



*Corrective Actions to Address the  
Disaster Recovery Material Weakness  
Are Being Completed*

**June 27, 2011**

**Report Number: 2011-20-060**

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* | [TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)

*Web Site* | <http://www.tigta.gov>



## HIGHLIGHTS

### **CORRECTIVE ACTIONS TO ADDRESS THE DISASTER RECOVERY MATERIAL WEAKNESS ARE BEING COMPLETED**

## Highlights

**Final Report issued on June 27, 2011**

Highlights of Reference Number: 2011-20-060 to the Internal Revenue Service Chief Technology Officer.

### **IMPACT ON TAXPAYERS**

Disaster recovery planning is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, computer operations, and data after a disruption. The Internal Revenue Service (IRS) is completing corrective actions to address a material weakness in its disaster recovery capabilities. Effective disaster recovery capabilities are critical to ensuring that the IRS's key information systems can be recovered with minimal disruption to service. In addition to the IRS needing these systems to administer the Nation's tax system, data and services provided by these systems are needed by Congress, the Department of the Treasury, tax professionals, taxpayers, and other Government agencies.

### **WHY TIGTA DID THE AUDIT**

The IRS requested that TIGTA evaluate the corrective actions for addressing its disaster recovery material weakness. In March 2005, the IRS declared its disaster recovery program a material weakness in accordance with the Federal Managers' Financial Integrity Act of 1982. The IRS prepared a corrective action plan that divided the material weakness into seven components and contained corrective actions for each of these components. The last of the corrective actions is scheduled to be completed in December 2011. The objective of the audit was to evaluate the IRS's progress in completing its corrective actions for addressing the disaster recovery material weakness.

### **WHAT TIGTA FOUND**

Corrective actions for addressing the disaster recovery material weakness are being adequately completed for six of the seven components. The IRS 1) created two disaster recovery Internal Revenue Manuals, 2) developed a disaster recovery training curriculum, 3) prioritized the recovery order of its systems based on the criticality of the business processes the systems supported, 4) is creating a program for performing reviews of its disaster recovery efforts and activities, 5) prepared, exercised, and tested disaster recovery plans for all of its systems, and 6) performs ongoing analyses of its recovery capabilities to identify gaps in its ability to meet business recovery requirements and to prioritize corrective actions.

During the course of the audit, TIGTA auditors recommended several changes to the corrective actions that the IRS completed, or was in the process of completing, prior to issuance of this report. Two items remain outstanding. The IRS does not have 1) a system for tracking whether employees with disaster recovery roles attend required annual training and 2) adequate metrics to assess progress and track improvements in completing the corrective actions.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the Chief Technology Officer ensure that the IRS develops 1) the capability to track the disaster recovery training of employees with disaster recovery roles and responsibilities and 2) metrics specifically designed to assess progress and track improvements in completing the disaster recovery corrective actions.

In its response to the report, the IRS agreed with TIGTA's recommendations. The IRS plans to 1) develop a formal process and monitoring system to track the completion of disaster recovery training by employees who have disaster recovery roles and responsibilities and 2) design metrics to assess the progress of the disaster recovery program.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

June 27, 2011

**MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER**

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

**SUBJECT:** Final Audit Report – Corrective Actions to Address the Disaster  
Recovery Material Weakness Are Being Completed  
(Audit # 201020024)

This report presents the results of our review of the Cybersecurity organization's<sup>1</sup> disaster recovery activities. The overall objective was to evaluate the Internal Revenue Service's (IRS) corrective actions for addressing its disaster recovery material weakness.<sup>2</sup> This review was requested by the Cybersecurity organization. This review also addresses the major management challenge of Security of the IRS and is part of our statutory requirements to annually review the adequacy and security of IRS technology. 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 Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

---

<sup>1</sup> See Appendix V for a glossary of terms.

<sup>2</sup> In March 2005, the IRS declared its disaster recovery program a material weakness in accordance with the Federal Managers' Financial Integrity Act of 1982.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

*Table of Contents*

**Background** .....Page 1

**Results of Review** .....Page 3

    Corrective Actions Are Being Adequately Completed for Six of the  
    Seven Components of the Disaster Recovery Material Weakness .....Page 5

Recommendation 1:.....Page 13

    Improvements Are Needed in the Corrective Actions for the Metrics  
    Component of the Disaster Recovery Material Weakness .....Page 14

Recommendation 2:.....Page 16

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology .....Page 17

    Appendix II – Major Contributors to This Report .....Page 20

    Appendix III – Report Distribution List .....Page 21

    Appendix IV – National Institute of Standards and Technology  
    Publications.....Page 22

    Appendix V – Glossary of Terms .....Page 23

    Appendix VI – Management’s Response to the Draft Report .....Page 26



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

*Abbreviations*

ECC	Enterprise Computing Center
IRS	Internal Revenue Service
IT	Information Technology
ITDRO	Information Technology Disaster Recovery Organization
MITS	Modernization and Information Technology Services
NIST	National Institute of Standards and Technology
SP	Special Publication
TSCC	Toolkit Suite With Command Centre



## *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed*

---

### *Background*

To carry out its mission, the Internal Revenue Service (IRS) is heavily dependent on an extensive network of computer systems spread across the country. During Fiscal Year 2009, the IRS reported that its computer systems processed more than 236 million returns, provided nearly 127 million refunds, collected more than \$2.3 trillion, received more than 296 million visits to its web sites, and received about 95 million electronically filed individual income tax returns. In addition to the IRS needing these systems, data and services provided by the systems are also needed by Congress, the Department of the Treasury, tax professionals, taxpayers, and other Government agencies. During Fiscal Year 2010, the IRS reported that its computer network contains about 131,000 workstations, 4,500 infrastructure and application servers, 310 midrange servers, and 18 mainframe computers.

Significant events such as the terrorist attacks on September 11, 2001, and Hurricane Katrina in August 2005 emphasize the need for organizations to have plans in place that will ensure essential operations can continue during a wide range of emergencies. Attacks and threats against IRS employees and facilities have risen steadily in recent years, highlighted by the February 2010 attack on an IRS facility in Austin, Texas. Disaster recovery is an organization's ability to respond to a disruption in services by implementing a plan to restore critical business functions within the stated disaster recovery goals. It is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, computer operations, and data. Disaster recovery plans<sup>1</sup> define the resources, actions, tasks, and data required to recover information systems. Effective disaster recovery capabilities are critical to ensuring that the IRS's key information systems needed to ensure the continuation of the Nation's tax system can be recovered with minimal disruption to service.

Federal disaster recovery requirements exist on several levels. The Federal Information Security Management Act of 2002<sup>2</sup> requires that Federal agencies develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. The Office of Management and Budget requires agencies to ensure that disaster recovery planning capabilities are in place and to provide for continuity of support and disaster recovery planning for their computer systems. Pursuant to its responsibilities under the Federal Information Security Management Act, the National Institute of Standards and Technology (NIST) issues guidance that requires agencies to develop and maintain a disaster recovery

---

<sup>1</sup> Information technology disaster recovery planning is also referred to as contingency planning. Because universally accepted definitions are not available, throughout this report we used the term disaster recovery.

<sup>2</sup> 44 U.S.C. §§ 3541 – 3549.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

program for their information systems to ensure that measures are in place to recover systems after a disruption. NIST guidance outlines the process for developing and maintaining effective disaster recovery plans. The Department of the Treasury requires bureaus to develop and implement a robust, cost-effective Information Technology (IT) security program that includes disaster recovery planning.

Examples of the key components that make up disaster recovery programs include 1) assessing the criticality and sensitivity of computerized operations and identification of supporting resources, such as developing a business impact analysis; 2) taking steps to prevent and minimize potential damage and interruption, such as establishing data backup processes; 3) developing comprehensive disaster recovery plans; 4) conducting periodic testing of disaster recovery plans; and 5) maintaining disaster recovery plans to keep them up to date.

In response to an audit recommendation made by the Treasury Inspector General for Tax Administration, the IRS, in March 2005, declared its disaster recovery program a material weakness in accordance with the Federal Managers' Financial Integrity Act of 1982.<sup>3</sup> To remediate this weakness, a Disaster Recovery Program Director was appointed in late Calendar Year 2005, and in October 2006 the IRS added disaster recovery into its overall Computer Security Material Weakness Plan. In October 2007, the IRS formed the Information Technology Disaster Recovery Organization (ITDRO) within the Modernization and Information Technology Services (MITS) organization's Cybersecurity office. The new office was formed to serve as a single focal point to provide oversight, accountability, and responsibility for developing and maintaining the IRS's enterprise disaster recovery strategy and for bridging the gap between business owners and IT operational staff. The office has a staff of about 50 employees. In Fiscal Year 2010, the MITS organization initiated a reorganization that will reassign the responsibilities of the ITDRO to two divisions within the Cybersecurity organization.

This review was performed at the ITDRO offices in Chamblee, Georgia, during the period June 2010 through March 2011. 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

<sup>3</sup> 31 U.S.C. §§ 1105, 1113, 3512 (2000).



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

## *Results of Review*

As part of its disaster recovery remediation efforts, the ITDRO reported the following major program enhancements from Fiscal Year 2008 through Fiscal Year 2010:

- Created two disaster recovery Internal Revenue Manuals.
- Developed a disaster recovery training curriculum, conducted outreach and awareness sessions, and published disaster recovery articles.
- Completed an enterprise business impact analysis that evaluated more than 600 business processes.
- Established application recovery priorities based on critical business processes<sup>4</sup> and operational impacts.
- Performed indepth assessments and gap analyses of business processes and enterprise disaster recovery capabilities.
- Developed disaster recovery plans for 161 applications and 23 general support systems.
- Updated all disaster recovery plans.
- Performed more than 400 disaster recovery tests and exercises.
- Established a documented and repeatable disaster recovery testing process including expectations, requirements, and templates.
- Tested disaster recovery plans for critical applications based on Department of the Treasury and NIST requirements.
- Was provided funding specifically for improving the IRS's disaster recovery capabilities in Fiscal Years 2010 and 2011.

Figure 1 describes the corrective actions for the seven components that comprise the disaster recovery material weakness. The ITDRO is responsible for managing the completion of these corrective actions.

---

<sup>4</sup> The IRS identified 18 critical business processes, such as processing remittances and processing tax returns, and determined the critical business processes that each of its systems support.



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

**Figure 1: Disaster Recovery Material Weakness  
Components and Corrective Actions**

<b>Components</b>	<b>Corrective Actions</b>	<b>Status</b>
Policy	<ol style="list-style-type: none"> <li>1. Develop and maintain an enterprise-wide Disaster Recovery Internal Revenue Manual specifically addressing business impact analysis, testing, exercise, and plan development guidance and templates.</li> <li>2. Conduct outreach and awareness sessions to ensure the Internal Revenue Manual is incorporated into day-to-day operations.</li> <li>3. Develop an enterprise-wide disaster recovery course curriculum.</li> </ol>	Completed 10/1/08
Business Impact Analysis	<ol style="list-style-type: none"> <li>1. Develop and maintain a prioritized list of critical IT systems that support critical business processes and establish site-based restoration priority documents.</li> <li>2. Conduct gap analyses surrounding the ability to restore via the critical business process.</li> <li>3. Develop an analysis comparing the recovery time objective and recovery point objective of both the MITS organization and Business Operating Divisions.</li> <li>4. Develop an infrastructure spend plan based on the analyses mentioned above.</li> </ol>	Completed 10/1/08
Disaster Recovery Compliance	<ol style="list-style-type: none"> <li>1. Complete internal auditing of the disaster recovery efforts to ensure accuracy and completeness as it relates to day-to-day operations and efforts to mitigate the material weaknesses and audits.</li> </ol>	Due Date 7/1/11
Disaster Recovery Plans	<ol style="list-style-type: none"> <li>1. Develop and maintain disaster recovery plans associated with general support systems, to include all components that support critical applications.</li> <li>2. Establish and maintain data and processing backup-recovery capabilities and ensure maximum allowable outage times meet the recovery time objectives of the applications being supported.</li> </ol>	Completed 12/28/10
Disaster Recovery Plan Test and Exercise	<ol style="list-style-type: none"> <li>1. Develop baseline expectations, requirements, and templates for disaster recovery plans and for disaster recovery plan tests and exercises.</li> <li>2. Identify roles and responsibilities of the MITS organization and Business Operating Divisions involved in the testing.</li> <li>3. Identify the frequency and type of testing required and reporting requirements.</li> <li>4. Conduct tabletop, functional, and end-to-end disaster recovery testing for critical applications based upon direction from the Department of the Treasury and the Federal Information Security Management Act.</li> </ol>	Completed 10/1/08



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

Components	Corrective Actions	Status
Technical Assessment	<ol style="list-style-type: none"> <li>1. Perform annual system risk assessments.</li> <li>2. Develop a true redundancy and resiliency analysis. Based on the critical business processes, develop a site-based restoration vulnerabilities analysis.</li> <li>3. Create a recovery point objective and recovery time objective analysis and gain concurrence from both the Business Operating Divisions and the MITS organization.</li> <li>4. Incorporate a technical assessment tool that will provide an infrastructure impact analysis in the event of a disaster.</li> </ol>	Due Date 7/31/11
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.	Due Date 12/31/11

Source: *The IRS Computer Security Material Weakness Plan for Fiscal Year 2010.*

***Corrective Actions Are Being Adequately Completed for Six of the Seven Components of the Disaster Recovery Material Weakness***

The IRS is adequately completing corrective actions for the 1) Policy, 2) Business Impact Analysis, 3) Disaster Recovery Compliance, 4) Disaster Recovery Plans, 5) Disaster Recovery Plan Test and Exercise, and 6) Technical Assessment components of the disaster recovery material weakness.

***Corrective actions for the Policy component are being adequately completed***

The Policy component contained three corrective actions that the IRS closed in October 2008. The three corrective actions are being adequately completed except for one remaining item in the third corrective action below.

Corrective Action 1 – Develop and maintain an enterprise-wide Disaster Recovery Internal Revenue Manual specifically addressing business impact analysis, testing, exercise, and plan development guidance and templates.

Disaster Recovery Internal Revenue Manual 10.8.60, *Information Technology Disaster Recovery Policy and Guidance*; Interim Disaster Recovery Internal Revenue Manual 10.8.62, *Information Technology Contingency Plan and Disaster Recovery Testing, Training and Exercise Program*; and IRS application and general support system disaster recovery plan templates were complete



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

and consistent with NIST Special Publication (SP) 800-34,<sup>5</sup> NIST SP 800-84, and Treasury Directive Publication 85-01, *Treasury Information Technology Security Program*.

Corrective Action 2 – Conduct outreach and awareness sessions to ensure the Internal Revenue Manual is incorporated into day-to-day operations.

The ITDRO used several methods to conduct disaster recovery outreach and awareness. They made presentations at each of the campuses and computing centers, distributed brochures and posters during these visits, and published articles in several different IRS electronic newsletters.

The outreach and awareness methods used by the IRS and the disaster recovery topics presented were complete and consistent with outreach and awareness methods and disaster recovery processes recommended by guidance in NIST SP 800-34 and NIST SP 800-50.

Corrective Action 3 – Develop an enterprise-wide disaster recovery course curriculum.

The IRS has a curriculum consisting of about 30 disaster recovery training courses that cover the various aspects of disaster recovery. These courses adequately covered disaster recovery topics appearing in NIST SP 800-34 and in the IRS disaster recovery material weakness plan. Course reviews prepared by attendees did not indicate any concerns with the content of the courses. The IRS training delivery methods were consistent with methods suggested in NIST SP 800-50.

However, the ITDRO is not able to track whether employees with disaster recovery roles attend required annual disaster recovery training. NIST SP 800-34 requires that employees with disaster recovery roles be trained annually. The IRS disaster recovery manual requires employees with disaster recovery responsibilities to attend annual disaster recovery training. The IRS's electronic training system tracks each employee's training, but it does not track whether employees have disaster recovery roles and attended disaster recovery training. The ITDRO told us that they were aware of the need to track the training of employees with disaster recovery roles and that the development of a tracking capability is included in their recently funded training plan. Until this capability is implemented, the IRS will not be able to ensure that employees are attending required annual disaster recovery training.

**Management Action:** During the course of the audit, we recommended to the ITDRO several changes to the first and third corrective actions, which it completed or was in the process of completing prior to us issuing this report.

**Corrective actions for the Business Impact Analysis component were adequately completed**

The Business Impact Analysis component contained four corrective actions that the IRS closed in October 2008. All four corrective actions were adequately completed. A business impact assessment is an ongoing activity within a disaster recovery organization, and business impact

---

<sup>5</sup> The titles of NIST publications are shown in Appendix IV.



---

## *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed*

---

analysis results are continuously updated and refined. The IRS has developed a repeatable business impact analysis process that provides updated and current information on the impacts of a disaster or disruption. In October 2008, the ITDRO reported the results of its initial business impact analysis efforts. The ITDRO expects to complete an updated business impact analysis report in June 2011.

### Corrective Action 1 – Develop and maintain a prioritized list of critical IT systems that support critical business processes and establish site-based restoration priority documents.

The ITDRO established and maintained a prioritized list of systems that support critical business processes and established site-based restoration priority documents in accordance with business impact analysis guidance recommended by NIST SP 800-34. To begin the process of creating a prioritized list of applications, the ITDRO identified 18 critical business processes and determined the critical business processes each application supported. The ITDRO then developed a methodology for scoring each application. The scoring system assigned points to each critical business process and to each application's recovery time objective. The more important critical business processes and the more time-critical recovery time objectives were assigned more points than those deemed less critical. The result ranked applications in order, starting with those with the most significant impact (highest scores) to those with the least impact (lowest scores).

### Corrective Action 2 – Conduct gap analyses surrounding the ability to restore via the critical business processes.

The ITDRO performed an analysis of application actual recovery times and the actual restoration times of the critical business processes those applications support. The analysis was limited to 62 applications residing at the IRS's three computing centers. Application recovery timeline diagrams have been prepared measuring the ability to recover the applications and restore the critical business processes supported by those applications. The results of the analysis were presented in terms of recovery situation assessments by computing center, application, and critical business process. Analysis updates following infrastructure upgrades have shown a steady reduction in restoration times of critical business processes. For example, the analysis indicates that the restoration time of the processing tax returns critical business process has been reduced from about 60 days to between 5 and 7 days. While these analyses have been conducted for the 62 applications at the three computing centers, future analyses will include approximately 100 remaining applications that support critical business processes.

### Corrective Action 3 – Develop an analysis comparing the recovery time objective and recovery point objective of both the MITS organization and Business Operating Divisions.

The IRS's business impact analysis included an analysis to identify gaps between the recovery time objectives of applications owned by the Business Operating Divisions and the recovery time objectives of the MITS infrastructure. The purpose of the analysis was to determine whether current MITS organization recovery strategies address Business Operating Division requirements



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

for application recovery. Each application underwent this analysis to produce a summary of potential gaps in the IRS's ability to recover applications within their stated time objectives. The analysis compared the recovery time objective of applications to the recovery time objective of the primary general support system in which the application resides. If the recovery time objective of the general support system was not sufficient to recover the application within its recovery time objective, a potential gap was identified. Highlighting potential gaps between requirements driven by Business Operating Division application recovery times and general support system recovery times can enable both the Business Operating Divisions and the MITS organization to prioritize and address deficiencies in disaster recovery capabilities. The gap analysis revealed significant deficiencies in the IRS's ability to quickly recover even the most critical tax processing systems. As of October 2008, gaps of 60 days or more were identified for some systems. Other gaps showed that some systems could not be recovered at all at an offsite location.

Since the initial gap analysis results in October 2008, the ITDRO has undertaken efforts to close the gaps between the Business Operating Division and MITS organization recovery time objectives. Under the Technical Assessment corrective action, the ITDRO continues to assess the IRS's IT infrastructure to identify, prioritize, and implement improvements in capacity and equipment in an effort to improve disaster recovery capabilities and shorten recovery times for applications and critical business processes. The ITDRO is currently conducting a Disaster Recovery Capabilities Analysis to determine the actual impacts of general support system failures on the applications that support the critical business processes. This analysis will provide information of the effect on the business operation if any part of the supporting systems is disrupted. Once the analysis is complete in June 2011, the results will be presented to the Business Operating Divisions, which will use the information to adjust their application recovery time objectives or provide resources to improve disaster recovery capabilities for the systems that support their applications and business operations.

Corrective Action 4 – Develop an infrastructure spend plan based on the analyses mentioned above.

Information about recovery capabilities identified in the gap analyses formed the basis for the infrastructure spend plan. The ITDRO identified short-term infrastructure needs to address mainframe enhancements to improve recovery times of applications that support the most critical returns and remittance processing business processes. In Fiscal Year 2010, for the first time, funding was provided specifically for improving the IRS's disaster recovery capabilities. Of a \$9 million allotment, \$5 million was expended in Fiscal Year 2010 for procuring equipment and storage capacity to improve recovery times of the most critical mainframe core tax processing systems. The remaining \$4 million will carry over to Fiscal Year 2011. For Fiscal Year 2011, an additional \$9 million has been approved for additional improvements that will go beyond mainframe improvements to include disaster recovery improvements for applications that



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

provide overall support to operational functions. The IRS's Fiscal Year 2012 Budget Request includes \$12 million to make further improvements in the IRS's disaster recovery capabilities.

**Corrective actions for the Disaster Recovery Compliance component are being adequately completed**

The IRS is in the process of completing its corrective actions for the Disaster Recovery Compliance component and expects to close it by July 2011. The corrective actions the IRS completed during the time of our audit fieldwork are being adequately completed.

Corrective Action 1 – Complete internal auditing of the disaster recovery efforts to ensure accuracy and completeness as it relates to day-to-day operations and efforts to mitigate the material weaknesses and audits.

The ITDRO developed a manual that provides guidance, procedures, and methodology for performing compliance reviews and audits that verify and validate whether disaster recovery planning processes and activities comply with requirements. The manual contains auditing procedures broken down into the following seven sections:

- Initiate and plan the program.
- Gather data for the project.
- Prepare for the compliance review.
- Conduct the compliance review.
- Consolidate findings for the draft report.
- Issue final report.
- Follow up.

The manual was generally complete and consistent with guidance recommended in NIST SP 800-115 and contained in the Treasury Inspector General for Tax Administration audit manual.

**Management Action:** During the course of the audit, we recommended to the ITDRO several changes to its corrective actions which it was in the process of completing prior to us issuing this report.

**Corrective actions for the Disaster Recovery Plans component were adequately completed**

The Disaster Recovery Plans component contained two corrective actions that the IRS closed in December 2010.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

Corrective Action 1 – Develop and maintain disaster recovery plans associated with general support systems, to include all components that support critical applications.

The ITDRO created a template for preparing application disaster recovery plans and another template for preparing general support system disaster recovery plans. The templates were complete and consistent with requirements in NIST SP 800-34.

The IRS has developed procedures for preparing disaster recovery plans, has prepared disaster recovery plans for all of its systems, and reviews and updates them on an annual basis as required by NIST SP 800-34.

Corrective Action 2 – Establish and maintain data and processing backup-recovery capabilities and ensure maximum allowable outage times meet the recovery time objectives of the applications being supported.

The IRS has a process in place whereby the ITDRO works with system owners to establish the systems' recovery time objectives, review the recovery processes, and identify system upgrades that can decrease actual recovery times. The process is consistent with the contingency planning process steps in NIST SP 800-34. The disaster recovery plan templates for applications and general support systems contain a section that requires insertion of the system recovery time objectives. IRS forms used to update disaster recovery plans ask for updated recovery time objectives. The Disaster Recovery Test Plan has a section that analyzes and compares actual recovery times of the systems included in the test to their recovery time objectives.

The IRS has recently installed system upgrades that reduced the recovery time objectives for certain applications from as much as 30–60 days to 5–7 days. However, this still exceeds recovery time objectives that range, depending on the application, from 12 to 36 hours. The IRS's efforts to address these gaps are covered in this report in the Business Impact Analysis and the Technical Assessment component sections.

**Corrective actions for the Disaster Recovery Plan Test and Exercise component were adequately completed**

The Disaster Recovery Plan Test and Exercise component contained four corrective actions that the IRS closed in October 2008.

Corrective Action 1 – Develop baseline expectations, requirements, and templates for disaster recovery plans and disaster recovery plan tests and exercises.

Disaster recovery policies and procedures, disaster recovery plan preparation guidance, and testing and exercising guidance in 1) Internal Revenue Manual 10.8.60, 2) Interim Internal Revenue Manual 10.8.62, 3) IRS application and general support system disaster recovery plan templates, and 4) IRS exercising and testing templates were complete and consistent with NIST SP 800-34, NIST SP 800-53, NIST SP 800-84, and Treasury Directive Publication 85-01 requirements.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

Corrective Action 2 – Identify roles and responsibilities of the MITS organization and Business Operating Divisions involved in the testing.

We reviewed all disaster recovery roles and responsibilities defined in IRS disaster recovery manuals and in the roles and responsibilities manual, not just roles and responsibilities for disaster recovery testing, and found that they were generally complete and consistent with NIST SP 800-12, NIST SP 800-16, NIST SP 800-34, NIST SP 800-37, and Treasury Directive Publication 85-01 requirements.

Corrective Action 3 – Identify the frequency and type of testing required and reporting requirements.

Testing frequency, type of tests required, and reporting requirements defined in IRS disaster recovery manuals were complete and consistent with NIST SP 800-34, NIST SP 800-53, NIST SP 800-84, and Treasury Directive Publication 85-01 requirements. For systems whose lack of availability would have only a limited adverse impact on the organization, the IRS requires that some of these systems receive a higher level of testing than is required by NIST and the Department of the Treasury requirements.

Corrective Action 4 – Conduct tabletop, functional, and end-to-end disaster recovery testing for critical applications based upon direction from the Department of the Treasury and the Federal Information Security Management Act.

Because the IRS closed this corrective action in October 2008, we reviewed disaster recovery exercising and testing during the Federal Information Security Management Act's 2008 reporting cycle and found that all systems received the levels of testing required by NIST SP 800-34, NIST SP 800-53, NIST SP 800-84, and Treasury Directive Publication 85-01 requirements, whereby systems whose lack of availability would have a more serious impact on the organization received more extensive testing.

**Management Action:** During the course of the audit, we recommended to the ITDRO several changes to the second corrective action, which it completed prior to us issuing this report.

**Corrective actions for the Technical Assessment component are being adequately completed**

The Technical Assessment component contains four corrective actions, and its original closure date has been extended from October 2010 to July 2011. Due to the ITDRO expanding the scope of its original corrective action, in September 2010, the Associate Chief Information Officer, Cybersecurity, executive owner of the disaster recovery material weakness, granted the ITDRO an extension to July 2011. The previous work efforts have expanded from a computing center focus to include campus assets. The expansion also takes into consideration people, processes, and technology considerations in a disruption or disaster. The corrective actions the IRS completed during the time of our audit fieldwork are being adequately completed.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

Corrective Action 1 – Perform annual system risk assessments.

The ITDRO conducts ongoing system risk assessments while other IRS programs perform annual as well as ongoing system risk assessments. Examples of these activities include, but are not limited to: annual Federal Information Security Management Act reviews including certification and accreditations, the enterprise continuous monitoring program, the disaster recovery plan testing program, ongoing system vulnerability assessments and scans, penetration testing and source code analysis, the Critical Infrastructure Protection program, and ongoing disaster recovery business impact and technical assessments.

Corrective Action 2 – Develop a true redundancy and resiliency analysis. Based on the critical business processes, develop site-based restoration vulnerabilities analysis.

The ITDRO began its efforts to develop a true redundancy and resiliency analysis with the Martinsburg Business Resiliency Analysis in 2009. The analysis focused on a disaster scenario at the Enterprise Computing Center (ECC) in Martinsburg, West Virginia, and the ability to recover the functionality of impacted applications and restore related critical business processes at the ECC in Memphis, Tennessee. The analysis identified deficits between ECC-Martinsburg and ECC-Memphis capabilities. For example, recovery times at ECC-Memphis for 15 key ECC-Martinsburg systems ranged from 3 days to more than 60 days and that other systems could not be recovered at ECC-Memphis. Subsequent infrastructure improvements during Fiscal Year 2010 identified in the infrastructure spend plan have resulted in reductions in the initial application recovery times down to the 5–7 day range. Since the initial ECC-Martinsburg analysis, the ITDRO has established the Disaster Recovery Capability Analysis to complete the analysis of applications supporting critical business processes at the computing centers and non-computing center locations. Through this project, the ITDRO is identifying and implementing IT technologies to further reduce the restoration times to hours based on business requirements.

Corrective Action 3 – Create a recovery point objective and recovery time objective analysis and gain concurrence from both the Business Operating Divisions and the MITS organization.

The analysis of recovery point and recovery time objectives is still in progress and has a target completion date of June 2011. As part of the business impact analysis workshops, each business unit was provided their specific recovery point and recovery time objectives for their review and approval. The Disaster Recovery Capability Analysis targeted for completion in June 2011 will provide the business units with more accurate information about current infrastructure capabilities and the time required to recover applications.

As of February 2011, the ITDRO has established the following recovery times for 97 of the 162 applications that support the critical business processes. The 97 applications include 44 (68 percent) of the 65 applications that support the top 2 critical business processes of returns and remittance processing.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

- 24 percent (23 applications) in 3 days or less.
- 25 percent (24 applications) in 3–5 days.
- 12 percent (12 applications) in 6–29 days.
- 39 percent (38 applications) in 30 days or more.

The Business Operating Divisions will use the Capability Analysis information to reevaluate their recovery time objectives to better align with technical capabilities or to consider providing funding for infrastructure improvements that will result in recovery times that meet their business needs.

Corrective Action 4 – Incorporate a technical assessment tool that will provide an infrastructure impact analysis in the event of a disaster.

To accomplish this corrective action, the ITDRO is deploying a web-based system, the Toolkit Suite with Command Centre (TSCC). The TSCC system is a decision-support tool and plan repository for disaster recovery. When a disaster occurs, the tool (when fully implemented) will identify the people, processes, and systems that have been impacted. It will provide critical information for decision making during disaster events and exercises, identify restoration priorities, and determine the disaster recovery plans that should be activated. Its contents will serve as the sole source for recovering, relocating, or rebuilding IRS business processes and supporting systems. This tool will be synchronized with and receive employee data from personnel and timekeeping systems, as well as systems, hardware, and server data from IT inventory systems.

The TSCC is a multi-modular system that will be implemented in phases. Full implementation is expected by Fiscal Year 2013. Currently, disaster recovery plans, incident management plans, and evacuation plans have been loaded into the system and it has been used in the most recent disaster recovery tests at the computing centers. At present, there are about 3,000 TSCC users across the IRS.

**Management Action:** During the course of the audit, we recommended a change to the ITDRO for the first corrective action, which it completed prior to us issuing this report.

## ***Recommendation***

**Recommendation 1:** The Chief Technology Officer should ensure that the capability is developed to track the disaster recovery training of employees with disaster recovery roles and responsibilities.

**Management's Response:** The IRS agreed with our recommendation. The IRS plans to develop a formal process and monitoring system to track the completion of



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

disaster recovery training by employees who have disaster recovery roles and responsibilities.

***Improvements Are Needed in the Corrective Actions for the Metrics  
Component of the Disaster Recovery Material Weakness***

The IRS is in the process of developing its corrective action for the Metrics component and expects to close it by December 2011. Improvements to corrective actions are needed for metrics the IRS is developing for each component, except for the Disaster Recovery Plan Test and Exercise component.

Corrective Action 1 – Establish and maintain collection and reporting of metrics to assess progress and track improvements in all component activity implementations over time.

The IRS provided us with its ongoing operational metrics and planned metrics. These metrics are designed to report on the various activities within the ITDRO for a given reporting period. However, the IRS does not have metrics specifically designed to assess progress and track improvements in the following five components of the disaster recovery material weakness over time.

- Policy component.
- Business Impact Analysis component.
- Disaster Recovery Compliance component.
- Disaster Recovery Plans component.
- Technical Assessment component.

For the Policy component, the IRS did not have metrics for the corrective action on conducting outreach and awareness sessions. For the corrective action on developing an enterprise-wide disaster recovery course curriculum, while the IRS has some metrics on disaster recovery courses created, courses delivered by the ITDRO, and attendance, it did not have metrics on the percentage of employees with disaster recovery responsibilities that attended any of the available IRS courses, not just courses developed by the ITDRO. This is an all-encompassing metric that measures the extent appropriate employees attend training.

For the Business Impact Analysis component, the IRS had a metric for the number of systems with a business impact analysis, but a more meaningful metric would be the percentage of systems with a completed business impact analysis. For the corrective action on gap analyses, metrics are needed, such as the percentage of systems that can be recovered within recovery time requirements, the percentage of systems that can be recovered slightly beyond recovery time requirements, and the percentage of systems that can be recovered significantly beyond recovery time requirements.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

For the Disaster Recovery Compliance component, the IRS had a metric for the targeted and actual number of reviews planned and the percentage of targeted reviews achieved. Metrics could be created for the number and percentage of compliance audits planned and completed and for the percentage of recommendations and corrective actions that have been implemented.

For the Disaster Recovery Plans component, the IRS had the following metrics for the corrective action on the development and maintenance of disaster recovery plans:

- The targeted number and actual number of disaster recovery plans reviewed as part of annual Certification and Accreditation.
- The percentage of targeted disaster recovery plan reviews achieved.
- The targeted number and actual number of disaster recovery plans completed.
- The percentage of targeted disaster recovery plans completed.
- The total number of disaster recovery plans reviewed and updated for the current Federal Information Security Management Act cycle.
- The percentage of disaster recovery plans written for critical systems.

Additional metrics for this corrective action could include:

- The percentage of general support systems that have a disaster recovery plan.
- The percentage of applications that have a disaster recovery plan.

For the corrective action on establishing and maintaining data and processing backup-recovery capabilities, metrics are needed, such as the percentage of systems that have established and successfully tested data backup-recovery capability and the percentage of systems that have established and successfully tested processing backup-recovery capability. In addition, for the Technical Assessment component, metrics are needed to measure the extent to which each of the corrective actions has been completed and the results that each has achieved.

The IRS needs to develop more specific metrics on the five components as it continues its work on this corrective action. The creation of metrics to assess progress and track improvements in components of the disaster recovery material weakness is required by the IRS Computer Security Material Weakness Action Plan. In addition, NIST SP 800-55 provides guidelines on how metrics can be used to determine the adequacy of in-place security controls, policies, and procedures. NIST SP 800-55 can be used to develop, select, and implement system-level and program-level metrics to indicate the implementation, efficiency, effectiveness, and impact of security controls and other security-related activities.

NIST SP 800-55 states that metrics are usually expressed as percentages and averages and that the process being measured must be measurable, consistent, and repeatable. One specific type of metric cited by NIST, implementation metrics, are metrics used to demonstrate progress in



## *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed*

---

implementing security programs, such as the percentage of systems that have approved system security plans. The IRS could use implementation metrics to measure the extent to which the corrective actions have been completed.

The IRS is still in the process of developing corrective actions for establishing and maintaining metrics. Improved metrics will help to facilitate decision making, improve performance, and increase accountability related to the completion of the disaster recovery corrective actions.

### ***Recommendation***

**Recommendation 2:** The Chief Technology Officer should ensure that metrics specifically designed to assess progress and track improvements in completing the corrective actions of five components of the disaster recovery material weakness over time are developed using guidance contained in NIST SP 800-55.

**Management's Response:** The IRS agreed with our recommendation. The IRS plans to design metrics using NIST SP 800-55 to assess the progress of the disaster recovery program.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to evaluate the IRS's corrective actions for addressing its disaster recovery material weakness. To accomplish our objective, we:

- I. Evaluated the effectiveness of corrective actions taken on completed components of the disaster recovery material weakness.
  - A. For the Policy component, we:
    1. Determined whether IRS disaster recovery manuals were complete and consistent with Federal requirements and guidance.
    2. Reviewed the frequency and scope of outreach and awareness sessions that the IRS conducted to help move the manuals into day-to-day operations.
    3. Determined whether IRS disaster recovery course curriculum sufficiently covered the range of elements comprised in a disaster recovery program.
  - B. For the Business Impact Analysis component, we:
    1. Reviewed the process used by the IRS to develop a prioritized list of critical systems.
    2. Determined whether the IRS completed its site-based restoration priority documents.
    3. Reviewed the process used by the IRS to conduct restoration gap analyses.
    4. Reviewed the IRS's analysis of Business Operating Division and MITS organization recovery time objectives.
    5. Reviewed the IRS's spend plan for reducing recovery times.
  - C. For the Disaster Recovery Plan Test and Exercise component, we:
    1. Determined whether IRS baseline expectations, requirements, and templates were complete and consistent with Federal requirements and guidance.
    2. Determined whether the IRS had a complete set of disaster recovery roles and responsibilities.
    3. Determined whether the frequency and types of testing required by the IRS and IRS reporting requirements were complete and consistent with Federal requirements.



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

4. Determined whether the IRS conducted appropriate annual exercises and tests for all Federal Information Security Management Act systems.
- II. Evaluated the effectiveness of corrective actions taken to date on open components of the disaster recovery material weakness.
- A. For the Disaster Recovery Compliance component, we evaluated the plans, procedures, and methods that the IRS will be using to conduct an internal disaster recovery compliance program.
  - B. For the Disaster Recovery Plans component, we:
    1. Determined whether the IRS had prepared and maintained disaster recovery plans for all Federal Information Security Management Act systems using IRS plan templates.
    2. Determined whether the IRS established and maintained data and processing backup-recovery capability.
    3. Reviewed the process used to establish and maintain whether recovery capability and outage times meet objectives.
  - C. For the Technical Assessment component, we:
    1. Determined whether the IRS performed annual risk assessments.
    2. Reviewed the IRS's process for developing a true redundancy and resiliency analysis.
    3. Determined whether the IRS developed a site-based restoration vulnerability analysis.
    4. Determined whether concurrence was obtained from both the MITS organization and Business Operating Divisions on recovery objectives.
    5. Determined how the IRS plans to use an application or tool it procured that assists in assessing and responding to a disaster.
  - D. For the Metrics component, we determined whether the IRS had developed appropriate metrics for assessing and tracking progress in completing its corrective actions.

**Internal controls methodology**

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for

---

<sup>1</sup> This component was open when we performed the audit, but is now closed.



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: the Cybersecurity organization's policies, procedures, and practices for addressing the disaster recovery material weakness. We evaluated these controls by interviewing staff of the Cybersecurity organization and by reviewing the corrective actions being taken to address the components of the material weakness.



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

**Appendix II**

*Major Contributors to This Report*

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Kent Sagara, Director  
Danny Verneuille, Director  
Carol Taylor, Audit Manager  
Joan Bonomi, Senior Auditor  
Richard Borst, Senior Auditor  
Stasha Smith, Senior Auditor  
Kasey Koontz, Auditor



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Director, Security Risk Management OS:CTO:C:SRM  
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 Liaison: Director, Risk Management Division OS:CTO:SP:RM



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

**Appendix IV**

*National Institute of Standards and Technology  
Publications*

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*

NIST Special Publication 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model (Draft)*

NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems*

NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*

NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*

NIST Special Publication 800-55, *Performance Measurement Guide for Information Security*

NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

**Appendix V**

*Glossary of Terms*

<b>Term</b>	<b>Definition</b>
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.
Certification and Accreditation	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the requirements for the system.
Cybersecurity Organization	Manages the IRS's IT Security program. It is responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing measures to assure the confidentiality, integrity, and availability of IRS electronic systems, services, and data. It is within the MITS organization.
End-to-End Testing	Testing that involves recovering applications and systems at the recovery location using the production environment.
Enterprise Computing Centers	IRS sites that support tax processing and information management through a data processing and telecommunications infrastructure.
Federal Managers' Financial Integrity Act of 1982	Requires each Federal agency to conduct annual evaluations of its systems of internal accounting and administrative control. Each agency is also required to prepare an annual report for Congress and the President that identifies material weaknesses and the agency's corrective action plans and schedules.



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

<b>Term</b>	<b>Definition</b>
Functional Exercises	Exercises in which recovery personnel execute their roles in a simulated operational environment. Functional tests involve retrieving, loading, and validating backup tapes and files.
Material Weakness	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.
Modernization and Information Technology Services	The IRS organization that delivers IT services and solutions which drive effective tax administration to ensure public confidence.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Office of Management and Budget	The office within the Executive Office of the President that helps executive departments and agencies implement the commitments and priorities of the President.
Recovery Point Objective	The point in time, prior to a disruption, that data can be recovered.
Recovery Time Objective	The maximum amount of time a system can remain unavailable before there is an unacceptable impact on other systems or supported business processes.
Resiliency	The ability to quickly adapt and recover from any known or unknown changes to the environment. Resiliency is not a process, but rather an end-state for organizations. The goal of a resilient organization is to continue mission-essential functions at all times during any type of disruption.



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

<b>Term</b>	<b>Definition</b>
Tabletop Exercises	Exercises that are discussion-based and take place in a classroom setting. Participants use disaster recovery plans to discuss how they would respond to a disruption scenario.



*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

**Appendix VI**

*Management's Response to the Draft Report*



CHIEF TECHNOLOGY OFFICER

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

JUN 06 2011



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

Terence V. Milholland  
Chief Technology Officer

SUBJECT:

Draft Audit Report – Corrective Actions to Address the Disaster  
Recovery Material Weakness Are Being Completed  
(Audit # 201020024) (i-trak #2011-21559)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. We appreciate your report recognizing that the Internal Revenue Service adequately completed six of the seven components of the Disaster Recovery Material Weakness, as well as acknowledging major enhancements completed during the disaster recovery remediation efforts from Fiscal Year 2008 through Fiscal Year 2010.

The IRS is committed to continuously improving the security of our information technology systems and disaster recovery processes; your suggested recommendations will further improve our security posture. We agree with both of the report recommendations made as a result of your audit. The attachment to this memo details our planned corrective actions to implement the recommendations.

Your continued support and the assistance and guidance your team provides have been a valuable resource to our organization. If you have any questions, please contact me at (202) 622-6800 or Andrea Green-Horace, Senior Manager Program Oversight, at (202) 283-3427.

Attachment



---

*Corrective Actions to Address the Disaster Recovery  
Material Weakness Are Being Completed*

---

Attachment

Draft Audit Report – Corrective Actions to Address the Disaster Recovery Material Weakness  
Are Being Completed (Audit # 201020024) (e-trak # 2011-21559)

---

**RECOMMENDATION #1:** The Chief Technology Officer should ensure that the capability is developed to track the disaster recovery training of employees with disaster recovery roles and responsibilities.

**CORRECTIVE ACTION #1:** The Disaster Recovery training program coordinator within the Cybersecurity, Security Risk Management organization, will establish a formal Disaster Recovery training curriculum that will be required to be administered annually to all enterprise-wide staff that have a direct role and responsibility supporting Disaster Recovery. This organization will then annually coordinate with all business and technical stakeholders to identify all staff who will be required to take the training for the current year. A formal process and manual monitoring system will be developed to track the completion of the training for each individual identified.

**IMPLEMENTATION DATE:** December 1, 2011

**RESPONSIBLE OFFICIAL:** ACIO, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

**RECOMMENDATION #2:** The Chief Technology Officer should ensure that metrics specifically designed to assess progress and track improvements in completing the corrective actions of five components of the disaster recovery material weakness over time are developed using guidance contained in NIST SP 800-55.

**CORRECTIVE ACTION #2:** Now that the Disaster Recovery Program component areas have reached a level of maturity, metrics will be designed, utilizing NIST SP 800-55 to assess the progress of the Disaster Recovery Program.

**IMPLEMENTATION DATE:** December 1, 2011

**RESPONSIBLE OFFICIALS:** ACIO, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.