MEMORANDUM

Washington
Metropolitan Area
Transit Authority

FINAL AUDIT REPORT WITH RECOMENDATIONS
Information Technology No. 11-001

SUBJECT: Review of Emergency Plans for Critical Information Technology Operations and Financial Systems

DATE: September 24, 2010

FROM: IG/OIG – Helen Lew /s/

TO: DGMA/CFO – Carol Kissal

This **Final Audit Report** entitled, *Review of WMATA's Emergency Plans for Critical Information Technology Operations and Financial Systems*, presents the results of our audit. The objectives of the audit were to determine (1) the status of WMATA's Department of Information Technology's (IT) contingency plans for critical information technology operational and financial systems, as well as the risks of not having fully developed plans, and (2) the status of WMATA's disaster recovery back-up facility and the risk associated with not having a fully operational back-up facility.

BACKGROUND

WMATA's IT systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.,* short-term power outage and disk failure) to severe (*e.g.*, equipment destruction and fire). The vulnerability risk may be minimized through technical, management, or operational solutions as part of the organization's risk management effort. It is generally not possible to completely eliminate all risks.[1] Emergency planning is designed to mitigate the risk of system and service unavailability by focusing on effective and efficient recovery solutions. WMATA is currently developing its Continuity of Operation Plans (COOP) for Headquarters, see definition below. The IT COOP will be the first plan updated, and this plan will be used as a model for other Headquarters' departments. The IT COOP is only one of the types of contingency-related

[1] For example, critical resources may reside outside the organization's control (such as electric power or telecommunications outages due to an earthquake), and the organization may be unable to ensure availability.

plans that should be considered in the IT contingency planning process. IT contingency planning represents a board scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning should fit into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning.

The National Institute of Standards and Technology's (NIST), *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, outlines some methodologies and types of plans that are recommended in the event of an IT service interruption. Three types of emergency plans outlined in that publication are discussed below.

> **IT Contingency Plan -** An IT contingency plan considers continuity of support for each major application and general support system, including activities designed to recover and sustain critical IT services following an emergency. These arrangements include organizational and business process continuity and recovery planning.
>
> **Disaster Recovery Plan (DRP) -** A DRP applies to major and usually catastrophic events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.
>
> **Continuity Of Operations Plan (COOP) -** A COOP focuses on restoring an organization's (usually a headquarters element) essential functions at an alternate site, and performing those functions for up to 30 days before returning to normal operations. Because a COOP addresses headquarters-level issues, it is developed and executed independently from other types of emergency plans. A COOP cannot be substituted for an IT Contingency Plan, but the IT Contingency Plan(s) can supplement the COOP as an attachment(s). The COOP is for systems that are critical to supporting an organization's infrastructure and is not just IT focused.

Two “Single Audit Reports” for fiscal years 2008 and 2009 of WMATA‘s Financial Statement indentified that there is no disaster recovery plan to facilitate recovery of business operations in case of a disaster. This issue was also cited in fiscal year 2010 by our external auditors in a Management Letter addressed to the Board of Directors. Further, in conducting our audit review, we applied the COBIT[2] and NIST methodologies.

AUDIT RESULTS

We found that: (1) WMATA has not fully developed IT contingency plans for critical IT operational and financial systems and, as a result, there is a risk of costly service interruptions; and (2) WMATA‘s disaster recovery back-up location at the Carmen Turner Facility is not fully operational, and redundant processing of critical applications cannot be performed, which further increases the risk of service interruptions.

Based on the above findings, we made five recommendations to the Deputy General Manager Administration/Chief Financial Officer (DGMA/CFO).

In the DGMA/CFO’s September 20th, 2010, response to a draft of this report, she indicated general agreement and concurrence with our findings and recommendations. The complete text of the DGMA/CFO response is included as Attachment I of this report.

Finding 1- WMATA Does Not Have Fully Developed IT Contingency Plans

WMATA has not fully developed IT contingency plans that are IT-focused and considers continuity of support for each major application and general support system, including activities designed to recover and sustain critical IT services following an emergency. Currently, WMATA has only an interim IT COOP that is still under development.

WMATA has been working with the Federal Emergency Management Agency (FEMA) and their consultant, Excalibur Management and Associates (EMA), to develop a COOP for IT. The COOP, once developed, will be headquarters-

[2] COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks. COBIT enables clear policy development and good practice for IT controls throughout organizations.

focused and limited to restoring essential headquarters' functions at an alternate site for up to 30 days before returning to normal operations. A date for the completion of the COOP has not been determined.

According to COBIT, the need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage, and providing periodic continuity plan training.

Although the current IT COOP under development addresses some risk areas, it does not contain fully developed contingency and DRP plans, which are essential elements of a COOP. Fully developed contingency plans help to alleviate other risks, and they consider each major application and general support system. Appendix I compares COBIT standards for an IT contingency plan to those elements not covered and/or missing in WMATA's IT COOP.

Properly designed plans address how to recover and sustain critical IT services following an emergency. The lack of fully developed and tested IT contingency plans increase WMATA's risk of costly IT service interruptions resulting from mild (*e.g.*, short-term power outages and disk failure) to severe (*e.g.,* equipment destruction and fire). As an example, MAXIMO[3] does not have a fully developed IT contingency plan. Without a fully developed contingency plan, the following IT systems and operations could be affected during a service interruption:

- PeopleSoft,
- Bus Maintenance,
- Rail Maintenance,
- Bus Operations Control Center,
- Operations Control Center,
- Track Systems Service Maintenance,
- Rail Operations Control System, and
- Facilities Management.

The above systems all interface with MAXIMO and have a range of approximately 300-3,000 users over a 24-hour period. A disruption of MAXIMO for a period exceeding 24 hours increases the risk that WMATA will be restrained from access to critical production data. In a worst-case scenario,

[3] MAXIMO is an IT system application considered by IT to be "Mission Critical" to WMATA operations.

data may be lost if MAXIMO is not restored within three days. A failure of that system could potentially cripple WMATA's essential business processes and hinder daily operations.

PeopleSoft is also considered by IT to be "mission critical" to WMATA operations. The PeopleSoft application is used to support critical business processes for multiple WMATA users. Without a fully documented and tested IT contingency plan for PeopleSoft, some operations, such as Accounting, Payroll, Human Resources, and even MAXIMO, could be affected. If a service interruption last longer than five days, there is a risk that PeopleSoft data would be lost, and WMATA's business processes and financial operations could be severely hampered or halted. As outlined in Appendix I, IT does not have fully documented contingency and DRP plans that addresses some key areas that should be considered.

Although IT personnel are taking training workshops that are focused on the COOP development, IT management stated that IT personnel working on the COOP have not had prior training on some important aspects of emergency planning, such as developing a contingency plan and DRP. In addition, based on our discussions with IT management and a FEMA/EMA representative, IT may not have the proper expertise to distinguish the difference between a COOP, an IT Contingency Plan, and a DRP.

The failure to have fully developed contingency plans that address all of the necessary elements of each major application and general support system increases the risk of service interruptions.

<u>Recommendations</u>

We recommend that the AGM/CIO:

1.1 Establish an estimated completion date for completing an IT COOP;

1.2 Ensure IT personnel fully develop contingency plans, including a DRP for critical IT operational and financial systems that considers each major application and general support system, and incorporate those plans into the COOP.

1.3 Ensure IT personnel developing the COOP and other emergency plans have the requisite expertise.

Management Comment

Management concurred with our finding and stated that when the CIO arrived in 2007, WMATA had an existing COOP that covered all WMATA departments including IT. However, the CIO and the Emergency Management Agency (EMA) determined that the existing plan was inadequate.

Management stated that as a joint effort, IT and EMA have developed a comprehensive and updated COOP that covers all WMATA departments including IT. At the time of this audit, this process had not been completed. Management also stated that the IT contingency plan is now incorporated in the IT COOP and IT Disaster Recovery Plan. The newly revised WMATA COOP was completed July 2010, and WMATA's EMA retained the services of an Industry Professional Subject Matter Expert to assist WMATA in developing the COOP and DRP.

OIG's Comment

Although IT management concurs with our finding, IT did not submit a copy of their revised COOP, contingency plan, and DRP for our review. Therefore, we did not evaluate the adequacy of those plans.

Finding 2 – WMATA's Disaster Recovery Back-up Location at the Carmen Turner Facility (CTF) Is Not Fully Operational

We found that WMATA's disaster recovery back-up location at the CTF is not fully operational, and IT cannot perform back-up processing of the major critical applications.

According to COBIT, control over the IT process of ensuring continuous service that satisfies the business requirements of making sure IT services are available, as required, and to ensure a minimum business impact of a major disruptions can be enabled by, among other things, back-up and recovery.

The CTF Data Center has been designated as the disaster recovery back-up location for the Headquarters' Jackson Graham Building (JGB) Data Center. Although the majority of the hardware has been installed at the CTF back-up location, IT still does not have the necessary software needed for redundant processing of critical applications (PeopleSoft, Maximo, Fare Collections, etc). The original milestone date for completion of the back-up center was August

2009. According to IT, the reason for the delays is the lack of available funds for software needed for redundant processing of mission-critical systems; this will be available in fiscal year 2011.

The former Chief of the IT Data Center and Infrastructure (DCI) told us that another reason for the delay in completing the back-up center is because the original construction of the back-up facility did not meet IT specifications. In September of 2009, IT submitted a "Non-Conformance Report" to the Office of Infrastructure Renewal Program Group's (IRPG),[4] identifying deficiencies that deviated from the original design and construction.

However, an IRPG official stated that the construction was completed based on the original specifications signed-off by the AGM/CIO in January 2008. IRPG said that IT changed the original specifications after the project had started. We did not validate the IRPG official's statement.

According to documents that we reviewed, in fiscal year 2009, $7.4 million was budgeted for redesign of both the JGB and CTF Data Centers. Approximately $3.2 million was spent for construction and equipment at the CTF Data Center. Aside from the $3.2 million, IRPG spent an additional $200,000 for the construction of the new CTF data center, bringing the total cost to about $3.4 million as of March 24, 2010. About $4.2 million was used for equipment at the JGB Data Center.

IT has not provided a new milestone date for when the CTF back-up Data Center will be fully operational.

The failure to have a fully operational back-up site increases the risk of not being able to provide IT services in a timely manner if a catastrophic event occurs that affects critical systems, applications, and business operations at the JGB Data Center.

[4] The Office of Infrastructure Renewal Programs (IRPG) is responsible for the planning, design, project management, installation, testing and commissioning for bus rail infrastructure renewal projects for facilities, electrical, mechanical, and structural projects.

Recommendations:

We recommend that the AGM IT/CIO:

2.1 Direct IT personnel to work with appropriate WMATA personnel to address operational issues to ensure the CTF Data Center is fully operational and capable of ensuring redundancy of WMATA's mission critical applications, systems, hardware, and network/data equipment.

2.2 Establish an estimated completion date for when the CTF will be fully operational.

Management Comment

Management concurred with our finding and stated that the CTF site is WMATA's secondary Data Center. IT has addressed all relevant internal Data Center operational issues to support operational readiness. Testing and training are scheduled to conclude by March 2011. The center will be fully operational in March 2011.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of the audit were to determine (1) the status of WMATA's IT Contingency Plans for critical information technology operational and financial systems, as well as the risks of not having fully developed plans; and (2) the status of WMATA's Disaster Recovery back-up facility and the risk associated with not having a fully operational back-up facility.

We focused our review of contingency planning on the following critical systems: Maximo, PeopleSoft, Rail Fare Collection System, IT Network Communication Systems, and IT security. We toured various user operations that are dependent on IT service for continued operations and interviewed user personnel at the various sites. We visited the disaster recovery back-up location at the CTF. We interviewed FEMA/EMA, IRPG, and key IT personnel. We reviewed documents relating to the COOP and the COOP currently being worked on by FEMA and its contractor, EMA. We also reviewed materials on a DRP and contingency plans. We used COBIT and NIST as criteria in our analysis.

We conducted our field work from April 15, 2010, to June 4, 2010. We held an exit conference with agency officials to discuss our preliminary findings on August 16, 2010.

We conducted our audit in accordance with *Government Auditing Standards,* appropriate to the scope. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the functions under audit. An audit includes assessments of applicable internal controls and compliance with requirements of laws and regulations when necessary to satisfy our audit objectives.

ADMINISTRATIVE MATTERS

Corrective actions proposed (resolution phase) and implemented (closure phase) by CFO will be monitored and tracked through the OIG's audit Accountability and Resolution Tracking system. Department policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth specific action items and targeted completion dates necessary to implement final corrective actions on the findings and recommendations contained in this report.

We appreciate the cooperation and assistance extended by your staff during our audit. Should you have any questions, please contact Andrew Clemmons, Assistant Inspector General for Audits, on (202) 962-1014 or me on (202) 962-2515.

Attachment

cc: CIO –Suzanne Peck
DGMO –Dave Kubicek
COUN –Carol A. O'Keeffe
CHOS –Shiva Pant

Appendix I.

COBIT Delivery and Support Section 4 - Ensuring Continuous Service (Note that audit analysis was done from 11/25/009 until July 31, 2010)

COBIT Standards for IT Contingency Plans	WMATA IT COOP current status
1. Emergency procedures to ensure the safety of all effected staff members.	Not completed in IT COOP, this is still in development.
2. Roles and responsibilities of the IT function, vendors providing recovery services, users of services, and support administrative personnel.	Roles and responsibilities partially defined, everything else is not completed in IT COOP.
3. A recovery framework consistent with a long-range plan for continuity.	Not completed in IT COOP, this is still in development.
4. Listing of systems resources requiring alternatives (hardware, peripherals, and software).	Not completed in IT COOP, this is still in development.
5. Listing of highest to lowest priority applications, required recovery times, and expected performance norms.	Not completed in IT COOP, this is still in development. A listing was created but not ranked from high to low.
6. Administrative functions for communicating and providing support services, such as benefits and payroll, external communications, cost tracking, etc., in event of a need to recover.	Not completed in IT COOP, this is still in development.
7. Various recovery scenarios from minor to loss of total capability and response to each in sufficient detail for step-by-step execution.	Not completed in IT COOP, this is still in development.
8. Specific equipment and supply needs are identified, such as high speed printers, signatures, forms, communications equipment, telephone, etc., and a source and alternative source defined.	Not completed in IT COOP, this is still in development.
9. Training and awareness of individual and group roles in the continuity plan	Not completed in IT COOP, this is still in development.

10. Testing schedule, results of last test, and corrective actions taken based on prior test(s).	Not completed in IT COOP, this is still in development.
11. Itemization of contracted service providers, including services and response expectations.	Not completed in IT COOP, this is still in development.
12. Logistical information on location of key resources, including back-up site for recovery of operating system, applications, data files, operating manuals, and programming/ system/user documentation.	Not completed in IT COOP, this is still in development. Back-up site (CTF Data Center) is not fully operational.
13. Current names, addresses, telephone number/cell/pager numbers of key personnel.	Completed in IT COOP, but this is still in development.
14. Reconstruction plans are included for re-recovery at original location of all systems resources.	Not completed in IT COOP, this is still in development.
15. Business resumption alternatives for all users for establishing alternative work locations once IT resources are available, i.e. system recovered at alternative site but user building is unavailable.	Not completed in IT COOP, this is still in development.