SOUTH FLORIDA WATER MANAGEMENT DISTRICT

Audit of the Disaster Recovery Plan

Report # 11-05

Prepared by
Office of Inspector General

J. Timothy Beirnes, CPA, Inspector General
Kit Robbins, CISA, CISM, CRISC, Lead Information Systems Auditor

sfwmd.gov

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

April 12, 2012

Audit and Finance Committee Members:
Mr. Timothy Sargent, Chair
Mr. Glenn J. Waldman, Vice Chair
Mr. James J. Moran, Member
Mr. Juan M. Portuondo, Member

Re: Audit of the Disaster Recovery Plan
Project No. 11-05

This audit was performed pursuant to the Inspector General's authority set forth in Chapter 20.055, F.S. The objectives focused on determining whether: 1) the District has a comprehensive up-to-date disaster recovery plan, 2) the District has defined locations where the disaster recovery plan could be executed, and 3) the District's Disaster Recovery Plan was periodically tested and any necessary adjustments were incorporated into the plan. The District's business solutions and the importance of the disaster recovery plan were the main focus. Kit Robbins and I prepared this report.

Sincerely,

J. Timothy Beirnes, CPA
Inspector General

TABLE OF CONTENTS

BACKGROUND

In accordance with the Office of Inspector General's Fiscal Year 2011 Audit Plan, we conducted an Audit of the Disaster Recovery Plan. The Disaster Recovery Plan provides support for the District's mission critical systems and infrastructure in case of a catastrophic event to the Primary Data Center in the Emergency Operations Center located at District Headquarters in West Palm Beach, Florida. There are three different Disaster Recovery groups at the District: 1) the Information Technology Infrastructure Systems Section, 2) the Supervisory Control and Data Acquisition (SCADA) Section, 3) and the Emergency Management, Safety and Security Section. Disaster recovery is defined as a number of elements that allow a business to resume operations after a major incident that results in complete interruption of service. The required elements include a hot site or a cold site and restart services. A hot site has all the equipment needed for data applications to continue operations. A cold site is a similar disaster recovery service, but the installation and possible purchase of additional equipment may be needed. A cold site could be a separate building with electricity only and no computer systems. Restart services are resources needed to resume operations. The decision of using a hot site or a cold site is based on the District management's risk tolerance and the cost. The concept of spending resources to protect against threats that may never materialize may seem inefficient in these economic times; yet, it is important to note that the costs of disaster recovery plans is far lower than being unable to resume operations soon after a disaster.

In early 2007, the Information Technology Infrastructure Systems Section created a Project Management Plan for an alternate data center. This provided a hot site with computer systems, network, processing, and storage capacity. A Project Oversight Team identified the primary mission critical systems to include SAP, email, BlackBerry, and WebEOC.[1] The Team identified the need for the Information Technology infrastructure to support a copy of these systems at the site.

In 2007, Network Access Point (NAP) of the Americas in Miami, Florida, was chosen as the alternate data center hot site due to its multiple safeguards and backups as a hosting facility. This alternate site met the minimum separation requirement of 50 miles

[1] WebEOC is the District's web-enabled crisis management system.

required by the Project Management Plan, and the immediate space availability allowed for an implementation prior to the 2007 Hurricane Season. Terremark World Wide, Inc.[2] operates the Network Access Point of the Americas. The District has contracted for 200 square feet of space at a cost of $239,000 annually. The Disaster Recovery Plan Team tests data recovery at the alternate data center in Miami on a semi-annual basis.

The Supervisory Control and Data Acquisition (SCADA) system is a separate information technology system that is not included in the Infrastructure Section's Disaster Recovery Plan. Some Information Technology Bureau employees help with the Supervisory Control and Data Acquisition (SCADA) testing. The backup equipment is located at the Fort Lauderdale Field Station and is tested to ensure that the Microwave Communication Equipment, SCADA Equipment, and Software (Telvent OASyS DNA SCADA Suite) work properly. This test, known as a Telvent OASyS Mode Switch Test, ensures that the District will be able to maintain and operate the Central and South Florida (C&SF) Project structures (control gates and pumps) from the backup facility. This Mode Switch Test is conducted on a semi-annual basis. In case of a total disaster to the Emergency Operation Center / Control Room and the Primary Control Center at District Headquarters, the Supervisory Control and Data Acquisition (SCADA) system operations will be performed at the Backup Control Center located at the District's Fort Lauderdale Service Center.

Lastly, in case of a disaster at the Emergency Operations Center at District Headquarters, the alternate Emergency Operations Center facility for the employees helping the Emergency Management, Safety and Security Section will be relocated to the District's Okeechobee Service Center. The Information Technology Bureau will help align with the District's Business Continuity Plan, which is the business strategy for returning to normal business operations. The "Hurricane Freddy Exercise" is part of testing this Business Continuity Plan, and simulates a hurricane situation at the District. The Continuity of Operations Plan exists at the District as the Business Continuity Plan and is outside the scope of this audit.

[2] Terremark World Wide, Inc. was recently purchased by Verizon Communications, Inc.

OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective of our audit was to determine whether the Disaster Recovery Plan is meeting its goals and is operating efficiently and effectively. Specifically, our objectives focused on determining whether: 1) the District has a comprehensive up-to-date disaster recovery plan, 2) the District has defined locations where the disaster recovery plan could be executed, and 3) the District's Disaster Recovery Plan was periodically tested and any necessary adjustments were incorporated into the plan. The District's business solutions and the importance of the disaster recovery plan were the main focus of the audit.

To achieve our objectives, we gathered evidence through inspections, analyses, and observations of the disaster tests. Recommendations were made where we identified areas for improvement. We interviewed relevant District Disaster Recovery Plan staff responsible for infrastructure support and testing. We reviewed disaster recovery documentation, system documentation, organizational charts, and observed the analyses and testing of the current systems deemed mission critical. The methodology included interviews with system administrators, system owners, and other Disaster Recovery Plan staff to ascertain the status, maturity, and overall efficiency of the Disaster Recovery Plans. The scope included the review of the current efficiency and effectiveness of the Disaster Recovery Plans. The Continuity of Operations Plan exists at the District as the Business Continuity Plan[3] and is outside the scope of this audit.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). These 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[3] Business continuity is a blanket term for measures taken to keep a business running in the face of various threats. It includes disaster recovery, backup, and contingency planning or consulting services.

AUDIT RESULTS

Executive Summary

Overall, our audit revealed that the current Disaster Recovery Plans have improved significantly in comparison to previous plans. There is sufficient planning, budgetary, and project management control processes in place to ensure that the activities and applications support the District's business processes and meet the operational needs after a disaster. Our review of the Disaster Recovery Plans disclosed that progress and continuous improvements have been made through testing and resolving minor issues. All three of the alternate facilities for disaster scenarios are sufficiently fulfilling the objectives of the plans. Mission critical data (SAP, email, BlackBerry, and WebEOC) and Supervisory Control and Data Acquisition (SCADA) system's data are adequately replicated in real-time with only seconds of delay.

The Disaster Recovery Plans are designed to far exceed its current Recovery Time Objective and Recovery Point Objective goals. The basic objectives of Recovery Time Objective and Recovery Point Objective are the starting point of business requirements to help drive the risk and cost of disaster recovery. The Recovery Time Objective is defined as how quickly the systems and services are operational after a disaster. Overall, the District's original Recovery Time Objective is to resume operations within twenty-four hours after a disaster. The Recovery Point Objective is defined as how much data loss is acceptable. Overall, the District's original Recovery Point Objective is eight hours of data loss, (i.e., one day's worth of data loss). SAP, email, BlackBerry, and WebEOC have a Recovery Time Objective of four hours and a Recovery Point Objective of five minutes. Supervisory Control and Data Acquisition (SCADA) systems have a Recovery Time Objective of four hours and a Recovery Point Objective of zero data loss.

Even though the Disaster Recovery Plans are continuously improved and are sufficiently supporting the District's mission critical systems, the following are some additional opportunities we recommend to fully realize the efficiency of the District's investment.

- Consider replacing the alternate data center at the Network Access Point of the Americas in Miami, the Backup Control Center at the Fort Lauderdale Service Center, and the backup Emergency Operations Center at the Okeechobee Service Center with one location. Consider a location 105 miles away from District Headquarters and the feasibility of using other Water Management Districts' facilities in a reciprocity type arrangement.

- Consider integrating all disaster tests in a single Disaster Recovery Strategic Plan.

- Consider assigning the responsibility of coordinating a single Disaster Recovery Plan to an appropriate District Project Manager outside of the Information Technology Bureau.

- Consider incorporating the single Disaster Recovery Plan into the Business Continuity Plan.

- Consider creating a Disaster Recovery Risk Management Oversight Team that defines critical business systems on an annual basis. The District's risk tolerance should be determined to establish what functions are mission critical to resume District operations.

- Determine an updated, acceptable Recovery Time Objective and a Recovery Point Objective for the single Disaster Recovery Plan.

Alternate Disaster Recovery Facilities are Adequate

The Disaster Recovery Plans use three different locations depending on the systems involved and the functionality needed to run different District operations. In case of a catastrophic event at the Emergency Operations Center, the following three locations would be used as alternate sites for disaster recovery. All three alternate facilities appear to be adequate.

- The Network Access Point of the Americas in Miami (Terremark) would be used for SAP, email, BlackBerry, and WebEOC.
- The Fort Lauderdale Service Center would be used for Supervisory Control and Data Acquisition (SCADA) system.
- The Okeechobee Service Center (or optionally the Saint Cloud Field Station) would be used as the Emergency Operations Center for the employees normally in the West Palm Beach Emergency Operations Center.

The current Emergency Operations Center building that houses the Primary Data Center was recently upgraded from a Tier I facility to a near Tier III facility (concurrently maintainable site infrastructure). Construction for the upgrade was completed in February 2012. A Tier III facility is appropriate for companies supporting internal and external clients twenty-four hours a day, seven days a week, such as service centers, but can schedule limited service as acceptable for short periods. A Tier III facility is sometimes used for companies spanning multiple time zones with employees spanning regional areas. Based on Disaster Recovery best practices, the

Network Access Point of the Americas in Miami - Terremark Building. Alternative site for IT Infrastructure Systems.

offsite Disaster Recovery site should have the same physical control and environmental monitoring as the original site, i.e., Emergency Operations Center. It should not be subjected to the same natural disaster as the original site and thus should not be located in proximity of the original site. The Okeechobee Service Center (or optionally the Saint Cloud Field Station) is a Tier I facility that is used as an alternative to the Emergency Operations Center in case of a disaster.

The alternate data center for SAP, email, BlackBerry, and WebEOC systems in the Infrastructure Disaster Recovery Plan is a Tier IV facility at the Network Access Point of the Americas in Miami. A Tier IV facility (fault tolerant site infrastructure) is justified for companies with an international market presence delivering 24 hours a day, 365 days a year services in a highly competitive client-facing market. Also, a Tier IV facility is needed for large, global companies where utilization of information technology provides a competitive advantage. The Network Access Point of the Americas in Miami is a Tier IV facility that is used as an alternative to the near Tier III facility of the Emergency Operations Center.

Disaster Recovery outsourcing of the alternate data center is common for an initial implementation partnership to improve service and efficiency levels, manage internal workload, provide specific expertise, and get the systems ready for a disaster recovery scenario. The Disaster Recovery Infrastructure Section Team has demonstrated that its partnership with Terremark, Inc., and their facility works well. Continued Disaster Recovery outsourcing may be used to add business value, streamline processes, provide staffing augmentation for limited term projects, and provide specific, niche skills. However, the cost of outsourcing the alternate data center must be determined based on District management’s risk tolerance. The District’s management needs to determine its Recovery Time Objective and whether outsourcing the alternative data center is efficient and effective.

For the Supervisory Control and Data Acquisition (SCADA) system, the Disaster Recovery Plan is using the Backup Control Center at the Fort Lauderdale Service Center. This is a sub Tier I to Tier I (basic site infrastructure) facility. A Tier I facility is for businesses with information technology mainly enhancing internal processes and who use a web-presence primarily as a passive marketing tool. An example of a Tier I facility might be a mid-size business with a facility that is safe at a Category Three Hurricane level (111-130 mph winds). The Fort Lauderdale Service Center is a Tier I facility that is used as an alternative to the near Tier III facility of the Emergency Operations Center / Control Room.

Recommendation

1. **Consider replacing the alternate data center at the Network Access Point of the Americas in Miami, the Backup Control Center at the Fort Lauderdale Service Center, and the backup Emergency Operations Center at the Okeechobee Service Center with one location. Consider a location 105 miles away from District Headquarters and the feasibility of using other Water Management Districts' facilities in a reciprocity type arrangement.**

   Management Response:

   Concur: The Information Technology Bureau will consider replacing the current alternate data center at the Network Access Point in Miami with a multi-purpose facility located at least 105 miles away from the District Headquarters. To accomplish this, we will write a Business Case that will summarize the attributes of each option to allow the business to make the selection decision. Upon completion, this information will be forwarded to District senior management for funding consideration. Completion of the Business Case will be completed by June 1, 2012.

   In addition to funding, a multi-purpose facility concept must have agreement between Information Technology, Emergency Management and Operations Control for the purpose and use of such a facility.

   Emergency Management has been in contact with the Emergency Management Director for the Department of Environmental Management (DEP) regarding meeting with the other water management districts on a variety of emergency management issues. We will place this item on the agenda for discussion during this upcoming meeting. This meeting will be completed by June 1, 2012.

Responsible Department:

Information Technology and Emergency Management

Estimated Completion:

June 1, 2012

Testing of the Disaster Recovery Plans

The testing of the Disaster Recovery Plans disclosed the recovery processes across the District have been accomplished. The Disaster Recovery Teams have sufficiently prepared and continuously improved the disaster recovery plan. All significant requirements have been met. There has been a demonstration of the progress by the documented disaster recovery testing procedures and the continuous improvement of the process.

The Disaster Recovery Plans are designed to far exceed its current Recovery Time Objective and Recovery Point Objective goals. The basic objectives of Recovery Time Objective and Recovery Point Objective are the starting point of business requirements to help drive the risk and cost of disaster recovery. The Recovery Time Objective is defined as how quickly the systems and services are operational after a disaster. Overall, the District's original Recovery Time Objective is to resume operations within twenty-four hours after a disaster. The Recovery Point Objective is defined as how much data loss is acceptable. Overall, the District's original Recovery Point Objective is eight hours of data loss, (i.e., one day's worth of data loss). SAP, email, BlackBerry, and WebEOC have a Recovery Time Objective of four hours and a Recovery Point Objective of five minutes. Supervisory Control and Data Acquisition (SCADA) systems have a Recovery Time Objective of four hours and a Recovery Point Objective of zero data loss. We noted that the testing and development process also helps to ensure that the Disaster Recovery Plans' activities support District's mission critical systems and the District's strategic priorities.

Testing of the Infrastructure Disaster Recovery Plan

The Disaster Recovery Infrastructure Section Team plans and executes at least two full tests for the established mission critical systems annually. The lessons learned results in continuous improvements. On January 21, 2011, the first full recovery test was attempted. The Disaster Recovery Infrastructure Section Team performed this test from District Headquarters using the data (SAP, email, BlackBerry, and WebEOC) stored at the Network Access Point of the Americas facility in Miami. Due to minor technical issues, partial tests had to be re-performed in February and March 2011. On April 15, 2011, another full test was attempted at the Miami facility. The test was a complete success, far exceeding the Recovery Time Objective and Recovery Point Objective. The Team did an excellent job of using primary and secondary employees and proved they could execute the Disaster Recovery Plan to recover data. The testing successfully brought data from the systems in Miami back to the original systems at District Headquarters.

All employees performing these tests reside within the Information Technology Bureau and currently no internal customers are involved in the test. Information Technology Bureau internal customers are defined as all District employees that are not in the Information Technology Bureau. An effective Disaster Recovery Plan is driven primarily by planning and involving from relevant District users. Disaster Recovery Plan for a computer system usually focuses on alternative procedures for processing transactions. It is important to delineate these processes that can be put in place while the computer system is not available during the recovery time. It appears there is a misconception that Information Technology is responsible for all of disaster recovery. However, the Information Technology employees are responsible for technical assistance and not for the functionality testing.

Recommendation

2. **Continue using primary and secondary Information Technology employees to execute the Disaster Recovery Plan. Consider requiring internal customers to create the business requirements and test the functionality.**

   Management Response:

   Concur: The Information Technology (IT) Bureau will continue to use primary and secondary Information Technology employees to execute the Disaster

Recovery plan where there is sufficient staff and skill set available. We will request the involvement of the business community in the disaster testing process at an early stage and during the Disaster Recovery test to ensure their specific needs are addressed and tested, and to increase our resilience to a disaster's impact. We will also request that internal customers create the business requirements. Information Technology is planning an IT-only Disaster Recovery test involving our remote site by February 4th 2012, and a more comprehensive test involving our remote site plus relevant IT customers by June 1st 2012.

Responsible Department:

Information Technology

Estimated Completion:

June 1, 2012

Testing of the Supervisory Control and Data Acquisition (SCADA) Disaster Recovery Plan

The Disaster Recovery Team for Supervisory Control and Data Acquisition (SCADA) (the "SCADA Team") system plans and executes at least two full mode switch tests annually. The lessons learned results in continuous improvements. On April 14, 2011, we observed the first partial mode switch test that was attempted. It was successful with some minor technical issues. The SCADA Team performed this test from District Headquarters. On May 25, 2011, we observed a full mode switch test that included the elimination of the microwave connectivity in the B66 building at the West Palm Beach Headquarters. The SCADA Team performed this full test using the Backup Control Center at the Fort Lauderdale Service Center. There were issues with retrieving some of the data at the Backup Control Center. Telvent, the software vendor, helped address the issues with the District Team. On June 29, 2011, we observed another full mode switch test conducted using the Backup Control Center at the Fort Lauderdale Service Center. Again there were minor issues; for example, slowness of retrieving data was caused by inconsistent system configuration. This issue was resolved by reviewing the error event log and the configuration has now been synchronized. Again, there were additional lessons learned and minor issues were addressed, but the ability to open and close flood gates and executing the District's core mission of flood control was a success. The SCADA Team showed continued improvement through the tests and engaged water managers as well as other relevant District staff during execution of the test at the Backup Control Center.

Recommendation

3. **Consider integrating all disaster tests to a single Disaster Recovery Strategic Plan.**

Management Response:

Concur: The Emergency Management Section is responsible for District-wide emergency management planning activities using an "all hazards" approach. The two primary planning documents related to this recommendation are the Comprehensive Emergency Management Plan (CEMP) and the Continuity of Operations Plan (COOP). Each of these plans have a specific language to address disaster recovery strategic planning activities. To better ensure the importance of emergency procedures associated with the alternate data center, Emergency Management will add specific language related to this topic to both the COOP and CEMP. This information will be added by June 1, 2012.

Each year during the Hurricane Freddy Exercise the Emergency Management Section designs the exercise scenario to test and validate identified plans, procedures and activities. We have in the past and will continue to build in exercise goals and objectives related to this recommendation. The Hurricane Freddy Exercise is scheduled for June 5th and 6th in 2012. Prior to the exercise we will test the Network Access Point data transfer capabilities and the results will be included in the Freddy After-Action Report.

Responsible Department:

Emergency Management

Estimated Completion:

June 10, 2012

Business Requirements and Business Involvement Needed

As there is value in having different quality disaster recovery tests for separate information systems and a business need for these mission critical Disaster Recovery Plans, the business requirements and involvement used to support these tests need some improvement. It appears the leaders of the different business processes had little involvement with the requirements and execution of the information used for the Disaster Recovery Plans. Also, the prioritization of these business critical systems is not continually reviewed by a steering committee.

In general, the Information Technology Strategic Plan and the District-wide governance vision delineate a standard for the involvement of the internal customers when it comes to disaster scenarios. This establishment by management allows leadership to make knowledgeable decisions in regards to future priorities for internal customers. However, internal customers are not always involved. Portfolio management manages the risk and the value to the internal customers of projects. District-wide governance best practices use a business case and portfolio management to prioritize projects. Projects with extended timeframes and expanded needs of scope increase the degree of risk and cost for the District. The main benefit of addressing the management leadership with the challenge of having internal customer involvement is that the District will show District-wide governance vision with prioritized projects. Disaster recovery, backup, and contingency planning are elements of the bigger Business Continuity Plan. The Information Technology Bureau assists with the Business Continuity Plan, but should not be the core group for measures taken to keep a business running in the face of various threats. This should be a business owner outside of the Information Technology Bureau.

Recommendations

4. **Consider assigning the responsibility of coordinating a single Disaster Recovery Plan to an appropriate District Project Manager outside of the Information Technology Bureau.**

   Management Response:

   Concur: Emergency Management has this responsibility currently. Plans are developed in the Emergency Management Section that has District-wide application. However, each Bureau/Section within the District is responsible for developing operational procedures that will explain "how" these plans will be executed. Each of these groups has Standard Operating Procedures (SOP) Coordinators that work very closely with Emergency Management to ensure conformity and applicability with umbrella District-wide plans. Emergency Management reviews procedures and meets with the SOP Coordinators periodically. Emergency Management will continue to work with the IT Bureau to ensure applicable emergency plans and procedures are updated and tested.

   Responsible Department:

   Emergency Management

   Estimated Completion:

   On-going

5. **Consider incorporating the single Disaster Recovery Plan into the Business Continuity Plan.**

   Management Response:

   Concur: As required by Florida Statutes, Chapter 282: *Communications and Data Process* is an Annex to the District's Continuity of Operations Plan (COOP). The IT Bureau will provide the Information Technology Disaster Recovery Plan to Emergency Management for review. Emergency Management will review this Annex to determine what additional information should be included to strengthen the COOP.

Responsible Department:

Information Technology and Emergency Management

Estimated Completion:

March 30, 2012

Disaster Recovery Risk Management Oversight Team Needed

A formal Disaster Recovery Risk Management Oversight Team has been lacking since the original reorganization of the Information Technology Bureau about seven years ago. The original process that was used to create a Disaster Recovery Plan was to discuss issues multiple times at the Information Technology Steering Committee meetings to obtain consensus about critical applications and systems. This committee was made up of Section Leaders from various areas. Also, special meetings were held with the SAP management and the WebEOC management. The original meetings did include the Section Leader of Emergency Management, Safety and Security because this Section is responsible for the Business Continuity Plan and the Hurricane Freddy Exercise. A Disaster Recovery Risk Management Oversight Team Meeting should be held annually, at a minimum. The main mission for this committee should be to create a realistic Recovery Time Objective and a Recovery Point Objective.

Once the decision to appoint a Disaster Recovery Risk Management Oversight Team has been finalized, an executive owner should be appointed as the Project Sponsor with additional accountable members outside the Information Technology Bureau. The District has multiple Disaster Recovery Plans and locations without direct and continuous "steering" from upper management when it comes to the definition of true mission critical systems and the risk tolerance of the District's functionality and operations of these systems. The Recovery Time Objective and Recovery Point Objective requirements should help define the risk and influence the cost. The longer Recovery Time Objective drives a higher disaster tolerance and a lower cost.

Recommendation

6. **Consider creating a Disaster Recovery Risk Management Oversight Team that defines critical business systems on an annual basis. The District's risk tolerance should be determined to establish what functions are mission critical to resume District operations.**

   Management Response:

   Concur: The Information Technology Bureau will champion this activity to the leadership team as part of other Information Technology Steering Committee matters to be considered. We will recommend that this body address the subject of Disaster Recovery prioritization at least once per year.

   The District's Comprehensive Emergency Management Plan (CEMP) allows the Director of Emergency Management to appoint an Emergency Management Advisory Committee. Emergency Management is in the process of assembling this Committee. As part of the committee structure we will add representative(s) from the IT Bureau to ensure these recommendations are addressed. The Committee will be assembled and meet by April 15, 2012. The Committee will review the information and make recommendations to the IT Bureau Chief and Emergency Management Director by July 27, 2012.

   Responsible Department:

   Information Technology and Emergency Management

   Estimated Completion:

   July 27, 2012

7. **Determine an updated, acceptable Recovery Time Objective and a Recovery Point Objective for the single Disaster Recovery Plan.**

   Management Response:

   Concur: The Information Technology Bureau will provide definitions of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to the

Emergency Management Advisory Committee (see recommendation 6) and ask that defining acceptable measures for the District's business recovery be assigned.

In general, RTO is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences, or the acceptable amount of time to restore the function. The RPO is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The business leadership team will ultimately set the RTO and RPO metrics to fit within the available resources. The RPO time period and the RTO time duration will be completed and included along with Audit Recommendation #4 and #6.

When recommended by the IT Bureau, Emergency Management will provide the information to the Emergency Management Advisory Committee for final approval. Once approved, the information will be provided to the Emergency Management Director for inclusion in appropriate planning documents.

Responsible Department:

Information Technology and Emergency Management

Estimated Completion:

September 30, 2012

Adequate Change Control and System Stability

Overall, the Change Control process for the Disaster Recovery environments are being handled adequately by the Disaster Recovery Teams using the Information Technology Infrastructure Library methodology of Change Control. There are regular Change Control meetings and normal approved changes are being implemented through the appropriate Information Technology Change Control process. For normal schedules and changes to the Disaster Recovery tests, the users are required to document and signoff on the changes prior to these being moved/tested in the production environments.

The System Stability for the Disaster Recovery Plan systems, specifically SAP, email, and WebEOC, has been an extremely stable environment since the use of the

Network Access Point of the Americas in Miami. A live disaster recovery scenario has yet to be moved to the Miami facility. In 2009, the System Stability of the Supervisory Control and Data Acquisition (SCADA) systems was moved by successfully transferring data to the Backup Control Center at the Fort Lauderdale Service Center. The Information Technology Bureau has partnered to create the Disaster Recovery Plan Teams that mitigate the risk of the systems interruptions. Downtime and normal change request windows have been minimal for most of the critical systems and the testing of the plans have been communicated well in advance with the District business solutions being able to maintain adequate service levels.