations.[1] An effective disaster recovery plan should document all aspects of the process of recovering from a disaster. Risks encountered in a disaster recovery that should specifically be addressed in the plan include:

- Electrical Power Supply - the risk that the electrical power that the system is dependent on will fail.
- Physical Architecture – the risk that the system will be damaged by water, fire, human sabotage, or other physical damage.

[1] 2003 Miller IT Audits, Xenia Ley Parker

- Documentation – the risk that system or process documentation will be inadequate or missing when needed.
- System Architecture – the risk that system hardware or parts will not be available when needed.
- Backup Media – the risk that the backup copies of the system software, the applications themselves, or the related user data, will not be available or complete (i.e., up to date).[2]

During our review, RCD management informed us that while a fully documented disaster recovery plan was not currently available, efforts have been made to address emergency situations. For example:

- Some of the existing SOPs address activities that would be included in a formal emergency or disaster recovery plan;
- The maintenance agreement with Motorola includes provisions for system recovery within certain time frames;
- Certain spare and backup equipment is stored for use in emergency situations; and
- Verbal communications have occurred within RCD as to what to do in the event of various types of emergencies (i.e., power failure, equipment failure, etc.).

Without documented emergency or disaster recovery plans, there is an increased risk that resources such as replacement parts and personnel, and system documentation will not be available when needed to recover from a disaster. We recommend that a formal disaster recovery plan for the 800 MHz system be developed, documented, periodically tested, and updated as needed.

A process to log 800 MHz system outages and their causes has not been developed.

There is not a process to document all instances of interruptions in 800 MHz system operations. As previously stated, we based our analysis of system availability/reliability on records and reports from user departments and not RCD.

[2] Handbook of IT Auditing, David M. Jordan

The documentation we relied on consisted of various emails and interoffice memorandums. While our review of those documents showed that there have only been eight instances of complete interruptions in operations since the 800 MHz system was implemented in 1998, there may have been other system failures, which were not included in our analysis due to the lack of a formal process for recording and tracking 800 MHz system downtime. Each reported interruption lasted for a relatively short period of time, ranging from approximately 20 seconds to 30 minutes. (For this report, we only considered failures to be incidents where the entire radio system was inoperable.) Incidents of system failure were noted to have occurred due to a variety of causes, including: lightning strikes, overheating of equipment, equipment failures, human error, and other unknown reasons (assumed to be atmospheric interference).

While the 800 MHz system appears to have been very reliable, a better understanding of 800 MHz system reliability could be obtained if there was a process in place to record and track all system downtime. A log of system failures also would provide management a source of information for analyzing causes of system failures and could assist in planning future maintenance activities.

We recommend that RCD management implement a process to log all disruptions of 800 MHz system operations, including the date, time of day, length of time, cause, and corrective action(s) taken to restore operations.

The RCD has not complied with Federal Aviation Administration (FAA) requirements to report tower lighting outages and to maintain records of all tower lighting outages.

Required notices relating to tower lighting failures have not been made to the FAA.

The FAA has specific rules (Catalog of Federal Regulations 47 Part 17 Subpart C 48 and 49) that govern the notification of extinguishment or improper functioning of lights on radio towers. The regulation states the FAA must be notified whenever "any top

steady burning light or any flashing obstruction light, regardless of its position" is extinguished or improperly functioning. The purpose of the notification is to provide the FAA the ability to provide notice to airplane pilots of incidents and locations of tall structures (i.e., radio towers) that do not have required lighting.

During the course of our site visits, we noted that a midlevel flashing light at the prime site tower was no longer functioning. When we inquired of management as to whether they had provided the FAA with the required notification, they responded that notification had not been made. RCD management had mistakenly interpreted FAA rules to mean that notification was only required when the top-most light was not functioning.

An additional requirement of the FAA is that a record must be maintained of any known extinguishment or improper functioning of a structure light. RCD management was unable to provide the required records.

We recommend that RCD management review and obtain an understanding of the FAA tower lighting and reporting requirements, and make appropriate notifications to the FAA when applicable. In addition, we recommend that the RCD develop a logging process to maintain records relating to tower lighting maintenance and FAA reporting.

The alarm monitoring system was not properly connected to the generator at the prime site. As a result, the proper persons were not notified when the system generator malfunctioned.

The alarm system that monitors the 800 MHz system was not properly connected to the generator that supports the prime site.

A properly functioning generator is a critical part of an electrical system. Generators provide power for the computer systems in the event of a loss of regular power. The alarm system that monitors the operation of the 800 MHz system is a critical part of the physical controls over the 800 MHz system.

During the contractor's regularly scheduled maintenance of the generator in November 2005, it was determined that the generator appeared to have been hit by lightning sometime in the past and was not working properly. However, because no alarm had been triggered, RCD mistakenly assumed that the generator was functioning properly.

To ensure that the alarm system can be relied upon, we recommend that RCD develop a process to periodically review the entire alarm to ensure that:

- Appropriate components of the 800 MHz system are connected to the alarm system;
- The alarm system is periodically tested and found to be working; and
- Adequate records of periodic maintenance show that all critical components have been periodically tested.

Contracted annual system emergency tests have not been conducted by the contractor to ensure that the 800 MHz system can be restored in a timely manner.

Annual system emergency tests have not been conducted.

The maintenance agreement with Motorola provides for a yearly system emergency test. Such test would provide assurance to RCD that Motorola can adequately and timely restore the 800 MHz system in the event of an emergency.

During our review, we were informed that annual tests have not been conducted since the first contract was executed in 1998. RCD management indicated that the MOC directed staff not to conduct the emergency testing due to the risk of unintentional damage to the system. The RCD was unable to provide documentation supporting their assertion that such direction was given; however, some MOC members recalled providing this direction to RCD.

The lack of emergency testing is an issue since there has never been a test of the emergency response activities to ensure that the 800 MHz system can be adequately restored in a timely manner.

We recommend that RCD management and the MOC jointly reconsider the risks related to the annual 800 MHz system emergency tests. If the decision is made to conduct annual emergency testing, we recommend that the results of such tests be documented for analysis to facilitate future process improvements. Conversely, if the decision to refrain from conducting those tests is reaffirmed, we recommend that documentation supporting that decision be generated and retained, and provisions requiring the tests should be removed from the annual maintenance agreement with Motorola to avoid paying for services not received.

There are service areas within the County where communications over the 800 MHz system are problematic.

Communication through the 800 MHz system is problematic in certain areas of the City.

There are two main methods in which the 800 MHz system's performance can be measured. The first is dividing the County into small measured quadrants and methodically testing the signal strength in each quadrant. The second is through reports from users describing the level of quality of communications at specific areas.

RCD management stated that there has not been any methodical testing of the 800 MHz since the 800 MHz systems was expanded in 1999. Therefore, without that level of detailed testing, it is not possible to definitively quantify the 800 MHz system's current performance. Therefore, we reviewed anecdotal reports from user departments.

Users from the Police and Fire Departments reported that there are several areas in the City where communication transmissions using the 800 MHz system are problematic. No other user departments reported transmission problems. Such problems were reported by users of lower power portable radios worn on police and firefighter uniforms and included difficulty in understanding transmissions due to static or degraded communications, as well as a total loss of communication. Portable radios (3 watt) are not as powerful as the radios that are mounted in vehicles (35 watts) that use the vehicles'

power rather than batteries. Examples of problematic areas included:

- Orange Avenue east of Monroe Street;
- Inside Governor's Square Mall; and
- Inside several of the downtown parking garages.

Discussions with RCD management identified factors that can negatively affect communication transmissions. These include:

Factors that could contribute to the areas of problematic communications were identified.

- Growth of vegetation that interferes with the signal;
- Construction of buildings that create a "broadcast shadow" (an area on the opposite side of a building from the radio tower in which radio signals have been blocked by the building);
- The lower power of the portable radios;
- Use of batteries that are in need of recharging;
- Use of radios in a manner that reduces the effectiveness of the radio (i.e., with the antenna pointing down); and
- Achieving 100% coverage of a large geographical area (i.e., Leon County) would be cost prohibitive and as such, should not be expected from any wireless communications system.

RCD management acknowledged that there are areas in the City where communications have been reported as problematic, but they maintain that it is the result of the above factors and not a deficiency of the 800 MHz system. The areas of problem communications that have been noted increase the potential that the 800 MHz system will not be available when needed.

An upgrade/replacement of the 800 MHz system is being considered due to maintenance concerns with the current system and changes in radio communication technology. As a result, the MOC has directed the RCD to contract with a consultant to identify technological options that should be considered when the current 800 MHz system is upgraded or replaced. RCD indicated

that the consultant contract was executed in March 2006 and estimates that the project will be completed by June 2006.

We recommend that system coverage be adequately addressed during this assessment, future evaluations, and any 800 MHz system upgrade or replacement projects that may occur.

Subsidiary inventory records of the individual 800 MHz system components were not available for review or verification of accuracy.

City Administrative Procedure 630, Internal Control Guidelines, outlines basic internal controls that should be in place to safeguard the City's assets. Specific controls identified include periodic verification of assets and subsequent comparison of those counts to related control records.

While the 800 MHz system is recorded in the City's financial records, there were not subsidiary records of the individual components.

Maintaining records of individual assets and conducting periodic verification of those assets is an internal control that has not been be implemented for the 800 MHz system. Our examination showed that the 800 MHz system was recorded in the fixed asset records in major groups (i.e., an entire tower site including all the related electronic components as a single asset). However, there were not records of the individual components that comprise the infrastructure of the 800 MHz system. Additionally, we noted that records as to what spare components are on hand and available for use were not available. Table 2 below illustrates the allocation of value among the various tower sites.

Table 2
Summary of 800 MHz System as recorded in the Financial Records

Location	Amount
Prime Site	$ 5,020,561
Blocker	$ 1,204,934
Crooked Rd.	$ 1,204,934
S.E. Farm	$ 1,204,934
Panther Creek	$ 1,204,934
Hopkins	$ 1,204,934
Total	$ 11,045,231

Subsidiary inventory records will help RCD account for the individual components of the 800 MHz system, and help ensure that adequate spare/replacement parts are on hand when needed.

We recommend that in order to ensure that the individual assets and related spare parts are accurately accounted for, subsidiary inventory records of these components making up the 800 MHz system locations be developed and maintained. Examples of items that make up the system and should be individually identified include radio network controllers, rectifiers, and dispatch consoles. Once the subsidiary records are developed, an annual verification of these assets should be performed.

The RCD standard operating procedures (SOPs) that provide guidance in the management and usage of the 800 MHz system are not consistently complied with nor are they up-to-date.

City Administrative Procedure 630, Internal Control Guidelines, charges every employee with complying with "Understanding and complying with the internal control procedures established in their department and division." RCD stated that the MOC approved the SOPs to provide procedures for the operation and oversight of the

800 MHz system in 1999 or 2000, but there was not documentation to support that the SOPs were approved.

Examples of SOPs (paraphrased) that have not been complied with, include:

- Creation of a user group consisting of a representative from each agency participating in the system;
- Entrance to 800 MHz locations by maintenance providers and contractors will only be with prior approval of RCD; and
- A team from the user group will conduct a security "audit" of the 800 MHz facilities.

RCD concurred that there were certain SOPs that were not complied with and that in general the SOPs needed to be updated. RCD also noted that compliance with some of the SOPs was dependent on the actions of the user agencies, not RCD. Regardless of the actions or lack of action by the user agencies, the MOC has charged the RCD with the responsibility of implementing the SOPs, and as such, RCD should make every effort to ensure compliance with the SOPs.

Noncompliance and out-of-date policies and procedures reduce the assurance that proper action will be taken in the course of operations. Standard operating procedures provide both management and staff a level of assurance in that the SOPs:

- Provide a basis for employee accountability;
- Serve as a tool for employees seeking guidance on the proper actions that should be taken in specific situations;
- Help ensure consistency and continuity in operations during occurrences of employee turnover; and
- Provide assurance to management that operations will be conducted in an efficient and effective manner.

We recommend that the SOPs be reviewed and updated to reflect best practices of the radio communications industry, the needs of the user agencies, and compliance with applicable laws and other

City policies and procedures. Furthermore, we recommend that future reviews of the SOPs be periodically conducted and revised as needed. We also recommend that RCD increase compliance with the current SOPs as established and approved by the MOC, and incidents of non compliance should be brought to the attention of the MOC for resolution.

System Security Controls

System security controls consist of physical and logical security controls.

System security controls can be divided into two categories: (1) physical security controls and (2) logical security controls. Both types of controls are necessary to ensure that the 800 MHz system is adequately safeguarded.

Physical security controls are those controls that prevent or deter theft, damage, and unauthorized physical access to system equipment. Activities that protect computer equipment from physical damage and theft include:

- Allowing only authorized persons responsible for maintaining the computer equipment into the rooms housing computer equipment;
- Providing detection features to alert staff of conditions related to heat, fire, smoke, water, dust/dirt, etc.; and
- Storing hazardous materials, such as cleaning chemicals, in separate locations from the computer equipment.

Logical security controls can be defined as controls restricting access into specific information systems and applications to prevent unauthorized individuals from altering, damaging, or destroying programs and/or data. Activities that protect programs and data from unauthorized logical access include:

- Allowing only authorized users to access system programs and data, and perform only appropriate, pre-defined functions. This is accomplished through managing user IDs and passwords, and assigning appropriate access capabilities within the program (i.e., related to job responsibilities).

- Monitoring, tracking, analyzing, and reporting suspected and actual security breaches (i.e., unauthorized access into computer equipment locations or information systems).
- Managing cryptographic keys to ensure that transmitted data is encrypted and adequately protected from unauthorized interception and access.

Each location housing a portion of the 800 MHz system should provide an adequate level of physical security to protect the equipment from damage. In addition, every logical access path into the 800 MHz system should be adequately secured to prevent unauthorized users from viewing, altering, or destroying the program or data.

Physical Security

During our audit, we noted the following controls for physical security over the 800 MHz system that should be improved.

Physical access controls into the 800 MHz prime site and tower sites need to be strengthened to prevent unauthorized persons from entering these facilities.

Specifically, we noted the following weaknesses:

Controls over the keys that provide access to facilities housing the system are not adequate.

- Facility keys were not adequately controlled to ensure that only authorized individuals can access the tower sites that house 800 MHz system components. During our review of physical security controls, we noted two issues related to controlling keys. First, there is not an inventory of keys or key holders. Second, the existing keys are not "security" keys, meaning that they can be easily duplicated. RCD management indicated that they have not maintained records identifying who has been provided keys to the 800 MHz system tower locations. The RCD manager stated keys had been given to City employees (RCD, other ISS staff, and police) and First Communications staff, but documentation of key distribution has not been maintained.

RCD was unable to verify that keys had been adequately controlled or that keys were only in the possession of currently authorized persons.

- The keys used to access the various tower sites were not "high-security-type" keys (i.e., not readily copyable) nor were they stamped "Do Not Duplicate." This control is to prevent easy and unauthorized duplication of keys and ensure the integrity of the key logs.

Even though RCD is responsible for securing the prime site, access to this facility is controlled by TPD.

- Physical access into the 800 MHz prime site is not controlled by RCD, but instead by TPD. Since RCD is responsible for the assets, protection and operation of the 800 MHz system and the building housing those assets, they should control and monitor who is authorized to enter the prime site. During a project to upgrade the security system at the police headquarters, TPD added the prime site to their security system without the approval or consent of RCD. Additionally, TPD is currently managing who is allowed physical access into the building without the involvement or approval of RCD. While the security system installed by TPD provides many positive features (such as logging of persons accessing the building), its installation has taken the ability to determine who is authorized to access to the prime site away from RCD.

A log of who enters 800 MHz facilities (with the exception of the prime site) is not generated.

- There is not a log maintained to identify who enters the various tower locations (with the exception of the prime site). City Administrative Procedure 809, Information System Security, identifies, as a minimum recommendation, a "traffic monitoring system for logging of traffic in and out" of the location. A log of who has accessed the various 800 MHz locations can assist RCD when attempting to identify the source of problems that may arise.

Without physical access controls, RCD cannot ensure that only authorized persons are accessing the 800 MHz system facilities. To strengthen these controls, we recommend that RCD:

1. Implement a process to control the issuance of keys to only persons who are authorized to access the 800 MHz system locations.
2. Replace or re-key the existing locks using keys that are designated high security or stamped "Do Not Duplicate."
3. Work with TPD management to review and approve individuals authorized to access the prime site.
4. Implement a process to log all individuals entering 800 MHz system facilities.

Environmental sensors were not in place to adequately monitor the locations where critical system infrastructure is located.

Monitoring the environment in which computer equipment is located is a control that should be in place due to the sensitivity of computer equipment to adverse conditions such as heat and moisture. City Administrative Procedure 809, Information System Security, recognizes this through the identification of certain monitoring activities that should occur in major communication equipment areas. Those monitoring activities include climate controls and water detection systems.

A lack of environmental sensors resulted in a disruption of operations of the 800 MHz system.

Due to the lack of sensors at the prime site, a problem with the air conditioners resulted in a system failure. In February 2005, a problem was noted with the air conditioning system at the prime site. In response, RCD began the process to repair/replace the air conditioning units. However, prior to the completion of that project, the air conditioning system failed. This shut down the air conditioning system and caused the temperature inside the prime site to increase to the point where the 800 MHz system shut itself down to prevent damage. Once the system shut down, immediate actions were taken to reduce the temperature, which enabled the system to come back on-line.

This interruption in operations could have been averted if temperature sensors had been in place. Notification to appropriate individuals would have allowed staff to take appropriate actions in a timely manner to prevent the 800 MHz system from shutting down. In October 2005, RCD management had temperature sensors installed at the prime site, approximately eight months after the above incident occurred.

We recommend RCD review the environmental sensors at each 800 MHz system location. Such reviews should evaluate the adequacy of the types of and warning thresholds of the sensors, the operation of the sensors, and connections of the sensors to the alarm monitoring system. Additionally, we recommend a testing plan be developed to periodically test the environmental sensors to ensure that they are working as intended.

Logical Security

The second area of system security controls is logical security. Logical security controls, located within computer systems and software applications, are designed to prevent unauthorized access or activities.

The central controller is the system software used to operate the 800 MHz system and is the only part of the 800 MHz system that has logical security control capabilities. The central controller is divided into two main areas: (1) systems maintenance and diagnostics and (2) operations. The system maintenance and diagnostic area is used to monitor the system and assist technicians in troubleshooting problems. The operations area is used to identify and authorize the radios that access and use the system.

Logical access to the central controller can be obtained through direct and remote access. Direct access (at the terminal in the prime site) can be restricted through physical security controls as well as through logical security controls; whereas remote access (through telephone or wireless connections) can only be controlled through logical security controls. Therefore, logical security

controls are critical to the overall security of the system. We noted two logical security weaknesses related to logical security that increase the risk that unauthorized users may access the system and authorized users may perform actions outside the scope of their authority. These weaknesses are:

- All users must utilize a single shared user ID and password to access the 800 MHz system software; and
- Access within the central controller cannot be limited such that users can access only the parts of the system needed to complete their assigned duties.

Users share a single user ID and password to obtain access to the central controller.

The National Institute of Standards and Technology Generally Accepted Principles and Practices for Securing Information Technology Systems § 3.11.1 states, "An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system." Furthermore, City Administrative Procedure 809, Information System Security states, "…privileges must not be extended unless a legitimate business oriented need for such privileges exists." Access to computer systems should be based on the principle of "least privilege", which means that users should be granted access only to resources needed to perform their duties.

Employees of both RCD and First Communications regularly access the 800 MHz system's software to perform a variety of tasks using the same user ID and password.

User access within the central controller has not been appropriately limited.

Without the use of a unique login ID for each individual accessing the system, it is not possible to limit a user's access to only the areas of the software that are needed to complete that user's job, nor is it possible to specifically attribute changes made to the software to a specific user. Additionally, a failure to limit users' access capabilities within the central controller increases the risk that unauthorized radios may be allowed into the 800 MHz system, as well as the risk that the system may be inadvertently damaged

by an individual performing activities outside their area of responsibility.

We acknowledge, along with RCD management, that these logical security weaknesses are inherent in the current 800 MHz system. Therefore, we recommend unique user IDs, password controls, and the ability to restrict users' access within the software be considered and included in any future upgrade or replacement of the system.

Conclusion

Recommendations have been made to improve operations, oversight, and the system controls relating to the 800 MHz system.

Overall, based on user department reports, the 800 MHz system appeared to have been very reliable. However, as noted in the body of this report, we noted the following areas where improvements should be made:

- Improve operations and oversight of the 800 MHz system. Specifically, RCD should:
  - Help ensure appropriate, organized, and timely actions when emergencies or disasters occur;
  - Provide a source of information for analyzing 800 MHz system failures;
  - Increase compliance with FAA directives;
  - Increase the reliability of alarm system monitoring for the 800 MHz system;
  - Resolve the issue of contracted annual emergency tests not being conducted;
  - Ensure that radio coverage is adequately addressed in any future upgrade or replacement projects;
  - Improve asset management at the system component level; and
  - Improve compliance with, and updating of, the 800 MHz system's standard operating procedures.
- Improve computer controls related to physical and logical security of the 800 MHz system. RCD should:
  - Improve controls over physical access in the 800 MHz system facilities;

- Increase the assurance that the environment in which the 800 MHz infrastructure is located is appropriate for computer operations; and
- Ensure that adequate logical security controls are considered in any future upgrade or replacement project.

Appendix A provides management's action plan to address each of the issues identified in this report.

We would like to thank and acknowledge the support of the Radio Communications Division of Information Systems Services, the Tallahassee Police Department, the Leon County Sheriff's Office, and First Communications, Inc.

Response from Appointed Official

City Manager Response:

The 800 MHz is an extremely important system as it provides radio coverage to our Public Safety and operating departments. I was pleased to see that the reliability of this system was outstanding (99.9%). The 800 MHz system is currently being analyzed by Tusa Consulting who gave high marks to the maintenance of our tower sites and system. I appreciate the work of the Office of the City Auditor and would like to note that most of the suggested action plans have been addressed and completed by staff. I am pleased with the success of this system and would like to thank the Office of the City Auditor and DMA/ISS for their efforts.

Appendix A – Action Plan

Action Steps	Responsible Employee	Target Date
A. Objective: To improve the oversight of the 800 MHz system.		
1. Conduct an assessment of the 800 MHz system on an annual basis and document the results of those assessments. The assessment will evaluate the Strengths, Weaknesses, Opportunities, and Threats of the system. Projects and activities planned for the next year will be based on the results of the assessment and budgetary constraints.	Leven Magruder (Project Manager)	11/1/06
2. Develop and document a process whereby activities/projects conducted by RCD staff will be reviewed by the System Manager to help ensure that the tasks are satisfactorily completed.	Leven Magruder (Project Manager)	12/1/06
B. Objective: To improve the preparedness for the recovery from emergencies or disasters.		
1. Conduct and document a risk identification/assessment (as it relates to disaster planning) of the 800 MHz system.	Leven Magruder (Project Manager)	6/10/06
2. Conduct and document an impact analysis.	Leven Magruder (Project Manager)	7/1/06
3. Develop a documented disaster/emergency recovery plan. That plan will be based on the risk assessment and impact analysis previously conducted.	Leven Magruder (Project Manager)	8/1/06
4. Periodically test (annually at a minimum) the disaster plan. The exact composition of the tests should vary from year to year and will be determined by RCD management.	Leven Magruder (Project Manager)	5/1/07

5. Review and revise the plan annually, or more frequently as appropriate.	Leven Magruder (Project Manager)	5/1/07
C. Objective: To improve the recording and tracking of 800 MHz system outages, their causes, and remedial actions taken.		
1. Develop a system or process to document all instances of 800 MHz system service interruptions. Included in that process will be the cause of the interruption, the date and time of the interruption, and the corrective actions taken to restore operation of the radio system.	Leven Magruder (Project Manager)	6/1/06
D. Objective: To improve compliance with FAA regulations relating to tower lighting.		
1. Review FAA requirements for radio facilities in general and those relating to the City's radio towers specifically.	Leven Magruder (Project Manager)	5/1/06
2. Conduct and document an evaluation of the City tower sites and monitoring practices to ensure the City's compliance with FAA requirements.	Leven Magruder (Project Manager)	5/1/07
3. Develop and maintain a logbook of all radio tower lighting outages in accordance with FAA requirements.	Leven Magruder (Project Manager)	5/1/06
E. Objective: To improve the reliance that can be placed on the alarm system that monitors the 800 MHz system.		
1. Review all aspects of the 800 MHz system to ensure appropriate parts of the system that can/should be monitored are connected to the alarm system (MOSCAD) that monitors the 800 MHz system.	Leven Magruder (Project Manager)	5/1/07
2. Develop a process whereby the alarm system monitoring various parts of the 800 MHz system is periodically tested.	Leven Magruder (Project Manager)	5/1/07

3. Develop a process whereby the testing of the alarm system is documented to help ensure that all critical components and connections have been tested.	Leven Magruder (Project Manager)	5/1/07
F. Objective: To review the emergency testing provisions of the 800 MHz system maintenance agreement and decisions previously made thereon.		
1. Clarify, and expand upon as needed, the scope of emergency testing to be conducted pursuant to the maintenance contract with Motorola.	Leven Magruder (Project Manager)	7/1/06
2. The MOC will review the decision to not conduct emergency tests (based on the scope as clarified above) of the 800 MHz system and a decision will be made as to whether such emergency testing should occur.	Leven Magruder (Project Manager)	7/1/06
3. Emergency testing will or will not occur as determined by the MOC. If the decision is made to NOT conduct emergency tests, then the provisions for such tests will be removed from the maintenance agreement.	Leven Magruder (Project Manager)	8/1/06
G. Objective: To evaluate the coverage of the 800 MHz system and take appropriate actions based on that evaluation.		
1. Address and evaluate system coverage as part of any project to upgrade or replace the current 800 MHz system.	Don DeLoach (CIO)	To be determined
H. Objective: To increase accountability and oversight of individual components and spare parts of the 800 MHz system.		
1. Develop a record of the individual components and spare parts of the 800 MHz system. These records will serve as a subsidiary inventory of the assets as recorded in the City fixed asset records.	Leven Magruder (Project Manager)	12/31/06
2. Conduct an annual verification of the assets in the subsidiary inventory records and resolve any discrepancies.	Leven Magruder (Project Manager)	12/31/06

I. Objective: To improve and update the standard operating procedures governing the 800 MHz system.		
1. Create a committee, comprised of current Public Safety users of the 800 MHz system, with a mission of reviewing and making suggestions as to revisions that are needed to the 800 MHz system SOPS. The System Manager is responsible for drafting and promulgating the SOPs with the MOC's approval.	Leven Magruder (Project Manager)	5/1/07
2. The System Manager will revise current SOPs and develop new SOPs as appropriate. The SOPs will include a provision whereby periodic review and revision are required (i.e. sunset provisions). The SOPs will also include provisions for the enforcement of compliance with the SOPs and the escalation of issues of noncompliance to the MOC for resolution.	Leven Magruder (Project Manager)	11/1/07
3. The System Manager shall present the revised SOPs to the MOC for approval and the MOC's approval will be documented.	Leven Magruder (Project Manager)	5/1/08
J. Objective: To improve the physical access controls relating to the various 800 MHz system locations.		
1. Develop a process whereby issuances of keys are recorded and signed for by the individual receiving the keys.	Leven Magruder (Project Manager)	5/1/06
2. Re-key existing locks with locks that require either high security type keys or new keys stamped "Do Not Duplicate."	Leven Magruder (Project Manager)	5/1/06
3. Develop a process whereby RCD is able to review and determine who is able to access the prime site using the security system maintained by TPD.	Leven Magruder (Project Manager) & Lt. Tom Maureau	5/1/08
4. Develop a process whereby all individuals entering 800 MHz system facilities are logged. Such logs will record the date and time the facility was entered and left and the purpose of the visit.	Leven Magruder (Project Manager)	5/1/06

K. Objective:	**To improve the monitoring of the environment of the 800 MHz system locations.**	
1. Review environmental sensors at every 800 MHz system location to ensure compliance with AP 809 and that the environment is adequate to support the functioning of the 800 MHz system.	Leven Magruder (Project Manager)	5/1/07
2. Develop a process whereby the sensors monitoring the environment of the 800 MHz system locations are periodically tested to ensure they are still functioning.	Leven Magruder (Project Manager)	11/1/07
L. Objective:	**To improve the logical security controls of the 800 MHz system.**	
1. Address and evaluate logical security controls as part of any project to upgrade or replace the current 800 MHz system.	Don DeLoach (CIO)	To be determined