TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Better Emergency Preparedness Planning Could Improve Business Continuity Efforts

February 13, 2009

Reference Number: 2009-20-038

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

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

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

February 13, 2009

MEMORANDUM FOR COMMISSIONER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Better Emergency Preparedness Planning Could Improve Business Continuity Efforts (Audit # 200820029)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) business continuity program ensures that employees can be protected and critical business processes and computer systems can be efficiently recovered during and after a disaster or emergency incident. We recently completed three separate reviews related to the business continuity program. The Government Accountability Office has also performed a recent review of IRS emergency planning.[1] This report presents our overall assessment of the IRS business continuity program based on those reviews. This audit was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of an overall strategy to evaluate the adequacy and viability of the suite of emergency plans[2] the IRS has in place.

Impact on the Taxpayer

The IRS' ability to protect its employees and provide service to taxpayers during and after a major disruption is dependent on the effective preparation of four integrated plans called the Business Continuity "Suite of Plans." However, many of the plans we reviewed were not up to date, have not been adequately tested, and did not contain sufficient detail to be effective. The deficiencies in the plans could affect the IRS' ability to process 235 million tax returns, issue $295 billion in refunds, and collect $2.7 trillion in revenue each year.

[1] See reports listed in Appendix IV.

[2] The occupant emergency plan, the incident management plan, the business resumption plan, and the disaster recovery plan.

Synopsis

Redundant operations and experience with major disasters have strengthened the IRS business continuity program. Each critical process is carried out at multiple locations, allowing the IRS to take advantage of its experienced workforce and similarly situated facilities to recover from a disaster. Although many employees responsible for executing the business continuity plans are cognizant of the strategies that they would follow to recover operations, these key employees might not be available after a disaster. Therefore, the IRS needs to be proactive and conduct thorough, upfront planning to protect its employees and to efficiently recover critical business processes and systems.

Many of the business continuity plans lacked key details. Our review of 39 incident management plans and 65 business resumption plans determined that the majority of the plans were incomplete and did not provide assurance that the IRS could efficiently respond to the full range of potential disasters or emergency incidents. Key details missing in the plans included 1) the location of the Emergency Operations Center where the incident management team would meet to begin addressing the emergency, and 2) procedures for recovering critical processes. We also found instances of incomplete and inaccurate disaster recovery plans for several major tax processing systems.

Business continuity plans were not routinely tested or were informally tested using tabletop exercises during which participants met and discussed the procedures they would follow. Lessons learned from testing disaster recovery plans were not always documented. When the lessons learned were documented, subsequent testing did not ensure that the weaknesses were retested to determine whether the plan weaknesses had been corrected. Comprehensive testing is needed to identify the gaps and weaknesses in the plans.

The absence of detailed planning information and inadequate testing are due to a lack of cross-functional coordination, leadership, and effective monitoring and oversight. Business continuity planning and testing require the involvement of many employees in virtually every IRS business unit, which increases the risk of insufficient planning and testing. Accountability for carrying out those plans is difficult to enforce across the organization, and the interdependence of the plans requires coordination to ensure that the plans are synchronized.

Recommendations

In our prior reports, we made recommendations to improve the development and testing of the specific business continuity plans. When those plans are viewed together, however, it is clear that cross-functional coordination, leadership, and effective monitoring and oversight are needed to ensure the effectiveness of the IRS business continuity efforts.

We recommended that the IRS Commissioner appoint an executive with cross-organizational authority to oversee the IRS business continuity program. The executive should serve as the chairperson of the Emergency Management and Preparedness Executive Steering Committee. This Committee is responsible for overseeing the business continuity plans. We also recommended that the IRS Commissioner require the newly appointed executive to monitor and ensure that comprehensive testing is conducted and documented for all four business continuity plans, ensure that weaknesses and gaps identified during testing are corrected and retested, and consider testing plans concurrently as opposed to testing the plans separately.

Response

IRS management agreed with the recommendations. The Emergency Management and Preparedness Executive Steering Committee is now chaired by the Chief, Agency-Wide Shared Services, who will direct and execute the cross-functional IRS-wide emergency management program. An executive has been appointed to lead the Physical Security and Emergency Preparedness Continuity Operations staff and focus exclusively on the oversight and enforcement of the continuity planning program. Lastly, the IRS will develop a Test and Exercise Program that requires integrated exercises of all four business continuity plans. The Program will require that exercises be scheduled and conducted with after-action reports and improvement plans completed and documented. Management's complete response to the draft report is included as Appendix V.

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, Acting Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.

Table of Contents

Appendices

Abbreviations

GAO	Government Accountability Office
IRS	Internal Revenue Service
PSEP	Physical Security and Emergency Preparedness

Background

Homeland Security Presidential Directive-20[1] requires that Federal Government agencies develop business continuity plans to enable the recovery of critical functions after a disaster or emergency. To comply with the Directive, the Internal Revenue Service (IRS) must develop and continually update its business continuity plans to protect employees and recover critical business processes, data, and information technology systems. Achieving continuity of operations in an organization as large as the IRS is challenging due to the wide range of incidents that could occur, such as acts of nature, power outages, and terrorist attacks. The IRS must protect more than 100,000 employees and contractors in more than 660 facilities located throughout the nation.

The difficult planning that must be accomplished to continue IRS processes after a disaster is warranted by the national and economic risks. A prolonged disruption could affect critical tax administration processes such as collecting taxes and processing tax returns and refunds. In Fiscal Year 2007, the IRS processed more than 235 million tax returns, collected almost $2.7 trillion in revenue, and issued 117 million refunds totaling $295 billion. Business continuity planning enables the IRS to have the ability to continue these critical business processes by providing a collection of strategies and plans that ensure that the IRS can efficiently recover critical processes and systems during and/or after a disaster.

In an emergency, the IRS would execute one or more of the following business continuity plans depending on the nature and severity of the incident:

1. <u>Occupant emergency plan</u> – This plan protects IRS employees and visitors in IRS facilities. It provides instructions needed to safely evacuate people from a facility or shelter them in place. This plan is the most significant because it protects lives. In addition, some business continuity experts have concluded that if they can protect their employees, they can eventually recover their business.

2. <u>Incident management plan</u> – This plan addresses the overall command structure that would be implemented in the event of an emergency. The focus of the command team is assessment, evaluation, coordination, and strategy development as events occur.

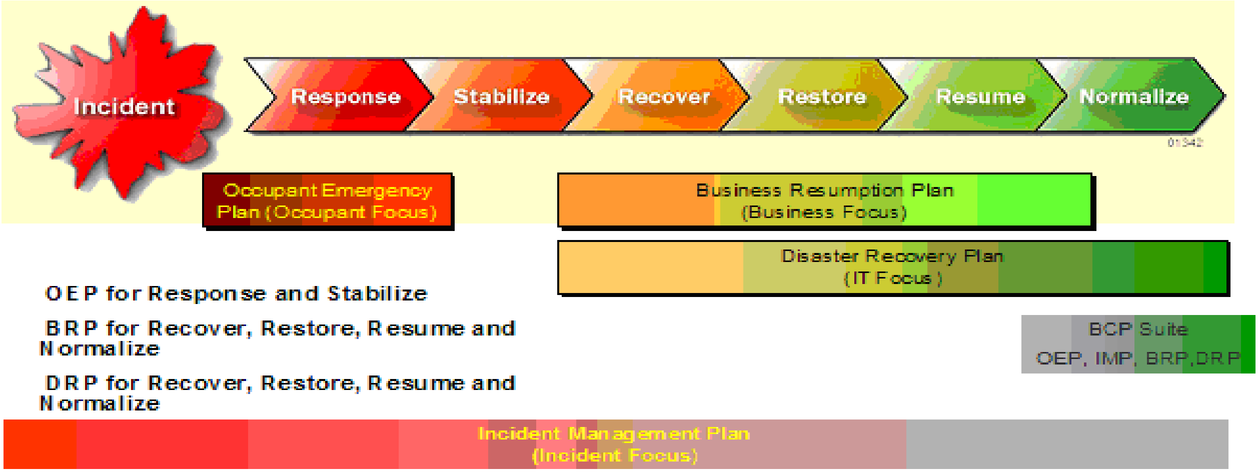
3. <u>Business resumption plan</u> – This plan is used to recover and restore disrupted business processes in affected facilities. It identifies business processes, resumption strategies, people, vital records, information technology systems, and other supporting assets.

[1] *National Continuity Policy*, dated May 4, 2007 (also known as National Security Presidential Directive-51). This Directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations.

4. Disaster recovery plan – This plan is used to recover and restore disrupted information technology systems and data. It identifies systems, procedures for recovering them, and the process for restoring operations at an alternate site.

These four plans, called the Business Continuity "Suite of Plans," are used to prepare for, respond to, and recover from a disaster or emergency incident. The relationship among the four plans is represented in Figure 1.

Figure 1: Relationship Among IRS Business Continuity Plans


Incident
Response
Stabilize
Recover
Restore
Resume
Normalize
01342
Occupant Emergency Plan (Occupant Focus)
Business Resumption Plan (Business Focus)
Disaster Recovery Plan (IT Focus)
OEP for Response and Stabilize
BRP for Recover, Restore, Resume and Normalize
DRP for Recover, Restore, Resume and Normalize
BCP Suite
OEP, IMP, BRP,DRP
Incident Management Plan (Incident Focus)

Source: The IRS Agency-Wide Shared Services organization. IT = Information Technology. BCP = Business Continuity Program. OEP = Occupant Emergency Plan. IMP = Incident Management Plan. BRP = Business Resumption Plan. DRP = Disaster Recovery Plan.

We recently completed reviews of each of these plans in three separate audits. The Government Accountability Office (GAO) has also performed a recent review of IRS emergency planning. The recommendations and IRS management responses in the reports for these four audits were focused on the development and testing of the specific business continuity plans.[2]

This report is a compilation of our review of the four prior audit reports. We performed this review at the Treasury Inspector General for Tax Administration office in Dallas, Texas, during the period May through October 2008. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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.

[2] See report titles and summary information in Appendix IV.

Results of Review

Redundant Operations and Experience With Major Disasters Have Strengthened the Business Continuity Program

The IRS' ability to recover its critical processes is strengthened by its extensive redundant operations located in various functions throughout the nation. Each critical process is carried out at multiple locations, allowing the IRS to take advantage of its experienced workforce and similarly situated facilities where work could be redirected. The IRS should also be able to benefit from its experience in recovering from previous disasters and emergency incidents. For example:

- On June 25, 2006, the IRS National Headquarters building flooded during a period of record rainfall and sustained extensive damage to its infrastructure. IRS officials reported activating several of the agency's emergency operations plans. The GAO review of IRS recovery efforts showed that while the IRS plans helped guide its response to the flood, in more severe emergency events, conditions could be less favorable to recovery.[3]

- Hurricane Katrina made landfall on August 29, 2005. It caused unprecedented damage to New Orleans, Louisiana, as well as the coastal areas of Mississippi and Alabama. Hurricane Rita followed less than 1 month later and further damaged New Orleans and the Gulf Coast area of Texas. The IRS had 25 offices affected by the Hurricanes, many of which were closed for short durations due to sustained power outages. Five offices received significant damage, which forced closure for longer periods of time. By taking aggressive actions after the storms, the IRS was able to relocate its employees and restore its operations.

- In 2001 and 2002, a number of government offices received mail or packages that seemed to contain the anthrax virus. While no IRS facility received mail that actually contained anthrax, mail-handling procedures were upgraded to address this possibility. For example, mail rooms in all facilities were isolated, self-contained ventilation systems were installed at all campus[4] mail rooms so that the rooms could be shut off from the remainder of the facilities, and hazardous material training and protective equipment were provided to pertinent employees.

[3] See report listed in Appendix IV.
[4] Campuses are 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.

Cross-functional Coordination Is Needed to Improve Business Continuity Planning and Testing

Planning efforts have not been sufficient to ensure efficient recovery from an emergency

While the IRS' redundant operations and experiences with disasters should enable it to recover its critical processes, complete and adequate business continuity plans are needed to ensure that the recovery is as quick and efficient as possible. Based on our prior audits, we concluded that the IRS occupant emergency plans have been more thoroughly developed than the other business continuity plans. We reviewed occupant emergency plans for 15 facilities in which the IRS was the primary tenant and, therefore, was responsible for preparing the plans. The plans were current and adequately identified the key personnel, including the alternates responsible for the facilities' evacuation in the event of an emergency. The plans also contained facility-specific emergency contact information and a general description of the facility characteristics.

Although occupant emergency plans contained detailed planning information, the IRS' other business continuity planning efforts have not been sufficient to ensure that critical business processes and systems are efficiently restored in the event of a disaster. We found a majority of the incident management, business resumption, and disaster recovery plans lacked detailed planning information and recovery strategies. The GAO also found gaps in the incident management plans and business resumption plans.[5] It reported that IRS business continuity plans do not provide assurance that the IRS could respond to the full range of potential disruptions.

Missing planning information could result in confusion, duplication of efforts, and a breakdown in communication if IRS staff relied on the plans. In an emergency incident, such as a terrorist attack or natural disaster, we believe that these deficiencies could result in delays in recovering critical business processes.

Incident management plans

The purpose of an incident management plan is to designate, in advance, the specific personnel and command structure to be activated in the event of an incident such as a hurricane, flood, or terrorist act. A critical component of this process is the establishment of an Emergency Operations Center where the incident management team will meet to begin addressing the emergency. The focus of this team is assessment, evaluation, coordination, and strategy development as events occur.

[5] See report listed in Appendix IV. The GAO reviewed the incident management plan for the IRS Headquarters Office in Washington, D.C. This building houses more than 2,200 of the IRS' estimated 104,000 employees. The GAO also reviewed the business resumption plans for the Wage and Investment Division, the Criminal Investigation Division, and the Office of Chief Counsel.

Our review of the incident management plans for 39 randomly selected facilities determined that the plans did not always include the information necessary to effectively respond to emergencies. Specifically:

- The locations of the primary Emergency Operations Center and/or the backup facility were not identified in 28 (72 percent) of the plans we evaluated.
- An alternate to the Incident Commander,[6] in the event he or she is unavailable, was not identified in 16 (41 percent) of the plans we evaluated. In addition, a backup for one or more other key incident management team personnel was not identified in 32 (82 percent) of the plans.
- An Initial Incident Commander, who would manage the response to an emergency until the Incident Commander could take over, was not identified in 12 (34 percent) of the 35 facilities we sampled where the Incident Commander was not physically located in the building. For example, at one site we reviewed, the Incident Commander was located more than 200 miles from the facility.
- A general description of the nature of the IRS business functions located at the site and complete and current contact information for the applicable functional Business Resumption Coordinators were not included in 33 (85 percent) of the plans we evaluated.
- Key elements of the incident management plan for the IRS Headquarters office were not addressed or were addressed only in part. For example, the GAO noted that although the plan listed the critical business processes in priority order, it did not establish recovery time objectives for the critical processes.

Business resumption plans

A business resumption plan should include the advance planning and preparations necessary to minimize loss and ensure the continuity of critical business processes. The pre-determined set of instructions and procedures that describe how business processes will be restored should be documented in the plan. A complete business resumption plan should include details such as a list and description of critical business processes that are conducted by the business function at the site; procedures for recovering each of the critical processes and sub-processes; other locations that perform the same business processes as those performed at the site covered by the plan; vital records needed by employees to perform their duties; and the amount of space, furniture, and other needs (e.g., copiers, printers, and fax machines).

[6] In general, the area Senior Commissioner Representative is the Incident Commander for the IRS field offices. The IRS has 15 Senior Commissioner Representatives located throughout the nation.

Most of the business resumption plans we evaluated were not adequately completed and would not facilitate the efficient recovery of critical IRS business processes. Our review of 65 business resumption plans determined that the plans did not:

- Include procedures for recovering each of the critical processes and sub-processes described in the business resumption plan – 16 plans (25 percent).
- Document other locations that perform the same critical business processes and sub-processes as those performed at the site covered by the plan – 43 plans (66 percent).
- Identify the vital records needed by the employees to perform their duties – 13 plans (20 percent). Some business resumption team leaders informed us that they had no vital records. Others stated that their vital records were electronic and accessible through the IRS network. However, the business resumption plans did not document these key details and recovery strategies.
- Document the amount of space, furniture, and equipment (e.g., copiers, printers, and fax machines) that would be required at the alternate facility – 25 plans (38 percent).

Disaster recovery plans

A disaster recovery plan should define the detailed tasks needed to recover the information technology systems, including the network, hardware, and software applications. The employees who restore the systems should be able to follow the detailed tasks in the plan exactly as they are written. This is important because the employees with the institutional knowledge of how to restore the systems might not be available after a disaster.

The IRS has more than 240 systems, each of which is owned by a business unit or the Modernization and Information Technology Services organization. Responsibility for maintaining a disaster recovery plan lies with the system owner. However, we determined that the system owners have not included sufficient details in their disaster recovery plans and have not kept the plans updated.

In a March 2004 audit,[7] we determined that the Master File[8] Disaster Recovery Plan was not detailed enough to be used verbatim to react to a worst-case scenario. We also found that the Plan was not reviewed quarterly and updated as needed. The Chief Information Officer agreed with our findings and, in December 2004, reported that corrective actions had been taken to address these weaknesses. However, our followup review[9] in February 2008 found the same weaknesses.

[7] *The Master File Disaster Recovery Exercise Was Completed, but Significant Vulnerabilities Should Be Addressed* (Reference Number 2004-20-053, dated March 2004).

[8] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.

[9] See Report 1 in Appendix IV.

Our followup review determined that quarterly reviews of the Master File Disaster Recovery Plan were not performed. In addition, while our observation of the Master File disaster recovery test determined that test participants were using the Master File Disaster Recovery Plan, our observation of one other mainframe disaster recovery test determined that recovery site personnel used a combination of the Disaster Recovery Exercise Plan (because a disaster recovery plan was not available) and individual reference materials they had brought to the exercise to recover the system(s).

In addition, our followup review determined that the disaster recovery plans of several significant tax processing systems were not updated in a timely manner. The five-volume disaster recovery plan for the Service Center Mainframe Consolidation was dated in 2006, with two of the volumes dated as early as March 2006; the disaster recovery plan for a major tax processing system was dated September 2004; and one disaster recovery document (previously shown to be named a Technical Contingency Planning Document) was dated December 6, 2001.

Business continuity plans were not routinely tested

Homeland Security Presidential Directive-20 requires Federal Government agencies to conduct annual tests of business continuity plans. To comply with this Directive and other directives from the Department of Homeland Security,[10] the Physical Security and Emergency Preparedness (PSEP) office provided testing guidance to the IRS business functions. Testing is critical to ensure the viability of the business continuity plans. In many ways, testing validates the recovery strategies, assumptions, and procedures against likely disasters or emergency events. The gaps and weaknesses in the various plans should be identified and corrected during comprehensive testing. Plans that are not tested might prevent the IRS from efficiently recovering its critical processes and systems.

Generally, five types of tests can be conducted to assess business continuity plans:[11]

Informal Testing:

1. Checklist test – This test involves reviewing the plan for content, completeness, and adherence to criteria.
2. Tabletop test – The participants in the testing exercise meet and verbally describe what activities, procedures, and tasks they would follow.

[10] Homeland Security Presidential Directive-5, *Management of Domestic Incidents*; Homeland Security Presidential Directive-7, *Critical Infrastructure Identification, Prioritization, and Protection*; and Homeland Security Presidential Directive-8, *National Preparedness*.
[11] Akhtar Syed and Afsar Syed, *Business Continuity Planning Methodology* (Mississauga, Ontario, Canada: Sentryx, 2004), 203-213.

Comprehensive Testing:

3. Parallel test – This type of test evaluates the recovery of processes at alternate sites without disrupting operations at the normal work site.
4. Simulation test – This test is a combination of simulations and actual operations transfers and might require some units to cease operations for the test period.
5. Full-interruption test – The organization activates all components of the business resumption plan.

During our fieldwork, we noted some improvements in the testing of occupant emergency plans. The PSEP office initiated new procedures to improve training exercises. An emergency evacuation checklist was developed to document the results of evacuation tests conducted after August 1, 2008. The checklist will be used to document issues such as whether employees quickly exited the building, alarms worked properly, evacuation team members knew their roles, and employees reported to their assigned assembly areas. The overall process for monitoring evacuation tests is also being improved by better defining roles and responsibilities at each level of involvement and by developing a methodology to track completion of the tests. These new procedures are scheduled to take effect during the first quarter of Fiscal Year 2009.

During our reviews, we found that many of the business continuity plans were not tested. For the plans that were tested, the scope of testing usually consisted of a tabletop exercise. Specifically:

- Occupant evacuation testing was not performed in Calendar Year 2007 in 5 (33 percent) of 15 buildings we evaluated. Where emergency testing was performed, key test results, such as whether employees were evacuated in a timely manner, disabled employees were properly evacuated, employees properly reported to their assigned assembly areas, and alarms functioned properly, were generally not recorded. In an emergency, a properly tested occupant emergency plan can reduce threats to the safety of IRS employees.
- An incident management plan exercise was not performed during either Fiscal Year 2006 or Fiscal Year 2007 at 3 (50 percent) of 6 IRS facilities with 250 or more employees that we evaluated. The three facilities where an exercise was not performed included two large field offices and a Computing Center.[12] We also found that where exercises were performed, detailed documentation regarding the test scope, deficiencies identified, and actions taken to address those deficiencies was not maintained in two of the three sites. As a result, the benefit of information accrued from these tests is not available to assist the IRS in its efforts to improve its incident readiness.

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

- The IRS business units had not tested 35 (54 percent) of the 65 business resumption plans during Calendar Year 2007. For the 30 plans that were tested, the scopes of the tests consisted of tabletop exercises. Participants, such as a Senior Commissioner Representative, a site coordinator, and a business resumption team leader, met and discussed how they would handle various emergencies or disasters. This type of testing is insufficient to identify gaps, omissions, and weaknesses in the plans. In addition, the results and weaknesses identified during the tests were not documented.
- The lessons learned from testing disaster recovery plans were not always documented. When the lessons learned were documented, subsequent testing did not ensure that the weaknesses were retested to determine whether the plan weaknesses had been corrected.

Management Action: Subsequent to completion of our audit fieldwork, the IRS advised us that lessons learned from disaster recovery tests are now being documented and weaknesses identified in previous testing are now being retested in subsequent test exercises. The IRS also informed us that it had updated its procedures for retesting vulnerabilities identified in previous testing. We plan to follow up on these corrective actions in future reviews.

In our prior reports, we made recommendations to improve the development and testing of the specific business continuity plans. When those plans are viewed together, however, it is clear that cross-functional coordination, leadership, and effective monitoring and oversight are needed to ensure the effectiveness of the IRS business continuity efforts.

First, the numbers of persons and organizations involved in these efforts increase the risk that planning and testing will not be adequate. While the PSEP office is responsible for providing guidance regarding occupant emergency, incident management, and business resumption plans, the guidance must be used in preparing and testing the plans by all IRS business functions, and the guidance must address employee safety and critical business processes that are carried out in more than 660 facilities. The Modernization and Information Technology Services organization is responsible for developing and testing disaster recovery plans.

Second, accountability for carrying out business continuity responsibilities is difficult to enforce across organizational lines. For example, the PSEP office provided a comprehensive template for planning and completing a business resumption plan. However, our prior review of these plans determined that 12 different templates were used by the 8 IRS business functions that we evaluated. Some functions used different templates within their own organizations. Conflicting priorities and budget concerns in the business functions contributed to noncompliance with the PSEP guidance, as did a lack of emphasis on testing. The PSEP office did not enforce its guidance across organizational lines. Also, the Emergency Management and Preparedness Executive Steering Committee, which consists of executives from several business units and is responsible for overseeing the business continuity plans, has not taken an active role in coordinating business continuity efforts. As of July 2008, this Committee had met only once since its inception in August 2005. The lack of regular meetings by the Emergency Management and Preparedness Executive Steering Committee was reported in our audit of the IRS business resumption plans.

Finally, the business continuity plans are interrelated. For example, business processes cannot be resumed without computer systems that support those processes. Consequently, business resumption plans must be synchronized with disaster recovery plans.

Management Actions: Subsequent to completion of our audit fieldwork, the IRS advised us that the PSEP office has augmented the program by assigning to the emergency management staff an executive whose sole focus is to oversee and enforce the business continuity requirements. However, we believe that the IRS Commissioner should appoint an executive with cross-organizational authority to oversee the business continuity program. In addition, on November 25, 2008, after completion of our fieldwork on this audit and 3 months after we completed our fieldwork for the audit of business resumption plans, the IRS provided several documents related to Emergency Management and Preparedness Executive Steering Committee meetings. However, due to the IRS' untimely submission of these documents, we were unable to review them.

Recommendations

Recommendation 1: To ensure that compliance with business continuity guidance is enforced across organizational lines and because of the interrelationships among business continuity plans, the IRS Commissioner should appoint an executive with cross-organizational authority to oversee the IRS business continuity program. The executive should serve as the chairperson of the Emergency Management and Preparedness Executive Steering Committee.

> ***Management's Response:*** The IRS agreed with this recommendation. The Emergency Management and Preparedness Executive Steering Committee is now chaired by the Chief, Agency-Wide Shared Services, who will direct and execute the cross-functional IRS-wide emergency management program. An executive has been appointed to lead the PSEP Continuity Operations staff and focus exclusively on the oversight and enforcement of the continuity planning program.

Recommendation 2: The IRS Commissioner should require the executive responsible for business continuity planning to monitor and ensure that comprehensive testing is conducted and documented for all four business continuity plans. The testing should ensure that weaknesses and gaps identified during testing are corrected and retested during subsequent test exercises. Because guidance for complete recovery can be found in multiple plans, consideration should be given to testing plans concurrently as opposed to testing the plans separately.

> ***Management's Response:*** The IRS agreed with this recommendation. A Test and Exercise Program is being developed that will require integrated exercises of all four business continuity plans. The Program will require that exercises be scheduled and

conducted, with after-action reports and improvement plans completed and documented. A copy of the exercise schedules and after-action reports and improvement plans will be forwarded to the PSEP Continuity Operations Program Office for review of lessons learned, trend analysis, and best practices.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS business continuity program ensures that employees can be protected and critical business processes and computer systems can be efficiently recovered during and after a disaster or emergency incident. The IRS uses a combination of four integrated plans called the Business Continuity "Suite of Plans" to prepare for, respond to, and recover from an incident or emergency. These plans include the occupant management plan, incident management plan, business resumption plan, and disaster recovery plan. We have previously conducted reviews of the business continuity plans in three separate audits. The GAO has also performed a recent review of IRS emergency planning.[1] This report presents our overall assessment of the IRS business continuity program based on results presented in those reports.

To accomplish the audit objective, we reviewed and summarized the results of our three prior audits that covered each of the four types of business continuity plans and the audit conducted by the GAO on IRS emergency planning.

[1] See reports listed in Appendix IV.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Stephen Mullins, Director
William A. Gray, Audit Manager
Michelle Griffin, Senior Auditor

Appendix III

Report Distribution List

Office of the Commissioner – Attention: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Commissioner, Large and Mid-Size Business Division SE:LM
Commissioner, Small Business/Self-Employed Division SE:S
Commissioner, Tax Exempt and Government Entities Division SE:T
Commissioner, Wage and Investment Division SE:W
Chief, Appeals AP
Chief, Communications and Liaison CL
Chief, Equal Employment Opportunity and Diversity EEO
Director, Office of Research, Analysis, and Statistics RAS
Chief, Agency-Wide Shared Services OS:A
Chief, Criminal Investigation SE:CI
Chief Financial Officer OS:CFO
Chief Human Capital Officer OS:HC
Chief Information Officer OS:CIO
Chief Technology Officer OS:CTO
Director, Office of Professional Responsibility SE:OPR
Director, Whistleblower Office SE:WO
Director, Employee Support Services, Agency-Wide Shared Services OS:A:ESS
Director, Information Technology Security OS:MA:IT
Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services, OS:A:PSEP
Director, Computer Security Incident Response Center and Information Technology Systems Disaster Recovery OS:MA:IT:C
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Chief, Agency-Wide Shared Services OS:A
    Chief Information Officer OS:CIO

Appendix IV

Recent Audit Reports on the Business Continuity Program

This appendix presents information on Treasury Inspector General for Tax Administration and GAO reviews of the IRS business continuity program.

In Fiscal Year 2008, we conducted three separate audits of four areas of IRS business continuity planning and issued the following reports:

1. *Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made* (Reference Number 2008-20-061, dated February 29, 2008).
2. *Emergency Preparedness at Internal Revenue Service Facilities Needs to Be Improved* (Reference Number 2008-10-148, dated September 17, 2008).
3. *Weaknesses in Business Resumption Plans Could Delay Recovery From a Disaster* (Reference Number 2008-20-178, dated September 17, 2008).

In Fiscal Year 2007, the GAO conducted a review of IRS emergency planning and issued the following report:

IRS Emergency Planning: Headquarters Plans Supported Response to 2006 Flooding, but Additional Guidance Could Improve All Hazard Preparedness (GAO-07-579, dated April 2007).

Recommendations from our reviews and management's responses to the recommendations

1) *Disaster Recovery Issues Have Not Been Effectively Resolved, but Progress Is Being Made* (Reference Number 2008-20-061, dated February 29, 2008). This report contained six recommendations related to the IRS disaster recovery program.

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

Management's Response to Recommendation 1: IRS management plans to evaluate and revise all existing disaster recovery plan documentation and templates used to perform and coordinate disaster recovery-related activities; ensure all plan documentation is standardized, accurate, comprehensive, appropriately detailed, up to date, and written in a clear, cohesive format; ensure plan documentation includes all relevant Federal Government guidance and all other critical information needed to perform disaster recovery-related activities; perform a comprehensive inventory analysis audit to ensure the accessibility and availability of all plan documentation and that the appropriate offsite storage and retrieval procedures are in place; and research a web-based centralized repository tool for maintaining disaster recovery documentation in a secure and readily accessible manner.

Recommendation 2: The Chief Information Officer should ensure effective completion of tasks as required in disaster recovery guidance incorporated in the Internal Revenue Manual[1] from the Office of Management and Budget, National Institute of Standards and Technology,[2] and the Federal Information Security Management Act.[3]

Management's Response to Recommendation 2: IRS management plans to develop a comprehensive disaster recovery Internal Revenue Manual and ensure all program-related documentation adheres to and complies with all relevant Federal Government guidance. In addition, management will ensure effective completion of tasks as required in Internal Revenue Manual disaster recovery guidance through the embedded Compliance function within the Cybersecurity organization's Disaster Recovery organization. Management will also provide status reports on each of the disaster recovery recommendations through bi-monthly meetings with the Deputy Commissioner for Operations Support.

Recommendation 3: The Chief Information Officer should ensure offsite storage vendors can timely deliver all disaster recovery backup files and documentation to the disaster recovery site using announced, unannounced, and actually planned tests.

Management's Response to Recommendation 3: IRS management plans to implement a documented repeatable process during the 2007-2008 annual Federal Information Security Management Act reporting period that includes an Information Technology Contingency Plan/Disaster Recovery Test Guide and Checklist. Management also plans to direct test participants to provide evidence of the recovery backup files' delivery and actual time frame for delivery. Business/System owners will update the Checklist with the results of the exercises and enter findings into the application/General Support Systems Plans of Action and Milestones. The completed Checklist will validate completion of the Tabletop Exercise and Functional Test

[1] The Internal Revenue Manual contains the policies, procedures, instructions, guidelines, and delegations of authority which direct the operation and administration of the IRS.

[2] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

[3] Part of the E Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301 (2002). The Federal Information Security Management Act includes protecting information and information systems from unauthorized access, use, disclosure, or modification, including controls for disclosure and confidentiality to protect personal privacy.

and document findings. It will then be loaded into Trusted Agent Federal Information Security Management Act as the artifact verifying the results of the exercise/test.[4]

Recommendation 4: The Chief Information Officer should ensure appropriate disaster recovery site personnel are identified and provided with annual training to ensure they have the ability to implement the disaster recovery plan in the event production site personnel are not available during a disaster.

Management's Response to Recommendation 4: IRS management plans to develop a comprehensive disaster recovery specific training curriculum; develop a specialized training course to address specific training requirements in various disaster recovery disciplines such as testing, plan development, business impact assessment, and compliance, and train all individuals who have disaster recovery responsibilities; initiate a site-to-site cross-training skill set evaluation and training program to ensure critical skill sets reside in a specific location, responsible individuals receive training, and skill sets are replicated in other locations; and develop a database as training is completed to provide an assessment report to management for use in evaluating training progress, qualified personnel, and skill set risks.

Recommendation 5: The Chief Information Officer should ensure that disaster recovery exercise lessons learned or action items deemed as critical are included in subsequent exercises.

Management's Response to Recommendation 5: IRS management plans to develop a repeatable process to ensure subsequent exercises include lessons learned or action items deemed as critical. As all Information Technology Contingency Plans and disaster recovery plans are exercised and tested, test participants will follow a formal Checklist to ensure documentation of system/organizational changes or problems encountered during plan implementation, execution, or testing. If more critical problems are found, Summary Findings will note where corrective actions and findings are documented for viewing and analysis by the Designated Approving Authority. Management also plans to develop a process for entering these findings in the application/General Support Systems Plans of Action and Milestones for monitoring and training, and require the Designated Approving Authority to sign the Checklist validating that the Tabletop Exercise and Functional Test have been completed and findings documented.

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

[4] The Trusted Agent Federal Information Security Management Act is an automated management tool that maintains Federal Information Security Management Act reporting data for application systems and their associated corrective actions. It captures and tracks security weaknesses and associated corrective milestones; and collects, processes and stores self-assessment information, as required under the Federal Information Security Management Act.

Management's Response to Recommendation 6: IRS management established the Modernization and Information Technology Services organization's Information Technology Disaster Recovery organization. The responsibilities of this program office include validating all closure activities for corrective actions and collecting and maintaining all documentation that supports closure and/or mitigation of all correction actions, material weaknesses, and any outstanding year-to-year weaknesses remediation recommendations. Management also established a process using project management schedules, work breakdown structures, and cross-functional correspondence that enables this office to provide management with a more effective assessment of material weakness remediation progress for disaster recovery.

2) *Emergency Preparedness at Internal Revenue Service Facilities Needs to Be Improved* (Reference Number 2008-10-148, dated September 17, 2008). This report contained three recommendations related to the IRS incident management and occupant emergency plans.

Recommendation 1: The Chief, Agency-Wide Shared Services, should revise the IRS' current incident management plan template and associated instructions to 1) better emphasize the need to ensure both primary and backup Emergency Operations Center locations are specified, backups are specified for all key incident management staff, an initial Incident Commander is identified where appropriate, a general description of the nature of IRS business functions located at the site is listed, and complete and current contact information for the applicable functional Business Resumption Coordinators is specified, and 2) require that all incident management plans be periodically reviewed to ensure that they are complete and accurate.

Management's Response to Recommendation 1: The IRS plans to revise the incident management plan template and procedures to incorporate the elements outlined in this recommendation.

Recommendation 2: The Chief, Agency-Wide Shared Services, should develop procedures requiring that 1) all significant IRS sites, including Computing Centers,[5] perform incident management plan exercises on a routine basis, and 2) the results of these exercises, including any plan weaknesses identified, be documented to facilitate an ongoing agency-wide analysis of trends and best practices.

Management's Response to Recommendation 2: The IRS plans to develop criteria for a multi-year testing, training, and exercise strategy consistent with Federal Government continuity directives that will address action item followups and/or lessons learned.

Recommendation 3: The Chief, Agency-Wide Shared Services, should consider developing a template to record the key results of occupant emergency plans evaluation testing, such as, the time to complete the evaluation, whether employees properly reported to assigned assembly areas, and whether alarms functioned properly.

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

Management's Response to Recommendation 3: The IRS has developed a comprehensive checklist to capture and record site evaluations. In addition, a structured process for monitoring evacuations and fire drills will be defined and implemented.

3) ***Weaknesses in Business Resumption Plans Could Delay Recovery From a Disaster*** **(Reference Number 2008-20-178, dated September 17, 2008).** The report contained four recommendations related to the IRS business resumption plans.

Recommendation 1: The Chief, Agency-Wide Shared Services, should instruct business units with a significant number of sites to establish a business resumption coordinator position to 1) perform a quality review of each business resumption plan prepared by the business resumption team leader at a site within the function, and 2) create and maintain a repository in each business unit to account for and control business resumption plans.

Management's Response to Recommendation 1: IRS management will coordinate the establishment of full-time business coordinator positions, as appropriate, to enhance the business unit continuity program.

Recommendation 2: The Chief, Agency-Wide Shared Services, should require all business functions to use the PSEP office business resumption plan templates and require all functions' business resumption coordinators to periodically brief the Emergency Management and Preparedness Executive Steering Committee on the completeness and adequacy of the business resumption plans.

Management's Response to Recommendation 2: IRS management will direct the use of standardized continuity templates developed by the PSEP office. In addition, the Emergency Management and Preparedness Executive Steering Committee will receive periodic briefings from select business coordinators.

Recommendation 3: The Chief, Agency-Wide Shared Services, should develop specific testing requirements and procedures for business resumption plans based on risk. Critical processes such as those we reviewed should be tested using comprehensive testing techniques such as parallel, simulation, or full-interruption tests.

Management's Response to Recommendation 3: IRS management will develop criteria for a multi-year testing, training, and exercise strategy. This strategy will be consistent with Federal Government continuity directives.

Recommendation 4: The Chief, Agency-Wide Shared Services, should instruct the Emergency Management and Preparedness Executive Steering Committee to 1) require business units to plan and conduct testing, document test results, and update business resumption plans annually, and 2) monitor testing activities conducted by the business units to ensure that the scopes of tests are sufficient to identify gaps and weaknesses in the plans.

Management's Response to Recommendation 4: IRS management will develop a multi-year testing, training, and exercise strategy that is consistent with Federal Government continuity directives.

Recommendations from a GAO review and management's responses to the recommendations

***IRS Emergency Planning: Headquarters Plans Supported Response to 2006 Flooding, but Additional Guidance Could Improve All Hazard Preparedness* (GAO-07-579, dated April 2007).**

To strengthen the ability of the IRS to respond to the full range of potential disruptions to essential operations, the GAO made the following two recommendations to the IRS Commissioner:

Recommendation 1: Revise IRS internal emergency planning guidance to fully reflect Federal guidance on the elements of a viable continuity capability, including the identification and prioritization of essential functions; the preparation of necessary resources and alternate facilities; and the regular completion of tests, training, and exercises of continuity capabilities.

Management's Response to Recommendation 1: The IRS will:

- Conduct a thorough gap analysis between Federal Preparedness Circular 65 elements and business continuity planning guidance.[6]
- Update the Internal Revenue Manual guidance and business resumption plan templates to reflect areas of improvement resulting from the gap analysis.
- Formally direct annual tests, training, and exercises of business resumption plans through the agency's Emergency Management and Preparedness Steering Committee.

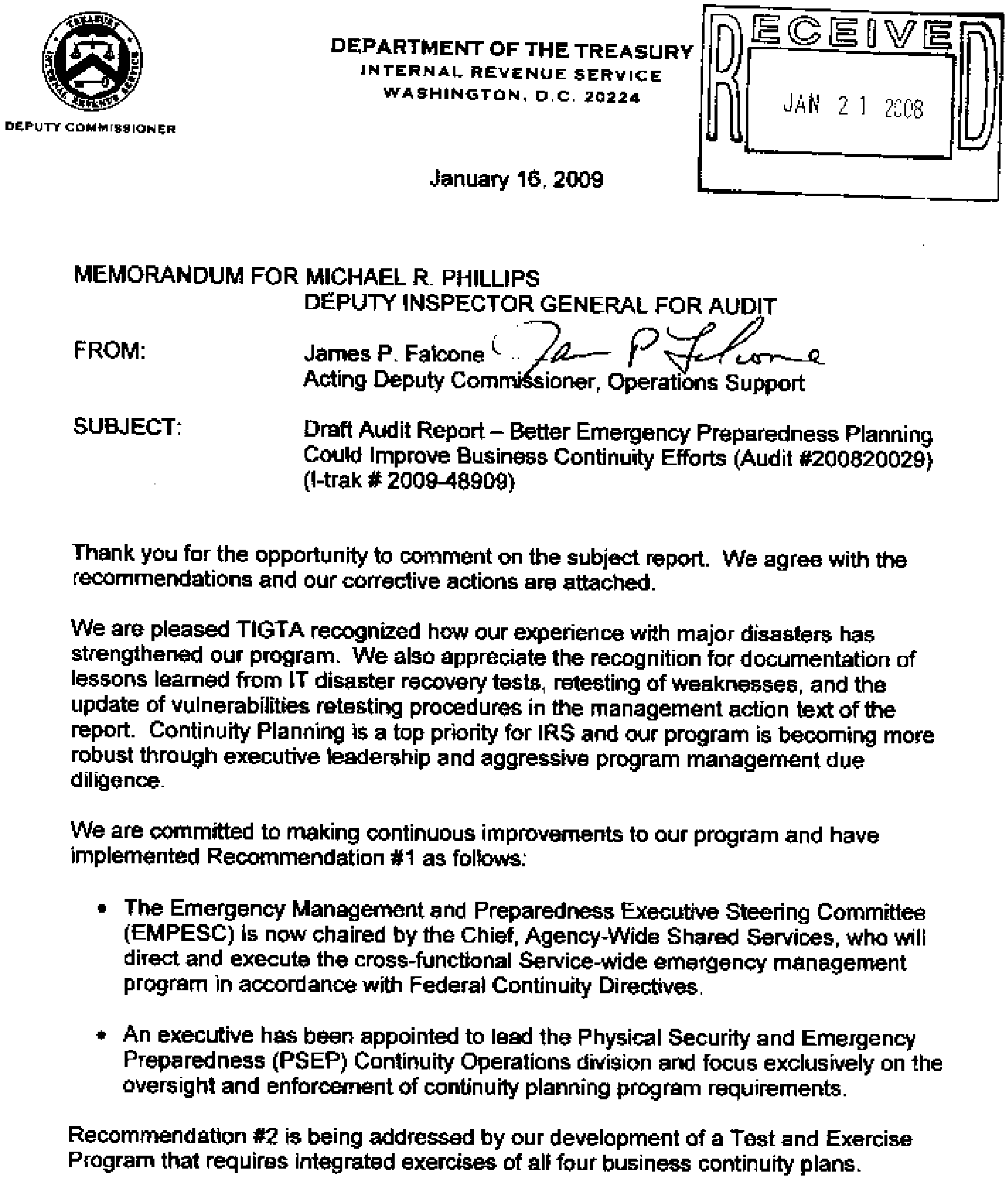
Recommendation 2: Revise IRS emergency plans in accordance with the new internal guidance.

Management's Response to Recommendation 2: The IRS will revise and implement its emergency plans based on the results of the aforementioned activities (in Recommendation 1).

[6] Federal Preparedness Circular 65 provides guidance to Federal executive branch departments and agencies for use in developing viable and executable contingency plans for the continuity of operations.

Appendix V

Management's Response to the Draft Report



DEPUTY COMMISSIONER

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

January 16, 2009

MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: James P. Falcone
Acting Deputy Commissioner, Operations Support

SUBJECT: Draft Audit Report – Better Emergency Preparedness Planning Could Improve Business Continuity Efforts (Audit #200820029) (I-trak # 2009-48909)

Thank you for the opportunity to comment on the subject report. We agree with the recommendations and our corrective actions are attached.

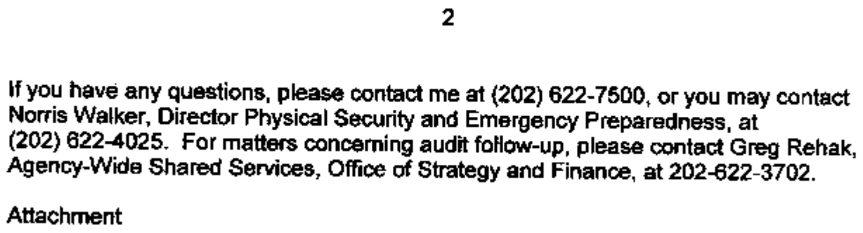
We are pleased TIGTA recognized how our experience with major disasters has strengthened our program. We also appreciate the recognition for documentation of lessons learned from IT disaster recovery tests, retesting of weaknesses, and the update of vulnerabilities retesting procedures in the management action text of the report. Continuity Planning is a top priority for IRS and our program is becoming more robust through executive leadership and aggressive program management due diligence.

We are committed to making continuous improvements to our program and have implemented Recommendation #1 as follows:

- The Emergency Management and Preparedness Executive Steering Committee (EMPESC) is now chaired by the Chief, Agency-Wide Shared Services, who will direct and execute the cross-functional Service-wide emergency management program in accordance with Federal Continuity Directives.

- An executive has been appointed to lead the Physical Security and Emergency Preparedness (PSEP) Continuity Operations division and focus exclusively on the oversight and enforcement of continuity planning program requirements.

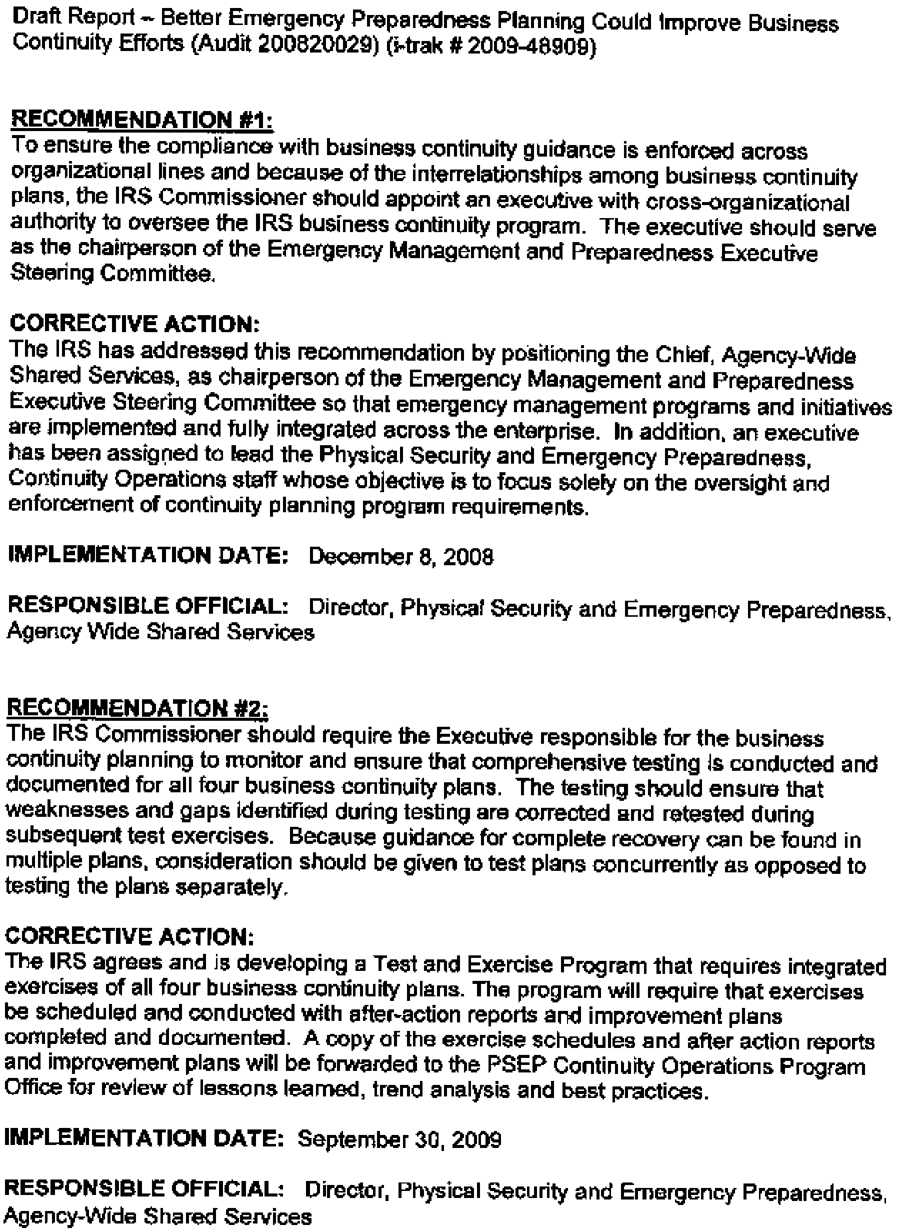
Recommendation #2 is being addressed by our development of a Test and Exercise Program that requires integrated exercises of all four business continuity plans.



2

If you have any questions, please contact me at (202) 622-7500, or you may contact Norris Walker, Director Physical Security and Emergency Preparedness, at (202) 622-4025. For matters concerning audit follow-up, please contact Greg Rehak, Agency-Wide Shared Services, Office of Strategy and Finance, at 202-622-3702.

Attachment



Draft Report – Better Emergency Preparedness Planning Could Improve Business Continuity Efforts (Audit 200820029) (i-trak # 2009-48909)

RECOMMENDATION #1:

To ensure the compliance with business continuity guidance is enforced across organizational lines and because of the interrelationships among business continuity plans, the IRS Commissioner should appoint an executive with cross-organizational authority to oversee the IRS business continuity program. The executive should serve as the chairperson of the Emergency Management and Preparedness Executive Steering Committee.

CORRECTIVE ACTION:

The IRS has addressed this recommendation by positioning the Chief, Agency-Wide Shared Services, as chairperson of the Emergency Management and Preparedness Executive Steering Committee so that emergency management programs and initiatives are implemented and fully integrated across the enterprise. In addition, an executive has been assigned to lead the Physical Security and Emergency Preparedness, Continuity Operations staff whose objective is to focus solely on the oversight and enforcement of continuity planning program requirements.

IMPLEMENTATION DATE: December 8, 2008

RESPONSIBLE OFFICIAL: Director, Physical Security and Emergency Preparedness, Agency Wide Shared Services

RECOMMENDATION #2:

The IRS Commissioner should require the Executive responsible for the business continuity planning to monitor and ensure that comprehensive testing is conducted and documented for all four business continuity plans. The testing should ensure that weaknesses and gaps identified during testing are corrected and retested during subsequent test exercises. Because guidance for complete recovery can be found in multiple plans, consideration should be given to test plans concurrently as opposed to testing the plans separately.

CORRECTIVE ACTION:

The IRS agrees and is developing a Test and Exercise Program that requires integrated exercises of all four business continuity plans. The program will require that exercises be scheduled and conducted with after-action reports and improvement plans completed and documented. A copy of the exercise schedules and after action reports and improvement plans will be forwarded to the PSEP Continuity Operations Program Office for review of lessons learned, trend analysis and best practices.

IMPLEMENTATION DATE: September 30, 2009

RESPONSIBLE OFFICIAL: Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services