TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made

February 29, 2008

Reference Number: 2008-20-061

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-622-6500
Email Address | inquiries@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 29, 2008

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Nancy A. Nakamura

FROM: *(for)* Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit # 200720005)

This report presents the results of our review to determine the effectiveness of the corrective actions taken to resolve the previously reported disaster recovery material weaknesses.[1] This review was part of the Treasury Inspector General for Tax Administration Fiscal Year 2007 Annual Audit Plan coverage.

Impact on the Taxpayer

The Internal Revenue Service (IRS) declared the Disaster Recovery Program[2] a material weakness in March 2005 and is taking several actions to improve the Program. However, Disaster Recovery Program weaknesses have not been effectively resolved. As a result, the IRS cannot ensure minimal disruption to tax administration activities, which include the collection of approximately $2.7 trillion in revenue for the Federal Government and processing of more than 228 million tax returns.

Synopsis

Treasury Directive 85-01, Information Technology Security Program, dated February 13, 2003, states the Bureau Chief Information Officers shall designate a point of contact to coordinate all policy issues related to information systems security. The Federal

[1] See Appendix V for a Glossary of Terms.
[2] The Disaster Recovery Program serves to facilitate cross-organizational buy-in, participation, concurrence, and communication of all IRS disaster recovery activities.

Information Security Management Act (FISMA)[3] requires Federal Government agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the disruption or destruction of information. Disaster recovery is an organization's ability to respond to an interruption in services by implementing a plan to restore critical business functions.

In March 2005, we reported[4] significant Disaster Recovery Program weaknesses continued to be unresolved and determined that 27 of 44 corrective actions for prior audit recommendations in the Program had not been completed. Therefore, we recommended, and the IRS agreed, the Disaster Recovery Program should be reported as a material weakness.

Since declaring the Program as a material weakness in March 2005, the IRS has effectively implemented some corrective actions to address prior audit recommendations and has taken other constructive measures to help ensure future progress toward ultimately resolving the material weakness. For example, on October 1, 2006, the IRS incorporated disaster recovery into the overall Computer Security Material Weakness Plan,[5] identifying five corrective action components. In December 2006, the Chief Information Officer listed the completion of corrective actions to demonstrate progress in resolving the Computer Security Material Weakness as one of the Chief Information Officer Commitments for Calendar Year 2007. Finally, in October 2007, the IRS formed a new Disaster Recovery Program Office within the Modernization and Information Technology Services organization's Cybersecurity organization to provide oversight, accountability, and responsibility for developing and maintaining the IRS Enterprise Disaster Recovery Strategy.

Several actions have been taken to address Disaster Recovery Program weaknesses. However, corrective actions to address prior audit recommendations and material weakness components have not been effectively implemented.

We also determined that some corrective actions taken by the IRS in addressing prior audit recommendations have not been effectively implemented. For example, copies of the disaster recovery plans were not stored at the recovery sites' offsite storage facilities or centralized in designated electronic file locations. In one disaster recovery exercise, participants used a combination of the Disaster Recovery Exercise Plan (because a Disaster Recovery Plan was not available) and individual reference material they had brought to the exercise to recover the system(s). Evidence supporting announced, unannounced, and annually planned tests of the offsite storage vendors' ability to timely deliver all backup files and documentation to the

[3] The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[4] See report #12 in Appendix IV.
[5] Computer Security Material Weakness Plan, IRS-2A-01-01, as Material Weakness Area 1-6, Information Technology Contingency Planning.

disaster recovery site was not available. Finally, documentation was not provided to support the disaster recovery training strategy.

Our review of the disaster recovery-related Computer Security Material Weakness Plan corrective actions determined the actions have not been effectively implemented. We identified a major information technology system directly supporting 4 of the 25 critical processes[6] and cited as having an Information Technology Contingency Plan. However, the system did not have an Information Technology Contingency Plan. The gap analysis (originally due October 1, 2005) of the current Modernization and Information Technology Services organization business resumption capabilities against business unit requirements, including both Recovery Point Objectives and Recovery Time Objectives, for all major systems has not been completed. Items notated as critical in disaster recovery exercise summary reports were not always addressed in subsequent year testing. Disaster recovery plan documentation is not standardized, complete, or accurate. Finally, the IRS is not currently collecting and reporting metrics to assess progress and track improvements within the Disaster Recovery Program.

Recommendations

The Chief Information Officer should ensure all Disaster Recovery Plan documentation is standardized, complete, accurate, readily accessible in the event of disaster, detailed enough to be used verbatim to react to a worst-case scenario, and reviewed quarterly; ensure effective completion of tasks as required in disaster recovery guidance incorporated in the Internal Revenue Manual from the Office of Management and Budget, National Institute of Standards and Technology, and the FISMA; ensure offsite storage vendors' ability to timely deliver all disaster recovery backup files and documentation to the disaster recovery site using announced, unannounced, and annually planned tests; ensure appropriate disaster recovery site personnel are identified and provided with annual training to ensure they have the ability to implement the Disaster Recovery Plan; ensure disaster recovery exercise lessons learned or action items deemed as critical are included in subsequent exercises; and ensure a permanent file is established for keeping documentation supporting closure of prior recommended corrective actions and completion of material weakness corrective action plan components related to the Information Technology Contingency Planning material weakness.

Response

IRS management agreed with our recommendations. Planned corrective actions include ensuring all Disaster Recovery Plan documentation is standardized, accurate, comprehensive, appropriately detailed, up-to-date, and written in a clear, cohesive format; ensuring the

[6] Eighteen critical business processes and seven critical administrative or infrastructure processes.

accessibility and availability of all Plan documentation; developing a comprehensive Disaster Recovery Internal Revenue Manual and ensuring all program-related documentation adheres to and complies with all relevant Federal Government guidance; ensuring effective completion of tasks as required in the Internal Revenue Manual; implementing a repeatable process that includes an Information Technology Contingency Plan/Disaster Recovery Test Guide and Checklist; developing a comprehensive disaster recovery specific training curriculum and training all individuals who have disaster recovery responsibilities; developing a database as training is completed to provide an assessment report to management for use in evaluating training progress, qualified personnel, and skill-set risks; and developing a repeatable process to ensure subsequent exercises include lessons learned or action items deemed as critical. Management also established the Modernization and Information Technology Services organization's Information Technology Disaster Recovery organization. The responsibilities of this program office include validating all closure activities for corrective actions and collecting and maintaining all documentation that supports closure and/or mitigation of all corrective actions, material weaknesses, and any outstanding year-to-year weaknesses remediation recommendations. Management's complete response to the draft report is included as Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Abbreviations

ECC	Enterprise Computing Center
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service

Background

Disaster recovery is an organization's ability to respond to an interruption in services by implementing a plan to restore critical business functions. In March 2005, we reported[1] significant Disaster Recovery Program[2] weaknesses continued to be unresolved and determined that 27 of 44 corrective actions for prior audit recommendations in the Program had not been completed. Therefore, we recommended and the Internal Revenue Service (IRS) agreed that the Disaster Recovery Program should be reported as a material weakness[3] and should include the following actions:

1. Obtain Modernization and Information Technology Services organization, Mission Assurance and Security Services organization (recently renamed to Cybersecurity and moved under the Modernization and Information Technology Services organization), and business unit executive support for the establishment of Business Resumption Strategy[4] and Disaster Recovery Strategy effort due dates and the monitoring and reporting of the progress and status of the efforts.
2. Complete the Business Resumption Strategy and Disaster Recovery Strategy efforts and identify the Modernization and Information Technology Services organization disaster recovery requirements (including Modernization requirements).
3. Conduct a gap analysis to identify the difference between the Modernization and Information Technology Services organization disaster recovery requirements and current capabilities.
4. Coordinate with IRS, Department of the Treasury, and Office of Management and Budget management to obtain the resources needed to correct the material weakness.

Disaster recovery is an organization's ability to respond to an interruption in services by implementing a plan to restore critical business functions. Based on reported significant Disaster Recovery Program weaknesses, the IRS reported the Program as a material weakness.

[1] See report #12 in Appendix IV.
[2] The Disaster Recovery Program serves to facilitate cross-organizational buy-in, participation, concurrence, and communication of all IRS disaster recovery activities.
[3] See Appendix V for a Glossary of Terms.
[4] The Chief, Agency-Wide Shared Services, is responsible for the overall IRS Business Resumption Strategy and the Associate Chief Information Officer, Management, is responsible for the Modernization and Information Technology Services organization's Business Resumption Strategy.

In March 2005, the IRS declared the Disaster Recovery Program a material weakness. On October 1, 2006, the IRS incorporated disaster recovery into the overall Computer Security Material Weakness Plan, IRS-2A-01-01, as Material Weakness Area 1-6, Information Technology Contingency Planning. Figure 1 describes the five material weakness corrective action components.

Figure 1: Material Weakness Corrective Action Components

Corrective Action Component	Description
Information Technology Contingency Plan prioritization	Maintain a prioritized list of critical information technology systems that support critical business processes and ensure Information Technology Contingency Plans exist for these systems.
Establish recovery capability	Develop and maintain Information Technology Contingency Plans associated with general support systems to include all components that support critical applications, establish and maintain data and processing backup-recovery capability, and ensure maximum allowable outage times meet the recovery time objectives of the applications being supported.
Disaster Recovery Plan test and exercise development	Develop baseline expectations and requirements for Disaster Recovery Plan and Disaster Recovery Plan tests and exercises. Identify roles and responsibilities for documenting the Disaster Recovery Plan and Disaster Recovery Plans testing requirements. Also, identify the frequency and type of testing required and reporting requirements.
Test and review adequacy of plans	Conduct both desktop and end-to-end disaster recovery tests for critical applications. Perform annual system risk assessments to promote and track Information Technology Contingency Plan and Disaster Recovery Plan improvements.
Material weakness area metrics	Establish and maintain collection and reporting of metrics to assess progress and track improvements in all component activity implementations over time.

Source: The IRS Computer Security Material Weakness Plan, IRS-2A-01-01, dated October 1, 2006.

This review was performed at the Modernization and Information Technology Services organization offices in New Carrollton, Maryland; Martinsburg, West Virginia; Memphis, Tennessee; and Atlanta, Georgia, during the period March through October 2007. We conducted this performance audit in accordance with generally accepted government auditing standards. Those 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. This review was part of the Treasury Inspector General for Tax Administration Fiscal Year 2007 Annual Audit Plan coverage under the major management challenge of Security of the IRS. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Several Actions Have Been Taken to Address the Disaster Recovery Program Weaknesses

Treasury Directive Number 85-01, *Department of the Treasury Information Technology (IT) Security Program*, dated February 13, 2003, states the Bureau Chief Information Officers shall designate a point of contact to coordinate all policy issues related to information systems security (including information technology security, operational security (threats and vulnerability assessments), emissions security, certificate management, electronic authentication, continuity planning, and critical infrastructure protection. Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004, requires agencies to take timely and effective action to correct management control deficiencies and to complete implementation of agreed corrective actions within 1 year to the extent practicable.

Our review of implemented corrective actions to address prior audit recommendations determined the IRS effectively implemented some of the corrective actions. For example:

1. In a March 2004 audit report,[5] we recommended the Chief Information Officer implement cost-effective solutions that would reduce the time needed to restore the Master File to the 36 hours required for critical business processes by revising the Master File backup procedures and Master File Disaster Recovery Plan to provide for storage of the disaster recovery backup files and documentation at the Enterprise Computing Center (ECC)-Memphis. The corrective action agreed to for this recommendation was effectively implemented. We verified the ECC-Martinsburg is using a process for shipping a copy of the Master File operating system files to the ECC-Memphis weekly.

   We also recommended the Chief Information Officer ensure disaster recovery tests are based on catastrophic scenarios and include tests integrated with the recoveries of interdependent systems. The recommendation was addressed. The IRS added the following systems to the Computing Center disaster recovery tests: the Automated Collection System (a mainframe-based system) in October 2004; the Customer Accounts Data Engine (a Tax Systems Modernization system) in September 2006; and the Automated Underreporter system (a mid-range computer system) in July 2007.

[5] See report #6 in Appendix IV.

2. In an April 2004 audit report,[6] we recommended for the offices reviewed (ECC-Martinsburg, ECC-Memphis, Atlanta Campus, and Atlanta Territory) that the Chief Information Officer ensure each site perform at least one exercise of each Disaster Recovery Plan element annually. The recommendation was addressed. We verified each office is conducting annual disaster recovery testing.

The IRS also annually performs comprehensive disaster recovery exercises to test recovery of systems and operations at its three Computing Center locations and is performing periodic stand-alone exercises for some critical systems. During three disaster recovery exercises we observed, the disaster recovery exercise participants effectively used the exercise plans to monitor the plan execution, held exercise status update meetings twice each day, worked together to resolve issues, and agreed to build lessons learned into future Disaster Recovery Exercise Plans.

In addition, in December 2006, the Chief Information Officer listed the completion of corrective actions to demonstrate progress in resolving the Computer Security Material Weakness as one of the Chief Information Officer Commitments for Calendar Year 2007. The current Disaster Recovery Program Director was appointed in late Calendar Year 2005 and was responsible for both the Disaster Recovery and the Computer Security Incident Response Center Programs until the programs were separated in July 2007. In October 2007, the IRS formed a new Disaster Recovery Program Office within the Modernization and Information Technology Services organization's Cybersecurity organization to provide oversight, accountability, and responsibility for developing and maintaining the IRS Enterprise Disaster Recovery Strategy. Additional staff and funding has been committed for disaster recovery through the new office.

Additional Management Actions Are Needed to Effectively Address Disaster Recovery Program Weaknesses

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003, and the Federal Information Security Management Act (FISMA)[7] require Federal Government agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the disruption or destruction of information. In addition, the FISMA requires management to identify and report significant vulnerabilities and the associated Plans of Action and Milestones to address the vulnerabilities. The vulnerabilities will be included in the Federal Managers' Financial Integrity Act of 1982[8] material weaknesses reported annually to the Secretary of the Treasury, Congress, and the President. The Internal Revenue Manual further emphasizes the importance of identifying and reporting material weakness control deficiencies that significantly impair the fulfillment of the IRS mission or that the Commissioner determines to be of sufficient

[6] See report #8 in Appendix IV.
[7] The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[8] 31 U.S.C. §§ 1105, 1113, 3512 (2000).

importance to be reported outside of the IRS until corrected. The Government Accountability Office *Standards for Internal Control in the Federal Government*[9] provide that documentation should be maintained to provide evidence of actions taken to address risks in a computerized information system environment and the documentation should be readily available for examination.

The FISMA also requires each Federal Government agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. An effective information security program should include, in part, subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate, and periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk but no less than annually. The Internal Revenue Manual states contingency development, testing, and maintenance shall be coordinated with other related plans including the Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan.

National Institute of Standards and Technology *Contingency Planning Guide for Information Technology Systems* (Special Publication 800-34), dated June 2002, states that, to be successful, management must develop or reexamine their information technology contingency planning policies and plans with emphasis on maintenance, training, and exercising the contingency plan. In addition, best practices outline performance indicators as a mechanism for measuring the success of the disaster recovery process and plan. Performance indicators may include periodic tests, periodic reports, and review and analysis of the disaster recovery process.

Corrective actions for prior audit recommendations have not been effectively implemented

Our review of 27 closed corrective actions (i.e., corrective actions reported as completed by the IRS in the Joint Audit Management Enterprise System) determined the IRS did not have documentation to show the actions were taken before closing all corrective actions and to show permanent improvements were made to the disaster recovery process. For example:

1. In an April 2003 audit report,[10] we recommended the Chief Information Officer ensure the ECC-Detroit and the ECC-Memphis store all required documents for all of their consolidated mid-range computer systems at the offsite facility (either in hardcopy or in an easily retrievable electronic copy). The IRS agreed to have the ECC-Detroit identify the documentation available and ensure copies were stored offsite. The IRS also agreed

[9] GAO/AIMD-00-21.3.1, dated November 1999.
[10] See report #3 in Appendix IV.

to conduct audits of mid-range systems for required certification documents as stated in the Internal Revenue Manual and any other appropriate documentation that were to be stored offsite. Finally, the IRS agreed to have its National Office provide complete documentation to the ECC-Detroit. After modifying the original corrective action completion due date from December 15, 2003, to April 15, 2004, to allow more time to develop an electronic system to track the offsite documentation and Disaster Recovery and Business Resumption Plans, the IRS showed the corrective action for this recommendation was closed as completed on April 1, 2004. However, during our observation of two disaster recovery tests, we determined the IRS did not have permanent hardcopies of the Disaster Recovery Plans stored at the recovery sites' offsite storage facilities or centralized in designated electronic file locations.

2. In an August 2004 audit report,[11] we recommended the Chief Information Officer test and evaluate the ECC-Detroit offsite storage vendor's ability to deliver in a timely manner the mainframe computer disaster recovery backup files and documentation to the ECC-Memphis and determine whether the ECC-Detroit backup procedures and Disaster Recovery Plan should be revised to provide for backup files and documentation to be stored at the ECC-Memphis. The IRS agreed to have the Enterprise Operations organization validate that the ECC-Detroit offsite storage vendor can deliver in a timely manner the mainframe computer disaster recovery backup files and documentation to the ECC-Memphis. The IRS also agreed that, in addition to the ECC-Detroit's annual planned disaster recovery exercise, it would annually conduct a random test of the offsite vendor's ability to deliver backup files in a timely manner. This test would be unannounced and, upon completion of the test, a determination would be made as to whether the Plan should be revised to provide for backup files and documentation to be stored at the ECC-Memphis. The IRS closed these corrective actions as completed as of January 6, 2005. However, the IRS was unable to provide evidence supporting announced, unannounced, and annually planned tests of the offsite storage vendor's ability to deliver in a timely manner all backup files and documentation to the disaster recovery site.

The corrective actions taken by the IRS to address prior audit recommendations did not effectively resolve the reported issues.

3. In the April 2003 audit report previously cited,[12] we recommended the Chief Information Officer develop a schedule to periodically train ECC-Detroit, ECC-Martinsburg, and ECC-Memphis employees in their disaster recovery roles and responsibilities. The IRS agreed to develop a disaster recovery training strategy and draft training manuals on roles and responsibilities. The corrective action was closed as completed on November 9, 2004. However, the IRS was

[11] See report #9 in Appendix IV.
[12] See report #3 in Appendix IV.

not able to provide (1) a copy of the disaster recovery training strategy, (2) copies of the training manuals regarding personnel roles and responsibilities, or (3) support for disaster recovery training (e.g., training dates, types, and participants). As a result of ineffective disaster recovery training, the IRS does not have personnel onsite at the recovery location to fully perform disaster recovery duties. During disaster recovery exercises, we observed employees who were responsible for restoring production systems performing the recovery duties rather than the personnel who were assigned to the recovery location.

4. In a March 2004 audit report,[13] we recommended the Chief Information Officer ensure the Master File Disaster Recovery Plan is complete, detailed enough to be used verbatim to react to a worst-case scenario, accurate, reviewed quarterly, and updated as needed. The IRS agreed the Director, ECC-Martinsburg, will ensure, as resources permit, that the Master File Disaster Recovery Plan will be revised to allow recovery by non-ECC-Martinsburg technical personnel and that the Master File Disaster Recovery Plan is complete, detailed enough, accurate, reviewed quarterly, and updated as needed. The IRS closed the corrective action as completed on December 7, 2004. However, our review of the Master File Disaster Recovery Plan determined reviews were not always performed quarterly. In addition, while our observation of the Master File disaster recovery test determined test participants were using the Master File Disaster Recovery Plan, our observation of one other mainframe disaster recovery test determined that recovery site personnel used a combination of the Disaster Recovery Exercise Plan (because a Disaster Recovery Plan was not available) and individual reference materials they had brought to the exercise to recover the system(s) during the disaster recovery exercise.

Material weakness corrective actions have not been effectively implemented

We reviewed the five open corrective action components documented by the IRS in its overall Computer Security Material Weakness Plan for improving the disaster recovery process. The results of our corrective action component review follow.

Information Technology Contingency Plan prioritization – Completion due date: September 30, 2008.

The IRS is in the process of replacing the Technical Contingency Planning Documents with Information Technology Contingency Plans and has scheduled completion of this effort over a 3-year period ending in Fiscal Year 2008. The new Information Technology Contingency Plans will include Appendix H (i.e., Disaster Recovery Plan), which provides specific procedures for recovering key application components.

[13] See report #6 in Appendix IV.

We judgmentally selected 8 of 30 major information technology systems identified as directly supporting the 25 critical processes[14] to determine whether the systems had Information Technology Contingency Plans prepared and tested. We found 1 of 8 systems did not have an Information Technology Contingency Plan prepared and tested, although the system was 1 of the systems supporting 4 or more of the 25 critical processes. The IRS Certification Program Office's schedule showed the system as having an Information Technology Contingency Plan. However, we determined the system still has a Technical Contingency Planning Document dated December 6, 2006.

Establish recovery capability – Completion due date as modified by management during our review: September 30, 2010 (completion was originally due September 30, 2008).

The IRS committed, originally by October 1, 2005, to performing the gap analysis of the current Modernization and Information Technology Services organization business resumption capabilities against business unit requirements and to include both Recovery Point Objectives and Recovery Time Objectives for all major systems in the analysis. In February 2007, the IRS hired a contractor to assist in preparation of a business impact analysis due to be completed in January 2008. The business impact analysis will include a gap analysis and confirm what applications there are and the expected Recovery Time Objectives and Recovery Point Objectives associated with the applications.

Disaster Recovery Plan Test and Exercise Development – Completion due date as modified by management during our review: December 31, 2008 (completion was originally due September 30, 2008).

Material weakness corrective actions have not been completed, and the IRS has extended the completion due dates.

The IRS is responsible for ensuring disaster recovery test and exercise activities include timely and efficient disaster recovery exercise results reporting. However, where lessons learned or action items from prior year tests were included and recommended as critical, the items were not always addressed in subsequent year testing. For example, a Calendar Year 2006 disaster recovery exercise identified the need to include in the Calendar Year 2007 exercise a test to ensure modified computer programming could be implemented while in a disaster recovery mode. The Calendar Year 2007 exercise summary report cites completion of this item as one of the main goals for the Calendar Year 2007 exercise; however, the goal was not accomplished because no one involved in the exercise ensured the prior year item was addressed.

Test and review adequacy of plans – Completion due date as modified by management during our review: December 31, 2010 (completion was originally due September 30, 2008).

Based on our review of offsite storage boxes and designated electronic file locations, the IRS is not properly maintaining contingency planning and Disaster Recovery Plan documentation for

[14] Eighteen critical business processes and seven critical administrative or infrastructure processes.

ready availability in the event of a disaster. For example, we found Disaster Recovery Plan documents are not timely updated, standardized (e.g., there are Disaster Recovery Plans, Information Technology Contingency Plans, and Technical Contingency Planning Documents), located in offsite storage or designated electronic file locations, complete, or accurate. However, management stated a working group has been established to review the various document templates to improve Disaster Recovery Plan standardization.

Material weakness area metrics – Completion due date as modified by management during our review: June 30, 2011 (completion was originally due March 31, 2009).

The IRS is not currently collecting and reporting metrics to assess progress and track improvements within the Disaster Recovery Program.

The deficiencies discussed continue because of (1) several changes in management, (2) management's determination that other issues were more important than disaster recovery issues, and (3) unapproved budget requests for resources and staff years needed to address disaster recovery issues. In addition, the IRS did not fully comply with established disaster recovery guidance in the Internal Revenue Manual incorporated from Office of Management and Budget, National Institute of Standards and Technology, and FISMA guidelines.

By not correcting previously reported deficiencies and having formal guidance in place to govern the disaster recovery process, the IRS may be unable to timely and successfully recover the systems and operations in a disaster. The IRS also may not ensure minimal disruption to tax collection of approximately $2.7 trillion in revenue for the Federal Government and processing of more than 228 million tax returns. Due to the continued program deficiencies, the Disaster Recovery Program material weaknesses should not be downgraded to a significant deficiency.

We are making no recommendations for in-process areas such as the completion of the gap analysis of the current Modernization and Information Technology Services organization business resumption capabilities against business unit requirements and the development of metrics.

Recommendations

The Chief Information Officer should ensure:

Recommendation 1: All Disaster Recovery Plan documentation is standardized, complete, accurate, readily accessible in the event of disaster (e.g., from offsite storage and designated electronic file library locations), detailed enough to be used verbatim to react to a worst-case scenario, and reviewed quarterly.

> ***Management's Response:*** IRS management agreed with this recommendation and plans to evaluate and revise all existing Disaster Recovery Plan documentation and templates used to perform and coordinate disaster recovery-related activities; ensure all

Plan documentation is standardized, accurate, comprehensive, appropriately detailed, up-to-date, and written in a clear, cohesive format; ensure Plan documentation includes all relevant Federal Government guidance and all other critical information needed to perform disaster recovery-related activities; perform a comprehensive inventory analysis audit to ensure the accessibility and availability of all Plan documentation and that the appropriate offsite storage and retrieval procedures are in place; and research a web-based centralized repository tool for maintaining disaster recovery documentation in a secure and readily accessible manner.

Recommendation 2: Effective completion of tasks as required in disaster recovery guidance incorporated in the Internal Revenue Manual from the Office of Management and Budget, National Institute of Standards and Technology, and the FISMA.

Management's Response: IRS management agreed with this recommendation and plans to develop a comprehensive Disaster Recovery Internal Revenue Manual and ensure all program-related documentation adheres to and complies with all relevant Federal Government guidance. In addition, management will ensure effective completion of tasks as required in Internal Revenue Manual disaster recovery guidance through the embedded Compliance function within the Cybersecurity organization's Disaster Recovery organization. Management will also provide status reports on each of the disaster recovery recommendations through bi-monthly meetings with the Deputy Commissioner for Operations Support.

Recommendation 3: Offsite storage vendors can timely deliver all disaster recovery backup files and documentation to the disaster recovery site using announced, unannounced, and annually planned tests.

Management's Response: IRS management agreed with this recommendation and plans to implement a documented repeatable process during the 2007-2008 annual FISMA reporting period that includes an Information Technology Contingency Plan/Disaster Recovery Test Guide and Checklist. Management also plans to direct test participants to provide evidence of the recovery backup files' delivery and actual time frame for delivery. Business/System owners will update the Checklist with the results of the exercises and enter findings into the application/General Support Systems Plans of Action and Milestones. The completed Checklist will validate completion of the Tabletop Exercise and Functional Test and document findings. It will then be loaded into Trusted Agent FISMA as the artifact verifying the results of the exercise/test.

Recommendation 4: Appropriate disaster recovery site personnel are identified and provided with annual training to ensure they have the ability to implement the Disaster Recovery Plan in the event production site personnel are not available during a disaster.

Management's Response: IRS management agreed with this recommendation and plans to develop a comprehensive disaster recovery specific training curriculum; develop

a specialized training course to address specific training requirements in various disaster recovery disciplines such as testing, plan development, business impact assessment, and compliance, and train all individuals who have disaster recovery responsibilities; initiate a site-to-site cross-training skill set evaluation and training program to ensure critical skill sets reside in a specific location, responsible individuals receive training, and skill sets are replicated in other locations; and develop a database as training is completed to provide an assessment report to management for use in evaluating training progress, qualified personnel, and skill set risks.

Recommendation 5: Disaster recovery exercise lessons learned or action items deemed as critical are included in subsequent exercises.

Management's Response: IRS management agreed with this recommendation and plans to develop a repeatable process to ensure subsequent exercises include lessons learned or action items deemed as critical. As all Information Technology Contingency Plans and Disaster Recovery Plans are exercised and tested, test participants will follow a formal Checklist to ensure documentation of system/organizational changes or problems encountered during plan implementation, execution, or testing. If more critical problems are found, Summary Findings will note where corrective actions and findings are documented for viewing and analysis by the Designated Approving Authority. Management also plans to develop a process for entering these findings in the application/General Support Systems Plans of Action and Milestones for monitoring and tracking, and require the Designated Approving Authority to sign the Checklist validating that the Tabletop Exercise and Functional Test have been completed and findings documented.

Recommendation 6: A permanent file is established for keeping documentation supporting closure of prior recommended corrective actions and completion of material weakness corrective action plan components related to the Information Technology Contingency Planning material weakness.

Management's Response: IRS management agreed with this recommendation and established the Modernization and Information Technology Services organization's Information Technology Disaster Recovery organization. The responsibilities of this program office include validating all closure activities for corrective actions and collecting and maintaining all documentation that supports closure and/or mitigation of all corrective actions, material weaknesses, and any outstanding year-to-year weaknesses remediation recommendations. Management also established a process using project management schedules, work breakdown structures, and cross-organizational correspondence that enables this office to provide management with a more effective assessment of material weakness remediation progress for disaster recovery.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of the corrective actions taken to resolve the previously reported disaster recovery material weaknesses.[1] To accomplish our objective, we:

I. Determined whether the disaster recovery issues in the Computer Security Material Weakness Plan, IRS-2A-01-01, Material Weakness Area 1-6, Information Technology Contingency Planning Section have been effectively resolved.

A. Reviewed Treasury Directives, Office of Management and Budget Circulars, the Internal Revenue Manual, industry best practices, and other guidelines governing disaster recovery.

B. Reviewed the Computer Security Material Weakness Plan, IRS-2A-01-01, Material Weakness Area 1-6, Information Technology Contingency Planning Section and evaluated the effectiveness of corrective actions for the five corrective action components. We interviewed IRS personnel and obtained a list of 30 critical information technology systems that support 25 critical processes.[2] We selected a judgmental sample of 8 of the 30 systems and obtained contingency plan documentation to determine whether each of the 8 major systems had an Information Technology Contingency Plan. The eight systems were selected for review based on being identified as supporting four or more of the critical processes and not being identified as tested during the disaster recovery exercise conducted in July 2007. We also reviewed management's efforts to establish the IRS' recovery capability in part via completion of a gap analysis that encompassed defining Recovery Time Objectives. We also determined the effectiveness of the disaster recovery planning test and exercise development activities by interviewing IRS personnel, reviewing applicable requirements, and identifying the degree of testing and participant involvement. We reviewed contingency plan documents in offsite storage boxes and/or at the disaster recovery test locations. Finally, we interviewed IRS personnel to determine whether any material weakness area metrics had been established and/or were being used.

C. Obtained a walkthrough of the ECCs to verify the disaster recovery process.

[1] See Appendix V for a Glossary of Terms.
[2] Eighteen critical business processes and seven critical administrative or infrastructure processes.

D. Determined whether Disaster Recovery Plans for the ECCs have been adequately tested and deficiencies identified from the disaster recovery tests have been adequately addressed. We reviewed the policies and procedures for conducting and evaluating tests, reviewed the Calendar Years 2006 and 2007 test plans, and requested documentation supporting disaster recovery-related training conducted prior to tests. We also observed the three ECC tests and reviewed the test results at the conclusion of the tests to determine the extent identified deficiencies (e.g., from the prior year) were addressed.

II. Determined whether the corrective actions identified by management to address prior audit recommendations in the Disaster Recovery Program[3] have been effectively implemented.

A. Reviewed the Joint Audit Management Enterprise System reports for the 35 open corrective actions (as of March 16, 2005) from prior Treasury Inspector General for Tax Administration audit reports to determine actions completed and the current due date for open corrective actions.

B. Determined whether the corrective actions implemented were the agreed-upon corrective actions (e.g., regarding personnel, training, and testing) and effectively resolved the disaster recovery vulnerabilities. We interviewed IRS personnel and requested documentation supporting the corrective actions the IRS reported as closed in the Joint Audit Management Enterprise System reports. We also assessed whether the corrective actions reported as completed established a repeatable process and considered the effectiveness of any alternative corrective actions taken in lieu of the agreed-upon corrective actions and/or the need for additional corrective actions. Finally, we discussed with management the justification for extending the completion date for the open corrective actions.

III. Used computer-based data for background information related to 30 applications the IRS identified as supporting its 25 critical processes. We did not determine the validity and reliability of the data based on the scope of audit work performed. However, we did verify that these 30 major applications were included as a part of the IRS' As-Built Architecture.

[3] The Disaster Recovery Program serves to facilitate cross-organizational buy-in, participation, concurrence, and communication of all IRS disaster recovery activities.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Scott Macfarlane, Director
Danny Verneuille, Audit Manager
Mark Carder, Senior Auditor
Olivia DeBerry, Auditor
Charlene Elliston, Auditor
Linda Screws, Auditor

Appendix III

Report Distribution List

Acting Commissioner C
Office of the Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Operations Support OS
Associate Chief Information Officer, Cybersecurity OS:CIO:C
Associate Chief Information Officer, Enterprise Operations OS:CIO:EO
Director, Disaster Recovery Operations OS:CIO:C
Director, Stakeholder Management OS:CIO:SM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
Associate Chief Information Officer, Cybersecurity OS:CIO:C
Director, Program Oversight Office OS:CIO:SM:PO

Appendix IV

Prior Audit Reports Addressing Disaster Recovery

1. *The Internal Revenue Service Has Made Substantial Progress in Its Business Continuity Program, but Continued Efforts Are Needed* (Reference Number 2003-20-026, dated December 2002).
2. *Progress Has Been Made in Protecting Critical Assets* (Reference Number 2003-20-047, dated February 2003).
3. *Improvements Are Needed to Effectively Implement the Disaster Recovery Strategy for Consolidated Mid-Range Computer Systems* (Reference Number 2003-20-084, dated April 2003).
4. *The Implementation of Software Products to Manage and Control Computer Resources Needs Improvement* (Reference Number 2003-20-151, dated July 2003).
5. *Risks Are Mounting as the Integrated Financial System Project Team Strives to Meet an Aggressive Implementation Date* (Reference Number 2004-20-001, dated October 2003).
6. *The Master File Disaster Recovery Exercise Was Completed, but Significant Vulnerabilities Should Be Addressed* (Reference Number 2004-20-053, dated March 2004).
7. *The Custodial Accounting Project Team Is Making Progress; However, Further Actions Should Be Taken to Increase the Likelihood of a Successful Implementation* (Reference Number 2004-20-061, dated March 2004).
8. *Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications* (Reference Number 2004-20-079, dated April 2004).
9. *Mainframe Computer Disaster Recovery Risks Are Increased Due to Insufficient Computer Capacity and Testing* (Reference Number 2004-20-142, dated August 2004).
10. *The Integrated Financial System Project Team Needs to Resolve Transition Planning and Testing Issues to Increase the Chances of a Successful Deployment* (Reference Number 2004-20-147, dated August 2004).
11. *To Ensure the Customer Account Data Engine's Success, Prescribed Management Practices Need to Be Followed* (Reference Number 2005-20-005, dated November 2004).
12. *The Disaster Recovery Program Has Improved, but It Should Be Reported As a Material Weakness Due to Limited Resources and Control Weaknesses* (Reference Number 2005-20-024, dated March 2005).

Appendix V

Glossary of Terms

Term	Definition
As-Built Architecture	Presents an enterprise view of the IRS Information Technology and Business environments and documents the Current Production Environment (applications, data stores, infrastructure, data interfaces) and related organizations, locations, technology platforms, etc.
Business Continuity Plan	Defines recovery responsibilities and resources necessary to respond to a disruption to business operations.
Business Recovery Plan	Outlines procedures to be used for the resumption of business after a disaster, specifically telling personnel, in detail, what has to be done to resume business in the event of a disaster or unplanned work stoppage (e.g., shipping work to a backup center if necessary).
Business Resumption Strategy	A strategy to resume normal business activities in the event of an emergency or interruption of daily business.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
Computing Centers	Sites that support tax processing and information management through a data processing and telecommunications infrastructure.
Continuity of Operations Plan	A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Term	Definition
Critical Processes	The most important IRS processes from which agencywide resource decisions will be made. There are 25 critical processes made up of 18 critical business processes (e.g., remittance processing, tax return processing, refund processing) and 7 administrative or infrastructure critical processes (e.g., provide a safe and equipped working environment, provide payroll).
Desktop Disaster Recovery Test	A desktop simulation exercise conducted for major systems that cannot conduct a live test annually but that still involve necessary participants and for which results are captured in a memorandum for the record.
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Disaster Recovery Strategy	A strategy to ensure the IRS' ability to recover operations within stated business recovery time and point objectives.
End-to-End Disaster Recovery Test	A full-scale live test of the disaster recovery capability with the actual systems, network, personnel, and procedures under actual operational conditions.
General Support Systems	Sets of resources that provide necessary information technology infrastructure support to applications and business functionality such that compromise would have a severe adverse effect on the IRS mission, tax administration functions, and/or employee welfare.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber attacks against an organization's information technology system(s).
Information Technology Contingency Plan	A plan developed to document procedures established to recover information technology systems (general support systems or applications), operations, and data after a disruption.

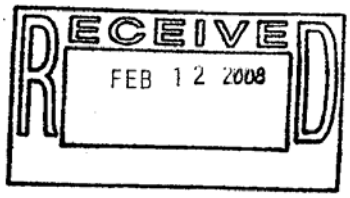
Term	Definition
Joint Audit Management Enterprise System	The Department of the Treasury's audit tracking and management control system that went live in January 2003 and replaced the IRS' Inventory Tracking Closure System as the system of record.
Master File	The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
Material Weaknesses	Internal accounting and administrative control deficiencies in operations or systems that, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports.
Operating System	Software that directs a computer's operations, controlling and scheduling the execution of other programs, and managing storage, input/output, and communication resources.
Plans of Action and Milestones	A management process that outlines security weaknesses pertaining to a specific system and the steps that need to be taken to remediate them. It details resources required to accomplish the milestones in meeting the task, and scheduled completion dates for the mitigation.
Recovery Point Objective	The point in time to which systems and data must be restored after an outage (e.g., end of previous day's processing) to resume processing transactions.
Recovery Time Objective	The period of time within which data and system and application functionality must be restored after an outage (e.g., 1 business day) to resume processing transactions.
Technical Contingency Planning Document	Document developed to contain the recovery strategies, essential resources, plans, and procedures necessary to allow someone at a disaster site to implement the recovery of the system in the event there is not a site disaster recovery analyst or Disaster Recovery Plan available.
Territory	An office that serves taxpayers within a specified geographical area.

Appendix VI

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



February 11, 2008

MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez
Chief Information Officer

SUBJECT: Draft Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit #200720005) (i-trak #2008-32294)

Thank you for the opportunity to review and respond to the subject draft audit report. We take our security posture very seriously, and as such, we are aggressively addressing issues to enhance the effectiveness of our Disaster Recovery Program.

In March 2005, your office recommended that we report the Disaster Recovery Program as a material weakness, and we agreed. We appreciate that your report acknowledges that we have effectively implemented some corrective actions to address prior audit recommendations and have taken other constructive measures to help ensure future progress toward resolving the material weakness. We have continued to address the challenges and risks associated with Disaster Recovery, and in October 2007, formed a new Disaster Recovery Program Office under the Office of Cybersecurity within the Modernization and Information Technology Services organization. This office provides oversight, accountability, and responsibility for developing and maintaining the IRS Enterprise Disaster Recovery Strategy.

We agree with, and will implement, all six of your report recommendations. The attachment to this memo provides our detailed corrective action plans to address the recommendations.

Thank you for your continued support and guidance. We look forward to working with TIGTA in the future on this important issue. If you have any questions, please contact me at (202) 622-6800. Members of your staff may also contact Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment

Management Response to Draft Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit #200720005) (i-trak #2008-32294)

RECOMMENDATION #1: The Chief Information Officer (CIO) should ensure all Disaster Recovery Plan documentation is standardized, complete, accurate, readily accessible in the event of disaster (e.g., from offsite storage and designated electronic file library locations), detailed enough to be used verbatim to react to a worst-case scenario, and reviewed quarterly.

CORRECTIVE ACTION TO RECOMMENDATION #1: We agree with this recommendation. Modernization and Information Technology Services' (MITS) Cybersecurity organization is:

- Evaluating and revising all existing plan documentation and templates used to perform and coordinate Disaster Recovery related activities;
- Ensuring all plan documentation is standardized, accurate, comprehensive, appropriately detailed, up-to-date, and written in a clear, cohesive format;
- Ensuring all plan documentation includes requirements stated in the Federal Information Security Management Act (FISMA), all relevant federal guidance from the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), Department of the Treasury, Treasury Inspector General for Tax Administration (TIGTA), Department of Homeland Security, etc., and all other critical information needed to perform Disaster Recovery-related activities;
- Performing a comprehensive inventory analysis audit to ensure the accessibility and availability of all plan documentation and that the appropriate off-site storage and retrieval procedures are in place; and
- Researching a web-based centralized repository tool for maintaining Disaster Recovery documentation in a secure and readily accessible manner.

IMPLEMENTATION DATE: January 1, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

RECOMMENDATION # 2: The CIO should ensure effective completion of tasks as required in disaster recovery guidance incorporated in the Internal Revenue Manual (IRM) from OMB, NIST, and FISMA.

CORRECTIVE ACTION TO RECOMMENDATION #2: We agree with this recommendation. MITS' Cybersecurity organization is:

- Developing a comprehensive Disaster Recovery Internal Revenue Manual (IRM), and ensuring that this and all program related documentation adhere to and comply with specific requirements stated in FISMA and all relevant federal guidance from OMB, NIST, TIGTA, Department of the Treasury, Department of Homeland Security, etc.;

Management Response to Draft Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit #200720005) (i-trak #2008-32294)

- Addressing and referencing the following publications and laws in the Disaster Recovery IRM being developed: NIST Special Publication 800-34; Treasury Directive Publication 85-01; FISMA requirements of the 2002 Act; and Public Law 107-347, E-Government Act of 2002; and
- Ensuring effective completion of tasks as required in IRM disaster recovery guidance through the embedded Compliance function within Cybersecurity's Disaster Recovery organization. To encompass the effectiveness and compliance of the IRM, we will monitor policy, develop plans, conduct tests, etc. to mitigate and correct weaknesses resulting from a breakdown in processes. Additionally, we are creating a database to capture and monitor all corrective actions. Work breakdown structures and enterprise life cycles will be monitored as well. Finally, we will provide status reports on each of the Disaster Recovery recommendations through bi-monthly meetings with the Deputy Commissioner.

IMPLEMENTATION DATE: October 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Offer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the JAMES and monitored monthly until completion.

RECOMMENDATION #3: The CIO should ensure offsite storage vendors can timely deliver all disaster recovery backup files and documentation to the disaster recovery site using announced, unannounced, and annually planned tests.

CORRECTIVE ACTION TO RECOMMENDATION #3: We agree with this recommendation. MITS' Cybersecurity organization is:

- Implementing a documented repeatable process during the 2007-2008 annual FISMA reporting period that includes an Information Technology Contingency Plan (ITCP)/Disaster Recovery Test Guide and Checklist. The Checklist guides test participants to the appropriate appendices in the ITCP that document the explicit step-by-step procedures necessary to recover a system. Two of the specific directives for functional exercises documented in the Checklist are: 1) verifying that backup media are stored at designated off-site locations and retrievable within timeliness criteria; and 2) checking the backup/off-site storage organization or vendor's delivery timeliness when request is made during other than normal working hours.
- Directing test participants to provide evidence of the recovery backup files' delivery and actual timeframe for delivery. Delivery and Check-In Logs and routing cover sheets are examples of the evidence that can be included to verify the delivery. Business/System owners will update the Checklist with the results of the exercises and enter findings into the application/General Support Systems (GSS) Plans of Action & Milestones (POA&M). The completed Checklist will validate completion of the Tabletop Exercise and Functional Test and document findings. It will then be loaded into Trusted Agent FISMA (TAF) as the artifact verifying the results of the exercise/test. This is a repeatable

Management Response to Draft Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit #200720005) (i-trak #2008-32294)

process to be performed annually based on annual FISMA reporting. The ACIO, Cybersecurity, obtained approval from both TIGTA and the Department of the Treasury for this process.

IMPLEMENTATION DATE: October 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the JAMES and monitored monthly until completion.

RECOMMENDATION #4: The CIO should ensure appropriate disaster recovery site personnel are identified and provided with annual training to ensure they have the ability to implement the Disaster Recovery Plan in the event production site personnel are not available during a disaster.

CORRECTIVE ACTION TO RECOMMENDATION #4: We agree with this recommendation. MITS' Cybersecurity organization is:

- Developing a comprehensive Disaster Recovery specific training curriculum;
- Developing a specialized Disaster Recovery training course, as part of the curriculum, to address specific IRS training requirements in various Disaster Recovery disciplines such as testing, plan development, business impact assessment, and compliance, and training all individuals who have Disaster Recovery responsibilities and for those who serve in a backup support role;
- Initiating a site-to-site cross-training skill set evaluation and training program to ensure critical skill sets reside in a specific location, responsible individuals receive training, and skill sets are replicated in other locations; and
- Developing a database as training is completed to provide an assessment report to management for use in evaluating training progress, qualified personnel, and skill set risks.

IMPLEMENTATION DATE: October 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the JAMES and monitored monthly until completion.

RECOMMENDATION #5: The CIO should ensure disaster recovery exercise lessons learned or action items deemed as critical are included in subsequent exercises.

CORRECTIVE ACTION TO RECOMMENDATION #5: We agree with this recommendation. MITS' Cybersecurity organization is:

Management Response to Draft Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit #200720005) (i-trak #2008-32294)

- Developing a repeatable process to ensure subsequent exercises include Disaster Recovery exercise lessons learned or action items deemed as critical. As all ITCPs and Disaster Recovery plans are exercised and tested, test participants will follow a formal Checklist to ensure documentation of system/organizational changes or problems encountered during plan implementation, execution, or testing within the Lessons Learned and Observations blocks on the Checklist. If more critical problems are found, Summary Findings will note where corrective actions and findings are documented for viewing and analysis by the Designated Approving Authority (DAA) prior to validation by signing the Checklist;
- Developing a process for entering these findings in the application/GSS POA&M for monitoring and tracking to ensure that future documentation and tests are updated to include any findings from the annual tests; and
- Requiring the DAA to sign the Checklist validating that the Tabletop Exercise and Functional Test have been completed and findings documented. The Checklist will then be loaded into TAF as the artifact verifying the results of the exercise/test. This repeatable process ensures critical findings will be included in subsequent exercises, as the Business Owner is prompted to review the POA&M prior annual testing.

IMPLEMENTATION DATE: October 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the JAMES and monitored monthly until completion.

RECOMMENDATION #6: The CIO should ensure a permanent file is established for keeping documentation supporting closure of prior recommended corrective actions and completion of material weakness corrective action plan components related to the ITCP material weakness.

CORRECTIVE ACTION TO RECOMMENDATION #6: We agree with this recommendation. To address this recommendation, MITS' Cybersecurity organization has:

- Formally established the MITS Information Technology Disaster Recovery Organization. The responsibilities of this program office include validating all closure activities for corrective actions and collecting and maintaining all documentation that supports closure and/or mitigation of all corrective actions, material weaknesses, and any outstanding year-to-year weaknesses remediation recommendations;
- Established a process using project management schedules, work breakdown structures, and cross-organizational correspondence that enables this office to provide management with a more effective assessment of material weakness remediation progress for Disaster Recovery; and
- Established a process to monitor the effectiveness of this action through compliance auditing.

Management Response to Draft Audit Report – Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made (Audit #200720005) (i-trak #2008-32294)

IMPLEMENTATION DATE: April 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the JAMES and monitored monthly until completion.

Page 5