The Disaster Recovery Program Has Improved, but It Should Be Reported As a Material Weakness Due to Limited Resources and Control Weaknesses

March 2005

Reference Number: 2005-20-024

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.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

March 1, 2005

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The Disaster Recovery Program Has Improved, but It Should Be Reported As a Material Weakness Due to Limited Resources and Control Weaknesses (Audit # 200420031)

This report presents the results of our review of the Internal Revenue Service's (IRS) disaster recovery program. The objective of this review was to provide an overall assessment of the IRS' disaster recovery program.

In summary, the IRS Commissioner stated, in the *IRS Strategic Plan 2005 – 2009*,[1] ". . . providing excellent service to taxpayers and enforcing America's tax laws in a balanced manner . . . are equally important priorities." The means and strategies to accomplish the Strategic Plan goals include "Develop, exercise and maintain continuity of operations plans, contingency plans and other measures to protect critical infrastructure." During Fiscal Years (FY) 2002 through 2004, IRS management initiated and/or completed several actions that demonstrated the increased emphasis on emergency management and preparedness, including disaster recovery planning. For example, Modernization and Information Technology Services (MITS) organization management implemented an inhouse Master File[2] disaster recovery capability and completed corrective actions on prior audit recommendations. Mission Assurance (MA) organization management began coordinating the Business Resumption Strategy and Disaster Recovery Strategy development efforts and established the Emergency

[1] Publication 3744, revised June 2004.

[2] The IRS database that stores various types of taxpayer account information. The Individual, Business, and Employee Plans Master Files were identified as critical business systems.

Management and Preparedness Working Group to help coordinate and facilitate the development of all IRS emergency preparedness activities.

However, significant disaster recovery program weaknesses continue to be unresolved. Our analysis of 11 prior Treasury Inspector General for Tax Administration (TIGTA) audit reports identified recurring disaster recovery program weaknesses, including modernization systems being placed in production without a disaster recovery capability, insufficient disaster recovery capacity, roles and responsibilities not being assigned and employees not being trained, and annual tests not being conducted or not being effective (see Appendix IV for a list of the 11 reports). We also determined 27 of 44 corrective actions for prior recommendations had not been completed.

Shrinking budgets have limited management's efforts to correct disaster recovery problems. The IRS Information Systems and Business Systems Modernization (BSM) budgets have decreased from 7,466 Full-Time Equivalents (FTE)[3] and $1.971 billion in FY 2003 to 7,385 FTEs (1.1 percent reduction) and $1.958 billion (0.7 percent reduction, including a 24.4 percent reduction in the BSM budget) in FY 2005.

Since October 2001, MITS organization management has worked to provide resources to improve disaster recovery capabilities, with limited results. After the terrorist attacks on September 11, 2001, the Congress approved $13.5 million for the Master File disaster recovery capability. However, requests for $74.1 million to fund disaster recovery needs were turned down. For FY 2005, Enterprise Operations office management requested $16.7 million for Enterprise Computing Center[4] mainframe computer improvements that would ensure disaster recovery capabilities. However, budget cuts have prevented management from reallocating funds to these items.

The Modernization Disaster Recovery Project has not developed and implemented a midrange computer system disaster recovery infrastructure although the Modernized e-File system[5] is in production and additional midrange computer systems, such as the Integrated Financial System[6] and Custodial Accounting Project,[7] are scheduled to enter production in FY 2005.

Finally, MITS organization management advised us personnel trained and responsible for disaster recovery support duties were reassigned to the MA organization in the October 2003 MA organization realignment, but the MITS organization is still responsible for the duties. Senior MITS and MA organization managers are working on

[3] A measure of labor hours in which 1 FTE is equal to 8 hours multiplied by the number of compensable days in a particular fiscal year. For FY 2004, 1 FTE was equal to 2,096 staff hours. For FY 2005, 1 FTE is equal to 2,088 hours.

[4] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

[5] Develops the modernized web-based platform for filing IRS forms electronically.

[6] Provides the IRS better financial budgeting, planning, tracking, reporting, and management.

[7] Uses a data warehousing approach to provide the IRS detailed taxpayer account information to be used for analysis and financial reporting.

this issue but, as of August 2004, had not resolved how best to transfer the personnel resources or work.

In addition, insufficient management oversight has hampered the identification and resolution of program weaknesses. MA organization management advised us the Federal Information Security Management Act (FISMA)[8] requirements are the focus of their security program oversight efforts. However, the TIGTA's FY 2004 FISMA report to the Department of the Treasury[9] stated the IRS Plans of Action and Milestones (POA&M) do not contain details sufficient to permit oversight and tracking of security weaknesses. As a result, the current POA&M system weaknesses could not be analyzed for recurring issues that might indicate systemic problems that should be elevated to the program weakness level. Insufficient resources and management oversight increase the risk that the critical systems supporting the IRS Commissioner's service and enforcement priorities cannot be timely recovered if a disaster occurs.

To ensure service and enforcement priorities can be met, we recommended the Chief Information Officer (CIO) report a disaster recovery program material weakness to the Department of the Treasury and include new and currently underway improvement activities in the corrective action plan. The CIO should also work with the Chief, MA, to implement FISMA POA&M procedures to analyze system weaknesses for systemic problems and elevate them as program-level weaknesses.

Management's Response: IRS management agreed with our recommendations and will declare the disaster recovery program a material weakness. IRS management responded the IRS could recover all vital data for the most mission critical information technology systems, including the Master File and the Customer Account Data Engine (CADE).[10] They are committed to increasing disaster recovery capabilities based on available funding and an evaluation of cost and risk factors. The MA organization is responsible for coordinating the development of an IRS-wide business resumption strategy. The MITS organization has identified its current disaster recovery and business resumption strategies, including both data recovery point and recovery time objectives, for all major systems. The crucial business processes were identified and prioritized and will be mapped to the specific computing system major applications and general supporting systems, and a gap analysis will be conducted to identify inadequate disaster recovery capabilities. IRS management will also coordinate with the Department of the Treasury and the Office of Management and Budget to request the necessary funding. In addition, IRS senior leadership established an executive working group to implement FISMA POA&M procedures. Management's complete response to the draft report is included as Appendix V.

[8] E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

[9] *Treasury Inspector General for Tax Administration Federal Information Security Management Act Report Fiscal Year 2004,* dated September 10, 2004.

[10] The CADE is the foundation for managing taxpayer accounts in the IRS modernization plan. The CADE will consist of databases and related applications to replace the IRS' existing Master File processing systems.

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

Background

The Internal Revenue Service (IRS) Commissioner stated, in the *IRS Strategic Plan 2005 – 2009*,[1] "… providing excellent service to taxpayers and enforcing America's tax laws in a balanced manner … are equally important priorities." The Strategic Plan includes the goal "Modernize the IRS through its People, Processes and Technology" and the objective "Ensure the Safety and Security of People, Facilities and Information Systems." The means and strategies to accomplish this objective include "Develop, exercise and maintain continuity of operations plans, contingency plans and other measures to protect critical infrastructure." The Strategic Plan states the IRS will implement disaster recovery capabilities for the Computing Centers,[2] plans for critical infrastructure assets, and business continuity plans for all mission critical and business essential processes, facilities, and assets.

Disaster recovery is an organization's ability to respond to an interruption in services by implementing a plan to restore critical business functions. Disaster recovery is a subset of interrelated business continuity disciplines including business resumption, occupant emergency planning, and incident management. A disaster recovery plan defines the resources, actions, tasks, and data required to restore information systems in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals, thereby minimizing the effects of a major disruption.

The Modernization and Information Technology Services (MITS) and Mission Assurance (MA) organizations have disaster recovery responsibilities. The MITS organization is responsible for developing and maintaining disaster recovery plans to support information system contingency and recovery operations. The MA organization is responsible for establishing policies and procedures, providing guidance, and overseeing the implementation of the policies and procedures.

[1] Publication 3744, revised June 2004.

[2] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

During Fiscal Years (FY) 2002 through 2004, we reviewed several IRS disaster recovery strategies and other disaster recovery related topics. Appendix IV lists the 11 prior audit reports reviewed for this review's overall assessment.

This review was performed in the offices of the Chief Information Officer (CIO) and Chief, MA, at the IRS National Headquarters in New Carrollton, Maryland, during the period June through November 2004. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Management Increased Emphasis on Emergency Management and Preparedness, Including Disaster Recovery Planning

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, requires Federal Government agencies to provide for continuity of support and contingency planning for their general support systems and major applications. The Internal Revenue Manual (IRM) states senior management responsibilities, shared among business units, require coordination, such as allocation of resources and training to implement business continuity plans, acquisition of alternate workspace, and development of priorities for restoring work. In particular, the Associate CIO, Information Technology Services, is responsible for ensuring information system resources are adequately protected and consistent with security policies, standards, and procedures and for ensuring contingency planning capabilities (e.g., disaster recovery). The Chief, MA, is responsible for ensuring all applicable security policies, procedures, and control techniques are implemented for systems and processing facilities; evaluating and overseeing all major information security programs; and managing core security operations, including existing disaster recovery capabilities.

During FYs 2002 through 2004, IRS management initiated and/or completed several actions that demonstrated the increased emphasis on emergency management and preparedness. For example:

- The MITS organization received $13.5 million for antiterrorist spending in January 2002 and implemented an inhouse Master File[3] disaster recovery capability to address the disaster recovery material weakness.

- In December 2003, the MA organization began coordinating the Business Resumption Strategy (BRS) and Disaster Recovery Strategy (DRS) development efforts with the MITS organization and other business units. Each organization is identifying its BRS and validating the critical business processes,[4] recovery time objectives,[5] and recovery point objectives.[6] This information will be used to set the DRS requirements and priorities for the MITS organization disaster recovery plans.
- The Chief, MA, issued a memorandum, dated July 2, 2004, to business operating division commissioners and support organization chiefs citing the Commissioner's priority to enhance the IRS' security posture and related emergency management and preparedness capabilities.
- In July 2004, the Emergency Management and Preparedness Working Group was established to help coordinate and facilitate all IRS emergency preparedness activities, including information systems contingency and disaster recovery planning.
- Corrective actions for Treasury Inspector General for Tax Administration (TIGTA) audit recommendations are being completed. Examples of corrective actions completed in FYs 2003 and 2004 include:

[3] The IRS database that stores various types of taxpayer account information. The Individual, Business, and Employee Plans Master Files were identified as critical business systems.

[4] Mission critical business processes include processing remittances, tax returns, and tax refunds; administrative and infrastructure critical processes include providing a safe and equipped working environment and processing payroll.

[5] The time needed to recover from a disaster; how long the IRS could afford to be without its information systems.

[6] Describes the age of the data to be restored in the event of a disaster; the amount of data the IRS could afford to lose.

- MA organization management coordinated with the various IRS organizations managing the business continuity and disaster recovery planning area to define the roles, responsibilities, and expectations for each area (see Appendix IV, Audit Report number 1).
- MITS organization management assigned the responsibilities for preparing and testing Computing Center disaster recovery plan sections to appropriate personnel (see Appendix IV, Audit Report numbers 3, 8, and 9).
- Detroit Computing Center management corrected midrange computer disaster recovery data and documentation backup and offsite storage problems (see Appendix IV, Audit Report number 3).
- MITS organization personnel conducted annual Computing Center mainframe computer system disaster recovery plan tests in 2004, including integrated testing of selected interdependent mainframe computer disaster recovery plans (see Appendix IV, Audit Report numbers 6 and 9).

While senior management has committed the IRS to emergency management and preparedness, additional resources and improved management oversight are needed to ensure the information systems that support the IRS Commissioner's service and enforcement priorities can be recovered timely if a disaster occurs.

Significant Disaster Recovery Program Weaknesses Continue to Be Unresolved

The Federal Information Security Management Act (FISMA)[7] requires each Federal Government agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operation for information systems that support agency operations and assets. Department of the Treasury Publication 85-01 (TD P 85-01), *Treasury Information Technology Security Program,* states bureaus shall develop and maintain detailed

[7] E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

disaster recovery plans and the associated recovery capability in the event normal operations are disrupted. The IRM requires IRS management to allocate the resources required to support the recovery of critical processes and applications, including computer hardware and software.

In addition, the Federal Managers' Financial Integrity Act of 1982 (FMFIA)[8] requires each Federal Government 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 the Congress and the President that identifies material weaknesses and the agency's corrective action plans and schedules.

Analysis of prior TIGTA audit reports identified recurring disaster recovery program weaknesses

We analyzed 11 prior audit reports to identify recurring disaster recovery program weaknesses and concluded IRS management has not effectively addressed the program weaknesses. Details about the audit reports analysis are included in Table 1 (see Appendix IV for a list of the 11 audit reports).

[8] 31 U.S.C. §§ 1105, 1113, 3512 (2000).

Table 1: Reported Disaster Recovery Program Weaknesses

Reported Issues **Audit Reports (Appendix IV lists the audit report titles)**	**Modernization systems being placed in production without a disaster recovery capability**	**Disaster recovery capability not sufficient or cost effectiveness not assured**	**Data not protected or easily retrievable**	**Disaster recovery roles and responsibilities not assigned and employees not trained**	**Disaster recovery plans not complete and accurate**	**Annual disaster recovery tests not conducted or not effective**
1. The Business Continuity Program				X		
2. Protecting Critical Assets			X	X		
3. The Consolidated Midrange Computer Systems		X	X	X	X	X
4. Software Products to Manage and Control Computer Resources				X		X
5. The Integrated Financial System	X					
6. The Master File			X	X	X	X
7. The Custodial Accounting Project	X					
8. Data Communications		X		X	X	X
9. The Mainframe Computer Systems		X	X	X	X	X
10. The Integrated Financial System						X
11. The Customer Account Data Engine	X					
Number of Reports	**3**	**3**	**4**	**7**	**4**	**6**

Source: TIGTA audit reports.

We also analyzed the status of IRS management's corrective actions on the recommendations included in the 11 audit reports. Details about the corrective action status analysis are included in Table 2.

Table 2: Status of Management's Corrective Actions

Status (as of September 4, 2004) Audit Reports (Appendix IV lists the audit report titles)	Number of Corrective Actions	Open and Original Date Not Due	Open With Extended Due Date	Closed by Original Due Date	Closed With Extended Due Date
1. The Business Continuity Program	4			4	
2. Protecting Critical Assets	2	1		1	
3. The Consolidated Midrange Computer Systems	9		2	3	4
4. Software Products to Manage and Control Computer Resources	1			1	
5. The Integrated Financial System	1	1			
6. The Master File	7	5	1	1	
7. The Custodial Accounting Project	1	1			
8. Data Communications	8	5		3	
9. The Mainframe Computer Systems	11	11			
10. The Integrated Financial System	0				
11. The Customer Account Data Engine					
Number of Corrective Actions	**44**	**24**	**3**	**13**	**4**

Source: TIGTA audit reports and Department of the Treasury Joint Audit Management Enterprise System Audit Summary reports.

The scheduled completion dates for 27 open corrective actions ranged from September 2004 to January 2007. Management had not responded to a draft report (Audit Report number 11) or provided completion dates for corrective actions to two recommendations as of the date of our analysis. Therefore, the corrective actions will not immediately alleviate the disaster recovery risks.

Shrinking budgets have limited management's efforts to correct disaster recovery problems

We determined insufficient resources was one of the causes for recurring disaster recovery problems. The IRS

Information Systems (IS) and Business Systems Modernization (BSM) budgets[9] have decreased over the last several years. In FY 2003, the IS and BSM budgets provided 7,466 Full-Time Equivalents (FTE)[10] and $1.971 billion. However, the President's FY 2005 IS and BSM budget requests would provide 7,385 FTEs (1.1 percent reduction) and $1.958 billion (0.7 percent reduction, including a 24.4 percent reduction in the BSM budget).

Since October 2001, MITS organization management has worked to provide resources to improve disaster recovery capabilities, with limited results. After the terrorist attacks on September 11, 2001, IRS management considered MITS organization requests for $87.6 million for disaster recovery improvements, and the Congress approved $13.5 million for the Master File disaster recovery capability. In the review and approval process, requests for $74.1 million were turned down, including:

- Designing and defining the architecture for the Competency-Based Organization (CBO) and enterprise command centers. MITS organization management cited these two areas as corrective action for a Master File Disaster Recovery TIGTA audit recommendation (see Appendix IV, Audit Report number 6) and is using operations funds to implement the CBO.
- Upgrading the Enterprise Computing Center (ECC) mainframe computer disaster recovery capability. Insufficient ECC processing capacity was a finding in the Mainframe Computer Disaster Recovery TIGTA audit report (see Appendix IV, Audit Report number 9).

[9] The IS appropriation includes all of the automated data processing and telecommunications resources, including labor, hardware and software purchases, and other operations expenses.

[10] A measure of labor hours in which 1 FTE is equal to 8 hours multiplied by the number of compensable days in a particular fiscal year. For FY 2004, 1 FTE was equal to 2,096 staff hours. For FY 2005, 1 FTE is equal to 2,088 hours.

For FY 2005, Enterprise Operations office management requested $16.7 million for ECC mainframe computer improvements (e.g., Unisys mainframe computer upgrades, Virtual Tape System[11] development) that would ensure disaster recovery capabilities. Management categorized the upgrades and improvements as unfunded critical needs, but MITS organization budget cuts have prevented management from reallocating funds to these items. Without the mainframe computer upgrades and improvements, management estimated that, by FY 2006, the ECC could not recover the systems that operate on the Unisys mainframe computers if a disaster occurs.

In addition, the Modernization Disaster Recovery Project has not developed and implemented a midrange computer system disaster recovery infrastructure although the Modernized e-File (MeF) system[12] is in production and additional midrange computer systems, such as the Integrated Financial System[13] and Custodial Accounting Project,[14] are scheduled to enter production in FY 2005. The Modernization Disaster Recovery Project did not implement the MeF system disaster recovery capability in FY 2004 because only $3.3 million of the $9.9 million in the budget was provided to develop the architecture. The funds provided did not cover the Project's priorities. As a result, work stopped on the midrange computer disaster recovery infrastructure. As of September 2004, the remaining funds had not been provided and the infrastructure will be delayed.

Finally, MITS organization management advised us personnel trained and responsible for disaster recovery support duties (e.g., preparing and maintaining plans, test

[11] A virtual tape system combines high-speed disk, high-capacity tape, and storage management software to allow quick access to tape volumes located physically on disk but appearing to the computer as conventional tape.

[12] Develops the modernized web-based platform for filing IRS forms electronically.

[13] Provides the IRS better financial budgeting, planning, tracking, reporting, and management.

[14] Uses a data warehousing approach to provide the IRS detailed taxpayer account information to be used for analysis and financial reporting.

schedules, etc.) were reassigned to the MA organization in the October 2003 MA organization realignment. However, the MITS organization continues to be responsible for completing the disaster recovery duties. MITS organization management also advised us senior MITS and MA organization managers are working on this issue but, as of August 2004, had not resolved how best to transfer the personnel resources or work.

Insufficient management oversight has hampered the identification and resolution of program weaknesses

We determined insufficient management oversight was also a cause for recurring disaster recovery problems. MA organization management advised us the FISMA requirements are the focus of their security program oversight efforts. Draft FISMA procedures (issued in August 2004) state TIGTA audit findings will be listed as system weaknesses on the FISMA Plans of Action and Milestones (POA&M). The guidelines suggest management analyze system weaknesses to identify systemic problems and elevate them to the POA&M program weakness level. The POA&M status for each system and program weakness is reported quarterly to the OMB. However, the TIGTA's FY 2004 FISMA report to the Department of the Treasury[15] stated the IRS POA&Ms do not contain details sufficient to permit oversight and tracking of security weaknesses. As a result, the current POA&M system weaknesses do not individually identify the TIGTA audit findings and, therefore, could not be analyzed for systemic problems (i.e., recurring issues that might indicate a systemic problem) that should be elevated to the program weakness level. The IRS continues to have significant disaster recovery program issues because it has not effectively implemented management controls, such as FISMA POA&M procedures.

The IRS Commissioner's service and enforcement priorities are heavily dependent on the information systems that support the critical business processes. However,

[15] *Treasury Inspector General for Tax Administration Federal Information Security Management Act Report Fiscal Year 2004*, dated September 10, 2004.

insufficient resources to implement and operate disaster recovery capabilities, and insufficient management oversight to ensure disaster recovery policies and standards are followed, increase the risk the critical systems supporting the Commissioner's service and enforcement priorities cannot be timely recovered if a disaster occurs.

Recommendations

To ensure the Commissioner's service and enforcement priorities can be met, the CIO should:

1. Report a disaster recovery program material weakness to the Department of the Treasury as part of the IRS' FMFIA annual evaluation of controls and include the following activities (new and currently underway) in the corrective action plan:

   - Obtaining MITS and MA organization and business unit executive support for the establishment of BRS and DRS effort due dates and the monitoring and reporting of the progress and status of the efforts.
   - Completing the BRS and DRS efforts and identifying the MITS organization disaster recovery requirements (including Modernization requirements).
   - Conducting a gap analysis to identify the difference between the MITS organization disaster recovery requirements and current capabilities.
   - Coordinating with IRS, Department of the Treasury, and OMB management to obtain the resources needed to correct the material weakness.

Management's Response: IRS management will declare the disaster recovery program a material weakness. IRS management responded the IRS could recover all vital data for the most mission critical information technology systems, including the Master File and the Customer

Account Data Engine (CADE).[16] They are committed to increasing their disaster recovery capabilities based on available funding and an evaluation of cost and risk factors.

The MA organization is responsible for coordinating the development of an IRS-wide business resumption strategy. The MITS organization has identified its current disaster recovery and business resumption strategies, including both data recovery point and recovery time objectives, for all major systems. A listing of the crucial business processes required to continue fulfilling IRS tax administration responsibilities has been identified and prioritized. Further analysis of this prioritization will include mapping the critical business processes to the specific computing system major applications and general supporting systems that directly support those IRS critical business processes, along with conducting a gap analysis to identify inadequate disaster recovery capabilities. In addition, IRS management will coordinate with the Department of the Treasury and the OMB to request the funding needed to support the business resumption and disaster recovery requirements.

2. Work with the Chief, MA, to implement FISMA POA&M procedures to analyze system weaknesses for systemic problems and elevate them as program-level weaknesses.

Management's Response: IRS senior leadership established an executive working group to identify roles and responsibilities and to provide the leadership and guidance needed to implement FISMA POA&M procedures.

[16] The CADE is the foundation for managing taxpayer accounts in the IRS modernization plan. The CADE will consist of databases and related applications to replace the IRS' existing Master File processing systems.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to provide an overall assessment of the Internal Revenue Service's (IRS) disaster recovery program. To accomplish this objective, we:

I. Reviewed guidance documents and interviewed Modernization and Information Technology Services (MITS) and Mission Assurance (MA) organization management officials to determine whether policies and procedures clearly defined the responsibilities for ensuring the disaster recovery program is effective.

   A. Reviewed Office of Management and Budget, Department of the Treasury, and IRS policies and procedures documents and prior Treasury Inspector General for Tax Administration (TIGTA) audits to document IRS management's disaster recovery program management and oversight roles and responsibilities.

   B. Interviewed MITS and MA organization managers about their disaster recovery oversight roles and responsibilities and determined whether the roles and responsibilities were clearly defined and effectively performed.

II. Reviewed 11 previously issued TIGTA audit reports on the IRS' disaster recovery program activities after the terrorist attacks on September 11, 2001, and the status of management's corrective actions to identify trends in the findings and recommendations.

   A. Reviewed 11 TIGTA audit reports and the Joint Audit Management Enterprise System Corrective Action Form status reports for 44 recommendations as of September 4, 2004, to identify trends.

      1. For the audits listed in Appendix IV, prepared a schedule containing the findings, recommendations, management responses and original due dates, and status of the corrective actions, including revised due dates and status descriptions.

      2. Evaluated the schedule prepared in Step II.A.1. to identify trends.

   B. Reviewed the trends identified in Step II.A.2. to determine whether corrective actions implemented on earlier recommendations were not effective and had an impact on later findings.

III. Determined the higher-level cause(s) for identified trends.

   A. Interviewed MITS and MA organization managers to obtain their explanations for the trends and determined whether other factors resulted in the corrective actions not being effective or implemented.

B. Reviewed documentation supporting the managers' explanations of other factors that resulted in the corrective actions not being effective or implemented and determined the causes of these factors.

Appendix II

Major Contributors to This Report

Margaret E. Begg**,** Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Danny Verneuille, Audit Manager
Frank Greene, Lead Auditor
Michael Garcia, Senior Auditor
Kim McManis, Auditor

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, Information Technology Services OS:CIO:I
Acting Director, Assurance Programs OS:MA:AP
Director, Operational Assurance OS:MA:O
Director, Stakeholder Management OS:CIO:SM
Director, Enterprise Operations OS:CIO:I:EO
Director, Detroit Computing Center OS:CIO:I:EO:DC
Director, Enterprise Computing Center OS:CIO:I:EO:MC
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 Management Controls OS:CFO:AR:M
Audit Liaisons:
    Chief, Mission Assurance OS:MA
    Associate Chief Information Officer, Information Technology Services OS:CIO:I
    Director, Enterprise Operations OS:CIO:I:EO
    Manager, Program Oversight Office OS:CIO:SM:PO

Appendix IV

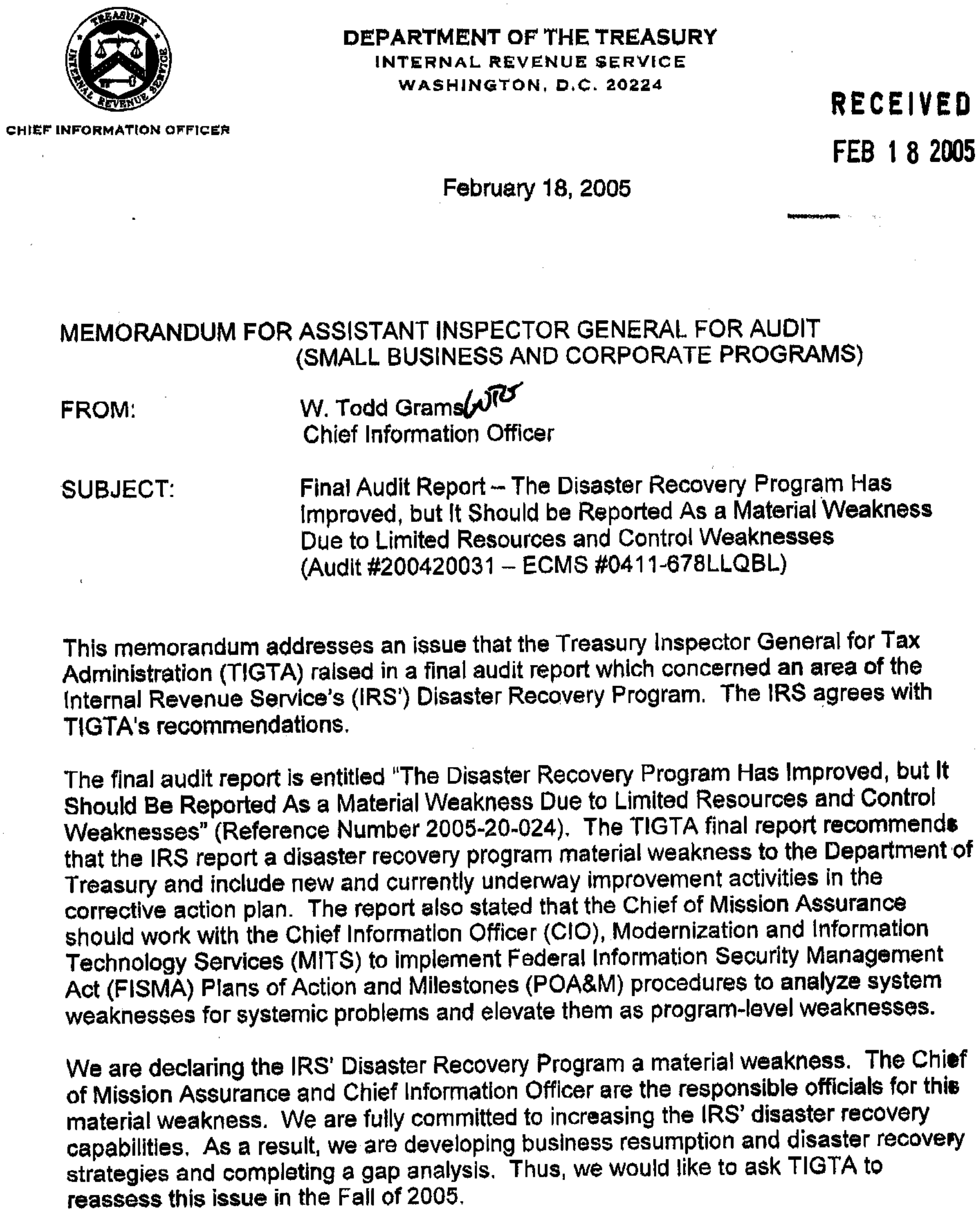
Previously Issued Audit Reports Reviewed

The 11 Treasury Inspector General for Tax Administration Audit Reports reviewed for the overall assessment of the disaster recovery program are:

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).

Appendix V

Management's Response to the Draft Report



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

CHIEF INFORMATION OFFICER

February 18, 2005

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
(SMALL BUSINESS AND CORPORATE PROGRAMS)

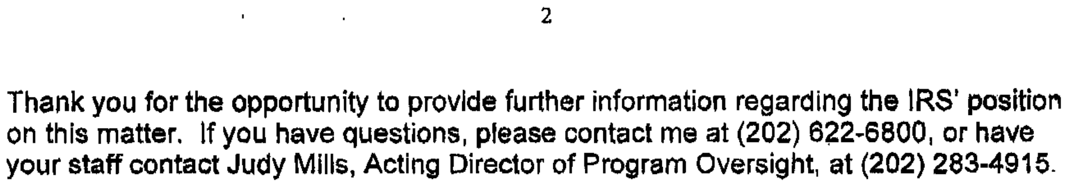
FROM: W. Todd Grams
Chief Information Officer

SUBJECT: Final Audit Report – The Disaster Recovery Program Has Improved, but It Should be Reported As a Material Weakness Due to Limited Resources and Control Weaknesses (Audit #200420031 – ECMS #0411-678LLQBL)

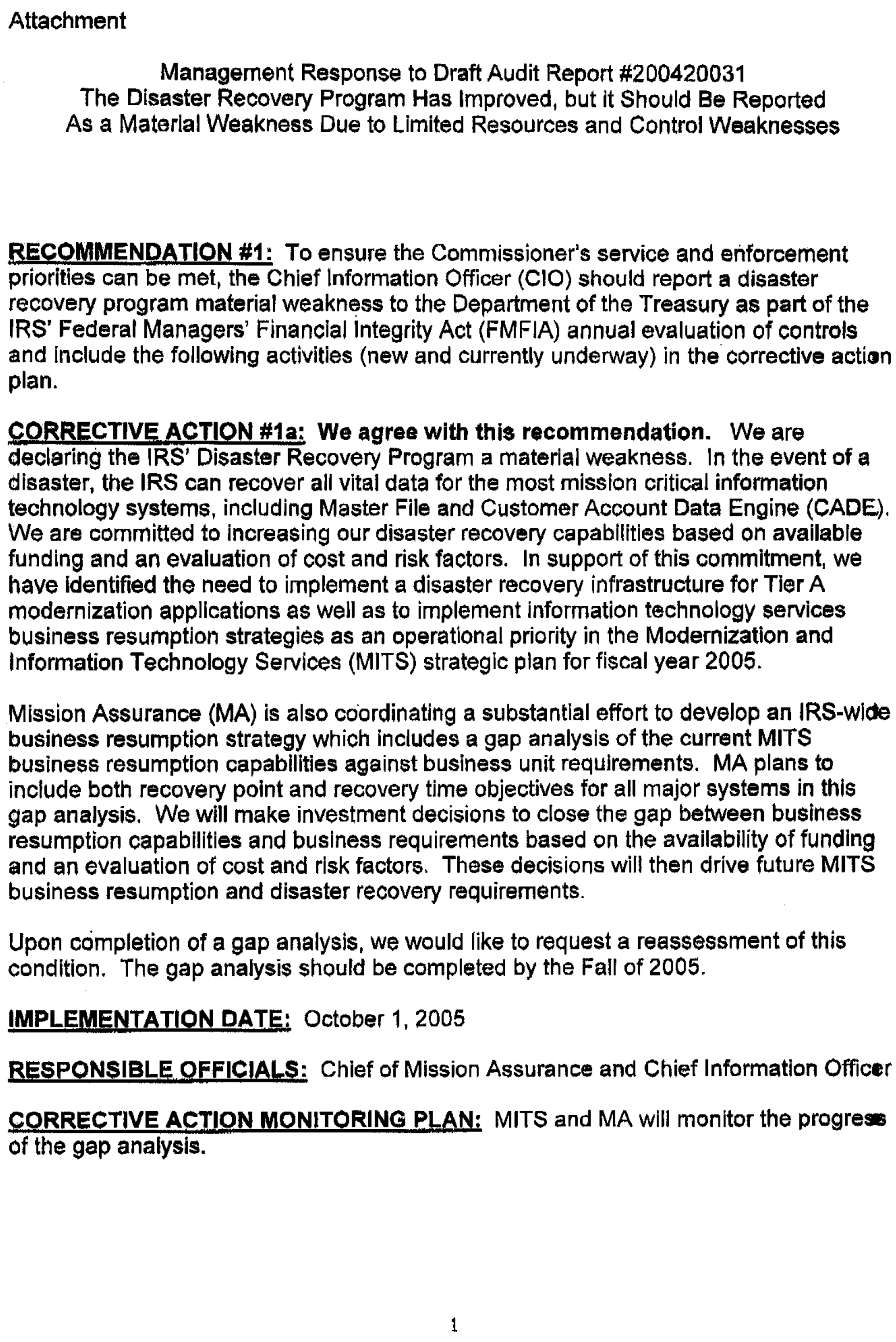
This memorandum addresses an issue that the Treasury Inspector General for Tax Administration (TIGTA) raised in a final audit report which concerned an area of the Internal Revenue Service's (IRS') Disaster Recovery Program. The IRS agrees with TIGTA's recommendations.

The final audit report is entitled "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). The TIGTA final report recommends that the IRS report a disaster recovery program material weakness to the Department of Treasury and include new and currently underway improvement activities in the corrective action plan. The report also stated that the Chief of Mission Assurance should work with the Chief Information Officer (CIO), Modernization and Information Technology Services (MITS) to implement Federal Information Security Management Act (FISMA) Plans of Action and Milestones (POA&M) procedures to analyze system weaknesses for systemic problems and elevate them as program-level weaknesses.

We are declaring the IRS' Disaster Recovery Program a material weakness. The Chief of Mission Assurance and Chief Information Officer are the responsible officials for this material weakness. We are fully committed to increasing the IRS' disaster recovery capabilities. As a result, we are developing business resumption and disaster recovery strategies and completing a gap analysis. Thus, we would like to ask TIGTA to reassess this issue in the Fall of 2005.



Thank you for the opportunity to provide further information regarding the IRS' position on this matter. If you have questions, please contact me at (202) 622-6800, or have your staff contact Judy Mills, Acting Director of Program Oversight, at (202) 283-4915.



Attachment

Management Response to Draft Audit Report #200420031
The Disaster Recovery Program Has Improved, but it Should Be Reported
As a Material Weakness Due to Limited Resources and Control Weaknesses

RECOMMENDATION #1: To ensure the Commissioner's service and enforcement priorities can be met, the Chief Information Officer (CIO) should report a disaster recovery program material weakness to the Department of the Treasury as part of the IRS' Federal Managers' Financial Integrity Act (FMFIA) annual evaluation of controls and include the following activities (new and currently underway) in the corrective action plan.

CORRECTIVE ACTION #1a: **We agree with this recommendation.** We are declaring the IRS' Disaster Recovery Program a material weakness. In the event of a disaster, the IRS can recover all vital data for the most mission critical information technology systems, including Master File and Customer Account Data Engine (CADE). We are committed to increasing our disaster recovery capabilities based on available funding and an evaluation of cost and risk factors. In support of this commitment, we have identified the need to implement a disaster recovery infrastructure for Tier A modernization applications as well as to implement information technology services business resumption strategies as an operational priority in the Modernization and Information Technology Services (MITS) strategic plan for fiscal year 2005.

Mission Assurance (MA) is also coordinating a substantial effort to develop an IRS-wide business resumption strategy which includes a gap analysis of the current MITS business resumption capabilities against business unit requirements. MA plans to include both recovery point and recovery time objectives for all major systems in this gap analysis. We will make investment decisions to close the gap between business resumption capabilities and business requirements based on the availability of funding and an evaluation of cost and risk factors. These decisions will then drive future MITS business resumption and disaster recovery requirements.

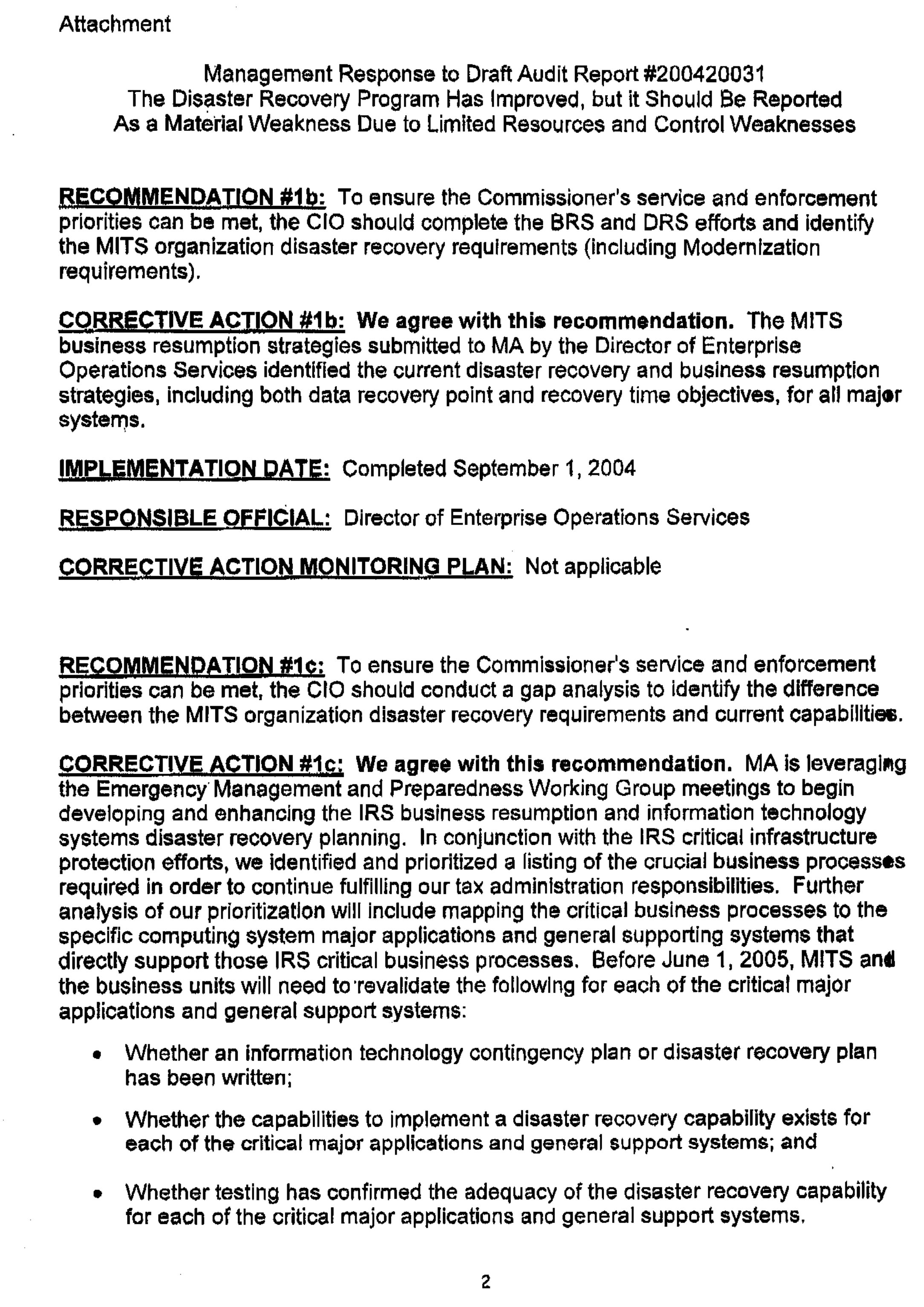
Upon completion of a gap analysis, we would like to request a reassessment of this condition. The gap analysis should be completed by the Fall of 2005.

IMPLEMENTATION DATE: October 1, 2005

RESPONSIBLE OFFICIALS: Chief of Mission Assurance and Chief Information Officer

CORRECTIVE ACTION MONITORING PLAN: MITS and MA will monitor the progress of the gap analysis.

1



Attachment

Management Response to Draft Audit Report #200420031
The Disaster Recovery Program Has Improved, but it Should Be Reported
As a Material Weakness Due to Limited Resources and Control Weaknesses

RECOMMENDATION #1b: To ensure the Commissioner's service and enforcement priorities can be met, the CIO should complete the BRS and DRS efforts and identify the MITS organization disaster recovery requirements (including Modernization requirements).

CORRECTIVE ACTION #1b: **We agree with this recommendation.** The MITS business resumption strategies submitted to MA by the Director of Enterprise Operations Services identified the current disaster recovery and business resumption strategies, including both data recovery point and recovery time objectives, for all major systems.

IMPLEMENTATION DATE: Completed September 1, 2004

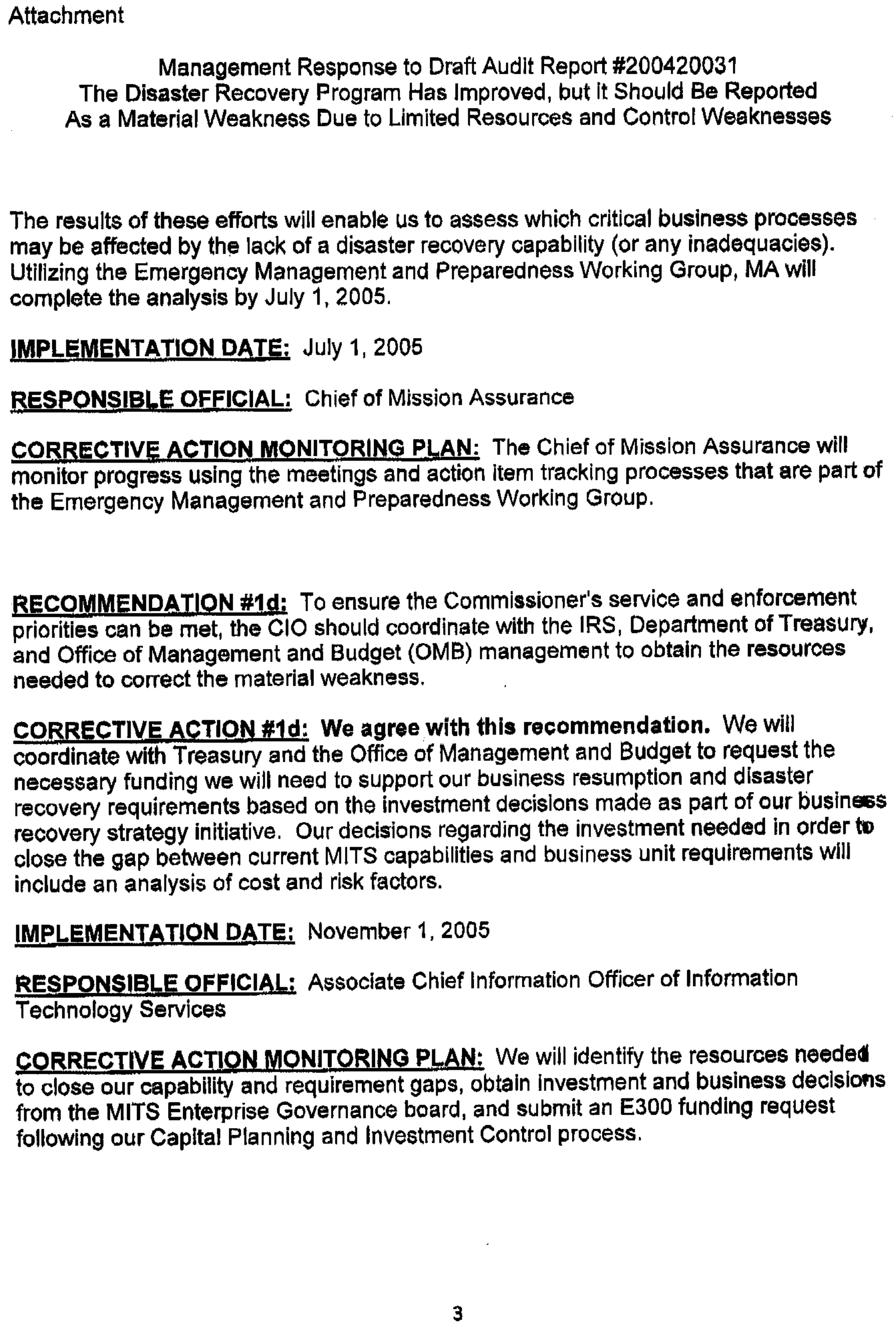
RESPONSIBLE OFFICIAL: Director of Enterprise Operations Services

CORRECTIVE ACTION MONITORING PLAN: Not applicable

RECOMMENDATION #1c: To ensure the Commissioner's service and enforcement priorities can be met, the CIO should conduct a gap analysis to identify the difference between the MITS organization disaster recovery requirements and current capabilities.

CORRECTIVE ACTION #1c: **We agree with this recommendation.** MA is leveraging the Emergency Management and Preparedness Working Group meetings to begin developing and enhancing the IRS business resumption and information technology systems disaster recovery planning. In conjunction with the IRS critical infrastructure protection efforts, we identified and prioritized a listing of the crucial business processes required in order to continue fulfilling our tax administration responsibilities. Further analysis of our prioritization will include mapping the critical business processes to the specific computing system major applications and general supporting systems that directly support those IRS critical business processes. Before June 1, 2005, MITS and the business units will need to revalidate the following for each of the critical major applications and general support systems:

- Whether an information technology contingency plan or disaster recovery plan has been written;
- Whether the capabilities to implement a disaster recovery capability exists for each of the critical major applications and general support systems; and
- Whether testing has confirmed the adequacy of the disaster recovery capability for each of the critical major applications and general support systems.



Attachment

Management Response to Draft Audit Report #200420031
The Disaster Recovery Program Has Improved, but It Should Be Reported
As a Material Weakness Due to Limited Resources and Control Weaknesses

The results of these efforts will enable us to assess which critical business processes may be affected by the lack of a disaster recovery capability (or any inadequacies). Utilizing the Emergency Management and Preparedness Working Group, MA will complete the analysis by July 1, 2005.

IMPLEMENTATION DATE: July 1, 2005

RESPONSIBLE OFFICIAL: Chief of Mission Assurance

CORRECTIVE ACTION MONITORING PLAN: The Chief of Mission Assurance will monitor progress using the meetings and action item tracking processes that are part of the Emergency Management and Preparedness Working Group.

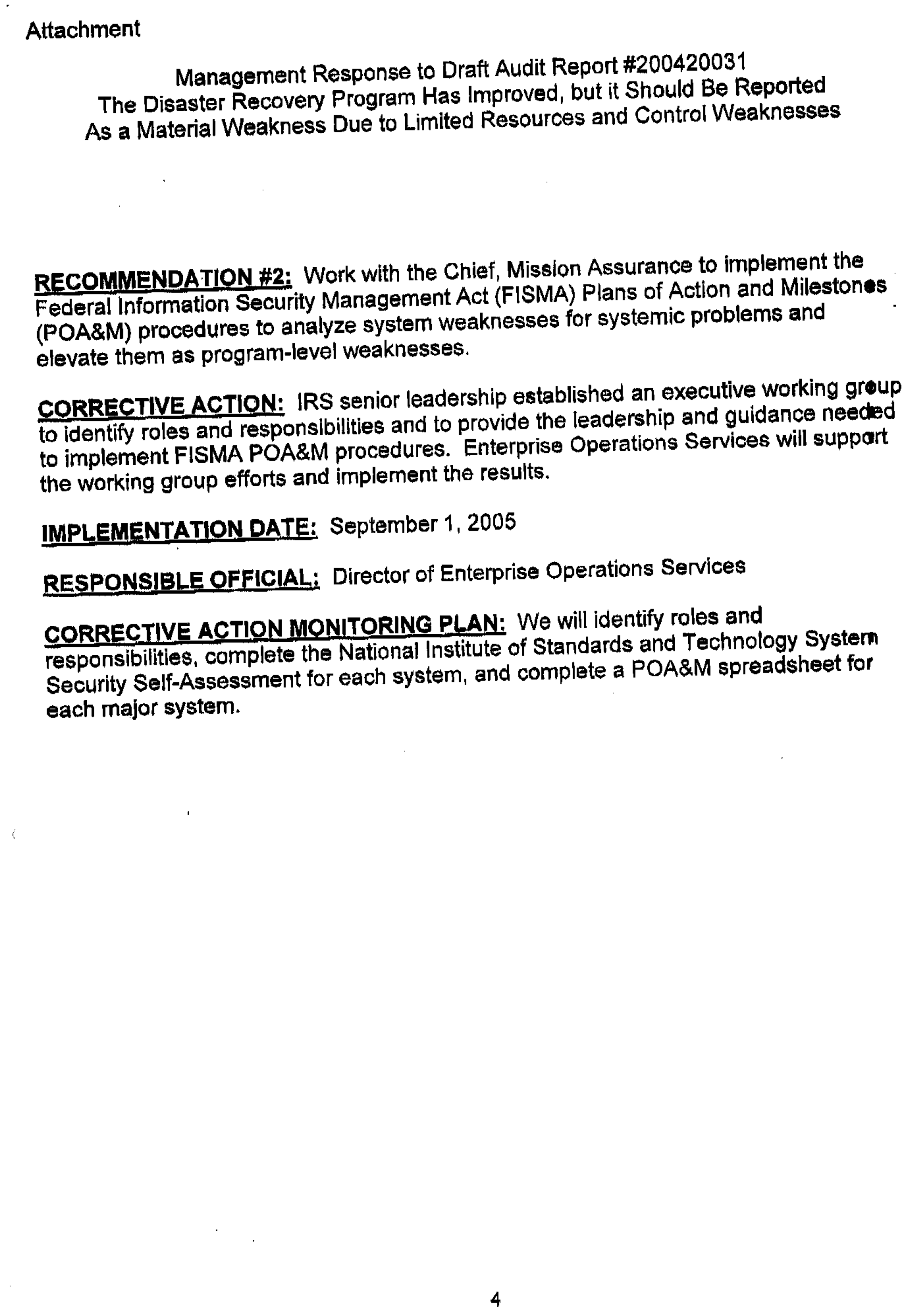
RECOMMENDATION #1d: To ensure the Commissioner's service and enforcement priorities can be met, the CIO should coordinate with the IRS, Department of Treasury, and Office of Management and Budget (OMB) management to obtain the resources needed to correct the material weakness.

CORRECTIVE ACTION #1d: **We agree with this recommendation.** We will coordinate with Treasury and the Office of Management and Budget to request the necessary funding we will need to support our business resumption and disaster recovery requirements based on the investment decisions made as part of our business recovery strategy initiative. Our decisions regarding the investment needed in order to close the gap between current MITS capabilities and business unit requirements will include an analysis of cost and risk factors.

IMPLEMENTATION DATE: November 1, 2005

RESPONSIBLE OFFICIAL: Associate Chief Information Officer of Information Technology Services

CORRECTIVE ACTION MONITORING PLAN: We will identify the resources needed to close our capability and requirement gaps, obtain investment and business decisions from the MITS Enterprise Governance board, and submit an E300 funding request following our Capital Planning and Investment Control process.



Attachment

Management Response to Draft Audit Report #200420031
The Disaster Recovery Program Has Improved, but it Should Be Reported
As a Material Weakness Due to Limited Resources and Control Weaknesses

RECOMMENDATION #2: Work with the Chief, Mission Assurance to implement the Federal Information Security Management Act (FISMA) Plans of Action and Milestones (POA&M) procedures to analyze system weaknesses for systemic problems and elevate them as program-level weaknesses.

CORRECTIVE ACTION: IRS senior leadership established an executive working group to identify roles and responsibilities and to provide the leadership and guidance needed to implement FISMA POA&M procedures. Enterprise Operations Services will support the working group efforts and implement the results.

IMPLEMENTATION DATE: September 1, 2005

RESPONSIBLE OFFICIAL: Director of Enterprise Operations Services

CORRECTIVE ACTION MONITORING PLAN: We will identify roles and responsibilities, complete the National Institute of Standards and Technology System Security Self-Assessment for each system, and complete a POA&M spreadsheet for each major system.

4