The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans

February 2000

Reference Number: 2000-20-031

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 29, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans

This report presents the results of our review of the Internal Revenue Service's (IRS) Disaster Recovery and Business Resumption planning efforts. In summary, we found the IRS needs to complete disaster recovery and business resumption plans for all major facilities and take steps to ensure resources are available to implement plans in the event of a disaster or failure.

Overall, our recommendations will reduce the risk of prolonged interruptions in tax administration and the risk of permanently lost data. The recommendations will help ensure the IRS can recover as quickly as possible from a disaster once contingency plans are completed for the sites that did not have them at the time of our review. The recommendations will also help ensure that important data files that were not stored off-site will be available to restore service in case of disaster.

IRS management agreed to the findings in this report, but did not agree with 2 of our 12 recommendations. The two recommendations suggested that the IRS purchase or establish agreements to lease back-up generators during times of need and to make alternative arrangements for space in the event of a disaster. The IRS believes that alternative approaches would be more effective and cost less. However, at the time of our review, most locations did not have adequate disaster recovery and business resumption plans to address these risks. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

Please contact me at (202) 622-6510 if you have questions, or your staff may contact Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Executive Summary

It is critical that the Internal Revenue Service (IRS) have the ability to resume operations in case of disaster. The IRS processes over 200 million tax returns and collects $1.7 trillion in taxes annually. The IRS also assists about 120 million taxpayers and issues 90 million individual refunds. Long delays in restoring IRS operations after a disaster would have a serious impact on taxpayer service and cause delays in collecting taxes.

The objective of this review was to determine whether the IRS' disaster recovery and business resumption plans are sufficient to ensure the IRS is capable of resuming operations in case of disaster or failure. This report does not address Year 2000 contingency planning, which was addressed in our report entitled, *Review of the Internal Revenue Service's Year 2000 Contingency Planning Efforts* (Reference Number 092705, dated March 1999).

Results

Although the IRS is making progress in its disaster recovery and business resumption planning efforts, these efforts are far from complete. The IRS does not have the plans or resources needed to recover from disasters or failures at many major locations. It also lacks adequate testing procedures to ensure that computer data back-up files and other necessary resources will be available in the event of a disaster. Without adequate contingency plans and back-up resources, the IRS is at risk of prolonged interruptions in tax administration and permanently lost data.

Overall, many of the problems we found have been reported to the IRS previously. The IRS has not yet developed adequate guidance and IRS managers have not taken the actions necessary to ensure contingency plans are completed timely and that resources needed to implement plans are available.

Disaster Recovery and Business Resumption Plans Are Not Complete

In the event of a disaster, recovery plans are needed to restore critical information systems, and business resumption plans are needed to restore important IRS functions, such as taxpayer service and tax return processing. However, 30 of 45 major IRS facilities (computing centers, service centers, and district offices) have not completed both disaster recovery and business resumption plans. The largest facilities without both types of plans include one computing center and four service centers which process and store a large volume of taxpayer data. Without both plans in place, these facilities are vulnerable to extended downtime after a disaster or failure.

Furthermore, the plans that had been completed did not always contain important information or provide for resources needed to resume business. Computing center and service center plans did not have listings of critical information systems or listings of equipment and supply needs. Five of the 10 service centers do not have electrical generators to support computer operations and other business functions in case of electrical outage. Service centers also did not have agreements for use of alternate space if needed. Disaster recovery and business resumption plans could not be fully implemented without these important resources.

Computer Information Needed to Resume Business in the Event of a Disaster Is Not Adequately Stored Off-site

Because of the large volume of electronic data used by the IRS, functions such as processing of tax returns, payments, and refunds cannot be fully restored without back-up computer data files. Back-up files need to be kept at an alternate location (off-site) to avoid damage during a disaster. The two computing centers and two service centers we reviewed did not store all necessary files off-site. These critical files included masterfiles, mainframe computer files, and minicomputer files.

Procedures to Test and Update Plans Are Not Adequate

Although computing centers and service centers have taken some steps to test and update plans that have been completed, additional guidance is needed to ensure all major facilities adequately test and update disaster recovery and business resumption plans. Adequate testing and updating would uncover the problems we identified, such as missing computer back-up files and resources needed to implement disaster recovery and business resumption plans.

Summary of Recommendations

The IRS should develop a master plan, including standards and a schedule for completion of disaster recovery and business resumption plans. Completion of plans for each major IRS location should be monitored. The IRS needs to obtain electrical generators for major processing locations, such as service centers, and establish agreements to provide alternate space for service centers when needed. It also needs to establish off-site back-up procedures for all important computer data files and verify monthly that back-up data files are completed and sent off-site.

To help ensure adequate plans and resources are put in place, the IRS should develop guidance to direct the testing and updating of disaster recovery and business resumption

plans. It should also incorporate disaster recovery and business resumption planning in the performance rating process for managers in charge of operations at major facilities.

Management's Response: Management agreed to most of our recommendations and will have the Office of Security and Privacy Oversight oversee the corrective actions taken in response to this report. Management disagreed with the recommendations covering back-up generators and alternate space arrangements because of the costs associated with the purchase or lease of generators and the maintenance of alternate space agreements.

Management disagreed with one portion of our benefits analysis relating to the general benefit of developing adequate business resumption plans which would reduce the risk of interruptions in processing and taxpayer service. Management believes it has an adequate strategy in place to reroute returns, remittances, and calls to unaffected operational customer service or return processing locations. They believe this strategy would significantly reduce the negative impact associated with an extended outage at one of the IRS facilities.

Office of Audit Comment: In regard to management's comments on back-up generators and alternate space arrangements, adequate contingency planning may allow alternate courses of action which are more cost effective. However, as noted above, during our review, many major IRS facilities did not have adequate disaster recovery and business resumption plans to provide these alternate strategies to resume business.

Locations that did have plans in place relied significantly on moving to alternate space without specifying what space alternatives were available or whether agreements were in place. Business resumption plans should be more specific in both areas to help facilitate effective and timely business resumption after a disaster or failure.

Management's disagreement with the portion of our benefits analysis relating to the reduced risk of interruptions in processing and taxpayer service assumes that a strategy is in place that would reduce these risks. Such a strategy should be included in disaster recovery and business resumption plans. Again, at the time of our review, most major IRS processing sites did not have adequate disaster recovery and business resumption plans to address these risks.

Objective and Scope

We initiated this review in conformance with the Internal Revenue Service (IRS) Restructuring and Reform Act, Pub. L. No. 105-206, 112 Stat. 685 (1998), which requires the Treasury Inspector General for Tax Administration to evaluate the adequacy and security of the IRS' information technology.

Our review evaluated the IRS' plans to recover and resume business in case of disaster.

The overall objective of the review was to determine whether the IRS' disaster recovery and business resumption plans are sufficient to ensure the IRS is capable of resuming operations in case of disaster or failure. This review did not address Year 2000 contingency planning, which was addressed in our report entitled, *Review of the Internal Revenue Service's Year 2000 Contingency Planning Efforts* (Reference Number 092705, dated March 1999).

To achieve our audit objective, we:

- Determined whether disaster recovery and business resumption plans were developed for IRS operations and whether the plans were sufficient to resume operations promptly.
- Determined whether back-up data files necessary to recover from a disaster are maintained off-site for IRS mainframe and minicomputer systems.
- Determined if the IRS has implemented adequate policies and procedures to ensure plans are tested and maintained.

We reviewed disaster recovery and business resumption plans at the Martinsburg and Tennessee Computing Centers, the Memphis and Andover Service Centers, and the New Jersey District. We also obtained information from a survey of all 10 IRS service centers and 33 district offices. We conducted audit work from October 1998 through May 1999. This audit was performed in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are included as Appendix I to this report. Major contributors to this report are listed in Appendix II.

Background

The OMB requires federal agencies to ensure appropriate contingency plans are developed to recover information systems.

The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, requires federal agencies to establish policies and assign responsibilities to assure appropriate contingency plans are developed and maintained by end users of information technology applications.

The IRS must maintain its ability to administer the nation's tax laws and continue operations in the event of disasters or failures at any of its facilities. Contingency planning is the primary tool the IRS has to recover from disasters and failures and to resume orderly operations. The Internal Revenue Manual (IRM) requires contingency plans be developed, implemented, tested, and maintained for all critical information systems.

The IRS includes both of the following components in its contingency planning process:

- Disaster recovery plans - needed to restore critical information systems necessary to perform the business operations.
- Business resumption plans - needed to resume business activities after a disaster or failure within specified guidelines generated by business priorities.

Responsibility for oversight of IRS disaster recovery planning rests with the SSE.

The IRS has taken action to develop disaster recovery and business resumption plans. It created the Office of Disaster Recovery, which was consolidated into the Office of Security Standards and Evaluation (SSE) in March 1998. In May 1995, the IRS developed a business resumption strategy for service centers. The Executive Office for Service Center Operations (EOSCO) and the Northeast Regional Office recently implemented a pilot program to assist in the completion

of service center and district office business resumption plans.

Results

While progress is being made, the IRS still does not have all the necessary plans in place to recover from disasters or failures.

The IRS is continuing to make progress in the preparation of disaster recovery and business resumption plans. The IRS has:

- Established responsibilities for disaster recovery and business resumption plans within the IRM.
- Established a Disaster Recovery and Business Resumption Group within the SSE.
- Trained employees on disaster recovery and business resumption planning at the five sites we visited.

However, the IRS' actions are not yet complete and critical operations do not all have comprehensive plans and the necessary resources needed to implement plans in the event of a disaster. Many of the problems that we found have been reported to the IRS in previous reports on IRS systems security by the General Accounting Office, the former IRS Inspection Service, and other IRS internal reviews.

Disaster Recovery and Business Resumption Plans Are Not Complete

Natural disasters, as well as attacks and threats against federal government facilities, give rise to the need for adequate contingency planning. In the event of a disaster, recovery plans are needed to restore critical information systems and business resumption plans are needed to restore important operations, such as processing of tax returns, payments, and refunds, and providing taxpayer service. Both disaster recovery and business resumption plans need to be completed and coordinated to be able to fully recover after a disaster.

Disaster recovery plans are needed to restore information systems and business resumption plans are needed to restore business operations; however, 30 of the 45 sites we surveyed had not completed both types of plans.

Despite the importance of having both plans at each major facility, many critical IRS facilities lack either one or both types of plans. We reviewed plans at five sites (including both computing centers, two service centers, and one district office) and surveyed all IRS service centers and district offices to determine the status of contingency planning at each location.

The IRS had not completed both disaster recovery and business resumption plans at 30 of 45 major sites (67 percent) including 1 computing center and 4 service centers. These IRS facilities process and store a large volume of taxpayer data. Only 8 of 33 district offices reported they had completed both types of plans. Table I shows the number of major IRS sites with disaster recovery and business resumption plans.

Table I – Number of IRS Sites with Disaster Recovery and Business Resumption Plans

Facility Type	Number of Facilities	Sites With Only Disaster Recovery Plans	Sites With Only Business Resumption Plans	Sites With Both Types of Plans
Computing Centers	2	1	0	1
Service Centers	10	0	4	6
District Offices	33	0	1	8
Totals	**45**	**1**	**5**	**15**

Furthermore, the IRS needs to improve the disaster recovery and business resumption plans that have been developed. According to government and industry guidelines, these plans should contain:

- All important systems and listings of mission critical applications with required recovery times (needed to establish priorities in bringing applications back on line).
- Alternate space agreements (needed to move operations to other office space).

- Listings of specific equipment and supply needs (needed to purchase or obtain equipment and supplies for alternate space).

Plans that have been completed do not have all necessary information and do not cover all important information systems.

We reviewed plans at five sites and found that these plans did not have all necessary information and did not cover all the important information systems and resources.

- One computing center did not include its mainframe systems for service centers in its disaster recovery plan.
- One computing center and two service centers did not include minicomputer systems in their disaster recovery plans.
- Two computing centers (for the consolidated service center mainframe systems) and two service centers did not list mission critical computer applications and the order of priority to restore these applications.
- Five service centers did not have electrical generators needed to continue operations in the event of a power outage (one of these did have a dual power source and may be able to continue operations if the outage affected only one source).
- Two service centers and the district office did not provide for alternate space needs in case of disaster.
- Two computing centers and one service center did not list all equipment and supplies needed to resume operations.

Certain plans were developed when required within specific time frames. However, the IRS must further emphasize timely and complete plan development.

The IRS must make sure that plans are developed and have all the important elements. Overall, IRS management has not emphasized timely plan development or assigned responsibilities to one office nationally for plan completion. Requiring plans to be in place within a specific time frame will help in setting the priority of this important task. For example, all 10 service centers were given specific dates for completing business resumption plans by the EOSCO and all service centers completed plans. However, the

SSE has not given service centers specific dates for completion of disaster recovery plans, and four service centers have yet to complete these plans.

Delays in recovering operations due to inadequate planning would have a significant adverse effect on the IRS' ability to provide taxpayer service and to collect taxes.

There is a considerable need for the IRS to complete plans for all major locations. It is critical that it has the ability to resume operations in case of disaster. The IRS processes over 200 million tax returns and collects $1.7 trillion in taxes annually. The IRS also assists about 120 million taxpayers and issues 90 million individual refunds. One service center's Fiscal Year 1998 activity during an average week included:

- Processing of approximately 530,000 tax returns.
- Issuing 206,000 refunds.
- Collecting approximately $126 million in revenue.

These totals are significantly higher during the peak tax return filing season from January through April. Long delays in restoring IRS operations after a disaster would have a serious impact on taxpayer service and cause delays in collecting taxes.

The IRS needs to develop an overall plan with scheduled time frames for completion of disaster recovery and business resumption plans for all major locations.

Recommendations

1. The SSE, in coordination with other IRS offices, should develop an overall IRS plan that includes standards and a schedule for completion of disaster recovery and business resumption plans. The SSE should monitor completion of plans for each major IRS location.

2. The Chief Operations Officer (COO) and the Chief Information Officer (CIO) should include disaster recovery and business resumption in the performance rating process for senior management and information officers at computing centers, service centers, and districts.

3. The Assistant Commissioner (Support Services) should purchase generators for service centers that do not have adequate generator capacity or establish agreements to lease generators during times of need.

4. The Assistant Commissioner (Support Services) should develop an IRS-wide memorandum of understanding with the General Services Administration (GSA) which specifies service center alternate space needs in the event of a disaster.

Management's Response: The Office of Security, Evaluation and Oversight (formerly the SSE) will coordinate with the responsible officials and will issue a memorandum for the completion of an overall IRS plan, which will include standards and a schedule for completion of disaster recovery and business resumption plans. The COO and the CIO will factor in the efforts of responsible senior managers and information officers to implement disaster recovery and business resumption during the performance rating process.

Management does not agree with the recommendations to purchase or lease generators for service centers that do not have adequate generator capacity and to establish an agreement with the GSA to specify service center alternate space needs in the event of a disaster because of the associated costs.

Office of Audit Comment: If management establishes adequate alternate courses of action which avoid the need for generators or alternate space, the risk of significant interruptions in processing and taxpayer service could be minimized. However, at the time of our review, most locations did not have adequate disaster recovery and business resumption plans, and the locations that did have plans in place relied significantly on moving to alternate space without specifying what space alternatives were available or whether agreements were in place. Disaster recovery and business resumption plans should be more specific in both areas to help facilitate effective and timely business resumption after a disaster or failure.

Computer Information Needed to Resume Business in the Event of a Disaster Is Not Adequately Stored Off-site

Back-up data files stored off-site are critical to disaster recovery planning. If back-up data files are not taken off-site, important tax information could be damaged if a disaster occurred at a primary facility. The IRS was not always storing important data files off-site.

The Martinsburg Computing Center (MCC) did not keep off-site back-up files needed to recover two of seven masterfiles

The IRS computer masterfiles contain taxpayer information for the entire nation. The IRS maintains and processes accounts on seven types of masterfiles, which include individual and business tax as well as information returns.

Two of the IRS' seven masterfiles were not sent off-site for back-up in case of disaster.

The MCC has off-site back-up procedures for the masterfiles. However, two of the seven masterfiles, the Debtor Masterfile and the Payer Masterfile, were not being stored off-site. The Debtor Masterfile identifies taxpayers with a debt to another government agency. The Payer Masterfile contains information on all sources and amounts of income and tax withholdings.

MCC personnel determined that the Debtor Masterfile was not stored off-site when they were preparing for the annual disaster recovery test. This happened because of a redesign of the database that was not reflected in the back-up procedures. In addition, computer programmers do not notify computing center personnel when changes are made to databases or programs that affect files needed to be stored off-site. As a result, computing center personnel responsible for sending files off-site must try to identify these files by reviewing all program changes.

The Payer Masterfile must be re-established each year. However, the data files created when re-establishing the

Payer Masterfile were not stored off-site. These files are necessary to restore the Payer Masterfile until current year processing begins in approximately May of each year. MCC personnel were unaware files were not being stored off-site because disaster recovery tests were conducted after the Payer Masterfile was restored. Once we found this problem, MCC personnel identified back-up data files needed to recover the Payer Masterfile for January through April and plan to send those files off-site beginning in January 2000.

The IRS should verify monthly that proper back-up files are sent off-site to avoid losing a significant amount of data.

Since data files for the Debtor and Payer Masterfiles were not stored off-site from January to May 1999, the IRS was vulnerable to almost five months of lost Debtor Masterfile data and the inability to process Payer Masterfile data. The IRS needs to establish procedures to verify all needed back-up files for critical systems are being completed and stored off-site monthly to avoid missing files in the event of a disaster.

Computing centers did not store back-up data files for mainframe systems off-site

All mainframe computer systems that are in the service centers are being consolidated into two computing centers.

Service center mainframe systems are being consolidated at the MCC and Tennessee Computing Center (TCC). Computer systems for five service centers will be consolidated at each computing center. The two computing centers will eventually maintain and process mainframe computer data previously processed by the service centers. The mainframe systems that are replacing service center mainframe operations are:

- **The Service Center Replacement System (SCRS)**- provides real-time access to on-line databases and perfects tax return information for input to IRS masterfiles.
- **The Integrated Collection System/Automated Collection System/Printer Replacement to Integrate New Tools (I/A/P) -** supports the tax collection and printed product processes.

- **The Security and Communications System (SACS) -** controls all IRS employee on-line access to taxpayer accounts.

While mainframe consolidation has many benefits, it also increases the risk that five service centers could lose mainframe computing capability if a disaster or failure happened at one computing center.

Consolidation of the SACS is complete for all 10 service centers. At the time of our review, the other mainframe computer systems had been consolidated for three service centers (Brookhaven, Kansas City, and Memphis). As consolidation is completed (two service centers in 1999 and five in 2000), computing centers' disaster recovery and off-site back-up files become increasingly important. In case of failure, the IRS could lose mainframe computer systems for five service centers at a time. To avoid this potential, the IRS plans to have computing centers back up each other for disaster recovery purposes, which should enable the 5 affected service centers to recover within 36 hours.

The IRS is not sending many of the files off-site that would be necessary to restore the data to its consolidated mainframe systems if a disaster occurred.

We reviewed off-site back-up files for IRS consolidated mainframe systems at both computing centers. The MCC was not sending any files for consolidated mainframe systems off-site and the TCC was sending only 38 of 118 needed database files (32 percent) off-site. Table II shows the number of computing center mainframe database files stored off-site.

Table II – Number of Service Center Consolidated Mainframe Database Files Stored Off-site

Systems	Number of Files That Need to be Stored Off-site	Number Off-site at Martinsburg	Number Off-site at Tennessee
SCRS	67	0	28
I/A/P	40	0	0
SACS	11	0	10
Total Database Files	**118**	**0**	**38**

One of the important files that was not sent off-site contained SACS security profile data, which control all IRS employees' access to taxpayer information. At the time of our review, the MCC and the TCC each had security profile data for its five service centers. Since consolidation for the SACS system is complete, the fact

that neither computing center was storing security profile data off-site created the risk of having half of all IRS employees without access to taxpayer information and unable to input information if a disaster occurred. Once we brought this to the attention of management, the Chief, Integrated Systems Software Branch initiated procedures for each computing center to send its security data profiles to the other computing center daily. However, to be better prepared for a disaster, computing centers should maintain the security profile data for all 10 service centers on line.

Computing centers were not sending back-up data files for consolidated mainframe systems off-site because disaster recovery procedures were not specific enough at each location.

Computing centers were not sending back-up data files for consolidated mainframe systems and masterfile off-site for the following reasons:

- Disaster recovery procedures were not specific enough at each location to complete off-site data back-ups as required, and systems were not taken off line long enough to complete back-up files needed for disaster recovery.
- Computing center personnel were not conducting monthly reviews to verify all back-up files needed to restore systems were being completed and stored off-site to recover IRS masterfiles.

Implementing adequate back-up procedures is important to ensure the IRS can continue operations at all service centers in the event of a disaster or failure at one of the computing centers.

Computing centers and service centers did not store back-up minicomputer files off-site

Minicomputer systems are also used for many important processing functions at computing centers and service centers.

Minicomputer systems also process data important to service center operations. These systems are significant to maintain IRS operations because many IRS functions rely on them for processing. The following are examples of important IRS minicomputer systems:

- **The Integrated Submission and Remittance Processing (ISRP) System** – processes tax returns and payments at service centers.

- **The Service Center Recognition/Image Processing System (SCRIPS)** – scans and captures tax data from simple one-sided tax returns, information returns, and remittance documents.
- **The Interim Revenue Accounting Control System (IRACS)** – performs summary-level revenue operations and revenue tracking functions.

Back-up data files for many of the IRS' minicomputer applications were not being stored off-site.

TCC, Memphis Service Center (MSC), and Andover Service Center (ANSC) personnel were sending back-up data files for only 11 of the 36 minicomputer applications (31 percent) off-site. Table III shows the number of minicomputer applications stored off-site.

Table III – Number of Minicomputer Applications Stored Off-site (as of April 1999)

Location	Number of Applications Needing Local Off-site Back-up Files	Number of Applications With Local Off-site Back-up Files
Tennessee Computing Center	5	1
Memphis Service Center	16	6
Andover Service Center	15	4
Totals	**36**	**11**

Following a reorganization of the MSC and the TCC in October 1998, responsibilities for off-site back-up files were not established. The ANSC system administrator had identified the files necessary for recovery, but the scheduling employees had not made provisions for storing all the required back-up files off-site. In all cases, personnel were not verifying that back-up data files were being sent off-site.

In addition, the IRS does not maintain a consolidated listing of minicomputer applications with specific requirements for off-site storage. The IRS does have general guidance (not listed by specific application) in the IRM for all "multi-user systems" and guidance for

each individual system in contingency plans. However, this information is not consolidated into one document that could be used by tape librarians or system administrators to easily verify all back-up files for minicomputer systems are being stored off-site.

Without procedures for off-site storage, ISRP system, SCRIPS, IRACS, and other minicomputer data could be lost if a disaster occurred. After we identified this problem, TCC personnel and ANSC personnel began storing needed minicomputer back-up files off-site.

Recommendations

5. MCC management should ensure personnel update the Payer Masterfile disaster recovery plan to include files needed for recovery prior to the first update. Personnel should ensure these files are sent off-site beginning in the Year 2000.

6. The Assistant Commissioner (National Operations) should update procedures to ensure that information systems programmers notify computing centers of program changes which affect off-site back-up files. Programmers should identify new file names so that the proper files are sent off-site when program changes are made.

7. The Assistant Commissioner (National Operations) should ensure computing centers maintain security profile data for all 10 service centers on line.

8. Computing center management should establish specific procedures to implement disaster recovery off-site procedures, follow specific back-up procedures for consolidated mainframe systems, and take all disaster recovery back-up files off-site. Off-site back-up files could be made from back-up files kept on site without affecting the operation of the systems.

9. Monthly, computing center and service center management should verify that all critical system files are backed up and sent off-site.

10. The Assistant Commissioner (National Operations), in coordination with the SSE, should develop a consolidated listing of off-site storage requirements for minicomputer applications.

Management's Response: The MCC Director will ensure that current back-up file names are added to the MCC Payer Masterfile portion of the Disaster Recovery Plan. A review of the files will be made during the annual plan review to add additional files or correct existing files. Files will be stored off site during the January though May time frame.

New procedures have been developed and will be included in the next revision of the Information Systems Operations Support Handbook (IRM 2.2.8) to ensure that information systems programmers notify computing centers of program changes which affect off-site back-up files.

The disaster recovery plan was revised to require that the computing centers back up the security profile data nightly and electronically transmit the data to each other. The data are stored on tape cartridges in automated tape libraries at each reciprocating computing center.

Computing centers implemented and tested procedures for backing up consolidated mainframe data files.

The computing and service centers will conduct a review of existing procedures to determine actions that can be taken to improve the verification process and determine the feasibility of monthly verifications.

Assurance that minicomputer system recovery requirements are met in disaster recovery plans will be reinforced as part of the corrective action for Recommendation #1.

Procedures to Test and Update Plans Are Not Adequate

To ensure disaster recovery and business resumption plans can be implemented when needed, plans must be continuously updated and periodically tested.

Disaster recovery and business resumption plans must be tested and updated to ensure plans remain current and complete. Otherwise, plans can quickly become obsolete, particularly in a changing business operations and information systems environment.

Tests must be sufficient to identify:

- Weaknesses in each plan's procedures.
- Missing resources needed to implement these plans.

Maintenance procedures must include provisions for:

- Incorporating necessary modifications discovered during testing.
- Continuous plan updates as IRS processes or personnel change.

Many of the disaster recovery and business resumption plans that are completed have not been adequately tested.

IRS guidelines require all computing centers, service centers, and district offices to have adequately tested and updated disaster recovery and business resumption plans. However, only 7 of 16 completed disaster recovery plans (44 percent) and 11 of 20 completed business resumption plans (55 percent) were tested. The completed and tested plans by facility type are in Table IV.

Table IV – Completed and Tested Plans

Facility Type	Number of Facilities	Disaster Recovery Plans		Business Resumption Plans	
		Completed	Tested	Completed	Tested
Computing Centers	2	2	2	1	0
Service Centers	10	6	5	10	10
District Offices	33	8	0	9	1
Total	**45**	**16**	**7**	**20**	**11**

Computing centers did not adequately test plans for recovery of consolidated mainframe systems

The MCC has local operating procedures for updating, annually testing, and certifying the masterfile portion of its disaster recovery plan. Overall, the MCC has followed its procedures to maintain and test this portion of the plan. Those tests identified the Debtor Masterfile back-up problems we noted previously (the tests did not identify the Payer Masterfile problem because it is not feasible to perform tests during peak filing season). However, the MCC has not:

- Developed a disaster recovery plan for consolidated mainframe systems.
- Approved and tested a business resumption plan.

The TCC's plans and testing are not adequate because it has not developed:

- An incident management plan to coordinate activities of the center's functions.
- A disaster recovery plan for minicomputer systems.
- A business resumption plan.

The IRS performed one disaster recovery test of its consolidated mainframe systems in September 1998 at the TCC. This test was performed to demonstrate that the MCC and the TCC could act as recovery sites for each other. However, that test did not use off-site back-up files that were being regularly prepared under normal operations, but instead included special procedures to ensure all necessary data files were available.

Tests did not always identify that the IRS does not have all necessary back-up files stored off-site.

Since the test did not determine that the IRS is not following its procedures and that necessary recovery files are not being maintained in off-site storage, the test was not a valid assessment of its recovery capabilities. Disaster recovery plan tests should simulate resources that could reasonably be available in the event of a

disaster to ensure missing files and other resources are identified.

After we completed fieldwork, the IRS performed an additional test in June 1999 that we did not evaluate.

Service centers' tests of business resumption plans were not adequate

Service centers without disaster recovery plans cannot perform adequate tests of their business resumption plans, since the two plans must be integrated properly to work.

Four service centers (including the two locations we visited) do not have disaster recovery plans. In addition, one service center with a disaster recovery plan has not tested the plan.

The service centers we visited had performed tests and made corrections to their business resumption plans. However, these tests would be of limited benefit since the disaster recovery plan is needed to restore information systems. Without that plan, it is unlikely a service center could resume operations.

Service center testing of business resumption plans ranged from mock disasters with building evacuations to only verifying telephone numbers listed in the plans. A plan subjected to mock disaster testing can generally be considered more reliable than one that has simply had the telephone numbers verified. However, mock disaster tests need to be designed considering the worst case situation. In one such test, one wing of the service center could not be accessed for up to six weeks, but this test did not identify an alternate space for employees or the lack of arrangements with the GSA to provide alternate space if the event had occurred during the peak filing season. Other tests were limited to reading through procedures or verifying telephone numbers in the plan.

Testing guidelines should be developed to ensure comprehensive tests are performed to identify weaknesses and assist in maintaining adequate plans.

District offices have not tested disaster recovery or business resumption plans

Only one district had performed testing of its business resumption plan.

Eight of the 33 district offices we surveyed responded that they had completed both disaster recovery and business resumption plans. But of these eight district offices, only one had performed any testing, and the test was only of its business resumption plan. Districts did not have specific guidance on how to conduct tests.

District offices perform many important functions, including on-site taxpayer service in addition to field compliance operations. It is important that they have plans in place and tested to help make sure they can resume business in the event of a disaster. Because most districts have not completed plans or conducted tests, the IRS needs to provide guidance to assist in this effort.

Recommendations

The IRS needs to provide better guidance to ensure plans are tested adequately. Adequate testing would have identified many of the problems we found.

11. The SSE should develop guidance to assist managers in developing sufficient plan testing and maintenance procedures. This guidance should include, but not be limited to:
    - Ensuring tests are based on off-site data or other resources that would reasonably be available in the event of a disaster.
    - Ensuring any assumptions included in the test are reasonable (e.g., availability of information systems).
    - Verifying that alternate support service organizations can provide necessary services or facilities.
    - Ensuring tests are of sufficient depth to identify plan limitations or areas needing clarification or revision.
12. The SSE should develop consolidated mainframe systems test plans that test disaster recovery at both computing centers using only back-up files stored off-site.

Management's Response: The Office of Security, Evaluation and Oversight developed and issued a guide to disaster recovery plan testing, "Procedural Guide to Exercise Plans." It will ensure tests are conducted and it will monitor the results. IRM 2.1.10.6 identifies the Head of Office as being responsible for the testing of the business continuity plans.

The Office of Security, Evaluation and Oversight will oversee the development of test plans, which will include the use of files from off-site storage. A recent test along with future tests will use files from off-site storage when conducting disaster recovery tests of the consolidated mainframe systems.

Conclusion

The IRS needs an overall plan to govern its disaster recovery and planning and to expedite completion of plans for all major locations.

The IRS has the responsibility to prepare for possible disasters and failures. Nonetheless, it has not yet developed adequate guidance and IRS managers have not taken the actions necessary to ensure plans are completed timely and that resources needed to implement plans are available.

Disaster recovery and business resumption plans should be completed for all major locations and should provide for all computer information and other resources needed to resume business in the event of a disaster. The IRS needs to develop an overall plan to ensure that adequate plans are in place. It also needs to develop guidelines for testing and updating plans for each type of location.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the Internal Revenue Service's (IRS) disaster recovery and business resumption plans are sufficient to ensure the IRS is capable of resuming operations in case of disaster or failure. This review did not address the IRS' Year 2000 contingency planning, which was addressed in a prior report, *Review of the Internal Revenue Service's Year 2000 Contingency Planning Efforts* (Reference Number 092705, dated March 1999).

We reviewed disaster recovery and business resumption plans at the Martinsburg Computing Center, the Tennessee Computing Center, the Memphis Service Center, the Andover Service Center, and the New Jersey District. We also surveyed all IRS service centers and districts. To evaluate the IRS' disaster recovery and business resumption efforts, we:

I. Determined whether disaster recovery and business resumption plans were developed for IRS operations and whether plans were sufficient to resume operations promptly.

   A. Determined the Office of Systems Standards and Evaluation's progress in establishing oversight policies for developing disaster recovery and business resumption plans.

   B. Determined if senior management emphasized disaster recovery and business resumption planning and also determined whether it was an element in their performance rating.

   C. Determined whether specific deadlines have been given to field offices for development of disaster recovery plans.

   D. Analyzed disaster recovery and business resumption plans and determined whether they adequately address business and disaster recovery procedures necessary for restoring essential IRS activities, systems, and assets.

II. Determined whether back-up data files necessary to recover from a disaster are maintained off-site for IRS mainframe and minicomputer systems.

   A. Determined whether essential or critical information systems have been identified.

   B. Determined whether management documented the critical requirements necessary to restore operations at each location.

C. Visited the off-premises storage facility. For selected systems, determined whether important files, computer programs, and documentation are stored at the facility and whether this information is sufficient and current enough to enable recovery.

III. Determined if the IRS has implemented adequate policies and procedures to ensure plans are tested and maintained.

A. Reviewed memoranda or other directives requiring the performance of disaster recovery and business resumption plan testing.

B. Reviewed the results of disaster recovery and business resumption tests at selected locations.

C. Determined if the procedures require that only the back-up databases and programs specified in the disaster recovery and business resumption plan are used for the test(s).

D. Reviewed the methods used to review the test results and perform necessary modifications to the plan.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Scott A. Macfarlane, Deputy Director
Michael E. McKenney, Audit Manager
Aaron R. Foote, Senior Auditor
Janice F. Gates, Auditor
Daniel M. Quinn, Auditor
R. Ed Sampson, Auditor

Appendix III

Report Distribution List

Deputy Commissioner Modernization C:DM
Deputy Commissioner Operations C:DO
Office of the Chief Counsel CC
Chief Information Officer IS
Chief Operations Officer OP
Deputy Chief Information Officer, Operations IS
Deputy Chief Information Officer, Systems IS
Executive Officer For Service Center Operations OP:SC
Assistant Commissioner (Information Systems Field Operations) IS:FO
Assistant Commissioner (National Operations) IS:O
Assistant Commissioner (Service Center Operations) IS:SC
Assistant Commissioner (Support Services) M:S
Assistant Commissioner (Systems Development) IS:S
Director, Office of Information Resource Management IS:IR
Director, Office of Security and Privacy Oversight IS:SPO
Director, Office of Security, Evaluation and Oversight IS:SPO:S
National Director for Legislative Affairs CL:LA

Appendix IV

Outcome Measures

This appendix presents information on the impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to the Congress.

The primary benefit of contingency planning is to ensure the availability of resources, including data, needed to continue operations in the event of a disaster. The cost to the government if the Internal Revenue Service (IRS) were not adequately prepared to recover would depend on the type of disaster and the type of facility affected.

Overall finding and recommendation:

The IRS does not have the plans or resources needed to recover from disasters or failures at many major locations. The IRS also lacks adequate testing procedures to ensure that computer data back-up files and other necessary resources will be available in the event of a disaster.

We recommended that IRS management develop an overall schedule to ensure completion of disaster recovery and business resumption plans, as well as provide guidelines for regular testing to make sure resources, such as data files, are available and plans can be implemented.

Type of Outcome Measures:

- Reduction of taxpayer burden - potential
- Protection of resources - potential

Value of the Benefit:

Completion of Disaster Recovery and Business Resumption Plans

With adequate plans in place, the IRS would be able to more quickly and efficiently restore operations and service at 30 locations.

Facilities Which Need to Complete Disaster Recovery/Business Resumption Plans	
Computing Centers	1
Service Centers	4
District Offices	25

The five service centers that did not have electrical generators at the time of our review are also vulnerable to interruptions in processing for the duration of any failure. Once generators are installed at these service centers, they will be able to continue processing in the event of a power failure.

Delays in restoring operations and service at any major IRS facility would be very costly to the government. For example, salary costs alone at just one service center for one week are approximately $1.3 million. That one service center on an average weekly basis also performs the following actions:

- Processes 530,000 tax returns.
- Issues 206,000 refunds.
- Collects approximately $126 million in additional tax payments.

Storing Data Files at Off-site Locations

Once the IRS stores all necessary data files off-site so that the data are available after a disaster or failure, it will be able to restore at least 105 mainframe and minicomputer data files and two masterfiles (the Debtor and Payer Masterfiles) that it would not otherwise have been able to restore.

Type And Number of Computer Data Files Not Stored Off-site at the Time of Our Review	
Masterfiles	2
Mainframe computer files	80
Minicomputer files	25

Not having these files would affect nearly every aspect of IRS operations, including processing of tax returns, payments, and refunds and providing taxpayer service. For example, if a disaster or failure caused the destruction of security profile data on the Security and Communication System at one computing center, half of all IRS employees who need access to taxpayer accounts for processing and taxpayer service would lose this access for an extended period of time.

Data are one of the IRS' most important resources. If data are lost or destroyed, the IRS may have to request taxpayers and institutions to provide the same information again and it would have to reprocess the data. In addition, any information the IRS could not reconstruct or obtain would result in permanently lost data and potentially lost revenue.

Methodology Used to Measure the Reported Benefits:

We included information from on-site visits, as well as survey information provided by each major location, in determining the number of IRS locations that still need to complete Disaster Recovery or Business Resumption plans and those that need electrical generators. The number of data files we noted as not being stored off-site are only those maintained by the IRS sites we visited. Other sites may also have important data files that are not stored off-site.

Appendix V

Management's Response to the Draft Report

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

COMMISSIONER

December 23, 1999

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Charles O. Rossotti
Commissioner of Internal Revenue

SUBJECT: Draft Audit Report – The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans

We have reviewed the Treasury Inspector General for Tax Administration (TIGTA) draft report on disaster recovery and business resumption plans, and we agree with many of your proposed recommendations. As you know, the Internal Revenue Service (IRS) initiated efforts to improve security almost 3 years ago. Since then, many corrective actions have been initiated, including actions to enhance the IRS' disaster recovery capabilities. Many of the issues raised in your draft report have already been addressed or were being addressed during your review. To date, corrective actions for six of the twelve issues have been completed. The remaining issues and actions were discussed with your staff during the review. However, the draft report does not reflect the Service's position on important issues including backup generator purchases and alternative space arrangements.

Besides the actions being taken by the IRS to enhance its disaster recovery and continuity of operations capabilities, it is also important to acknowledge that other safeguards are in place that will help to minimize the effects of a disaster or major system failure. For example, the recommendation to maintain service center operations using generators fails to address both the reason that generators are used at our centers and the high cost of increasing generator backup capacity. As discussed with your staff, generators and battery backup systems are used to ensure the safe shutdown of our mainframe computers—they were not acquired to support service center operations. With mainframe consolidation, which is moving mainframe computers out of the service centers, the need for generators has lessened because our battery backup systems should assure this safe shutdown at service centers. This letter's "Limited Official Use" enclosure includes the IRS' more-detailed positions on such items.

As previously discussed with your staff, we do not concur with your benefits analysis. The IRS strategy to reroute returns, remittances, and calls to unaffected operational customer service or return processing locations was not covered in the report. These actions would significantly mitigate the negative impact associated with an extended outage at one of these facilities. Management established this strategy to avoid the magnitude of revenue, tax return processing and customer service losses projected in your report.

As is the case with U.S. General Accounting Office reports which have also delineated specific weaknesses and vulnerabilities with specific facilities and facility types, we are asking that this report be labeled and protected as "Limited Official Use." This is because its distribution increases the risks associated with disclosing the identified weaknesses and vulnerabilities. We recommend that your staff work directly with the Director of the Office of Security Evaluations & Oversight, who can be contacted at 202-283-4500, to discuss the limited distribution of the report and to agree on a redacted version of the report that can be released to the public. In this regard, future draft reports addressing disaster recovery and other security weaknesses should be labeled and protected as "Limited Official Use" until the Director of the Office of Security Evaluations & Oversight has assessed it for potential risks associated with the disclosure of the weaknesses and vulnerabilities.

As requested, this letter is not a "Limited Official Use" document. Its enclosure, however, is a "Limited Official Use" document, so that we could adequately address the sensitive weaknesses and vulnerabilities reported by TIGTA. Accordingly, we have designated the enclosure and your draft report as "Limited Official Use" documents. In this regard, they should be restricted to only officials with a "need to know" and should not be released publicly.

In closing, thank you for assisting our efforts to improve the IRS' disaster recovery capabilities. Please include a copy of this response and its enclosure in your "Limited Official Use" version of your final report. If you have any questions, or if you would like to discuss this response in more detail, please contact, Len Baptiste, Director of the Office of Security and Privacy Oversight at 202-622-8910.

Attachment

Responses to TIGTA's November 4, 1999 Draft Audit Report, entitled The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans

The following material must be protected as "LIMITED OFFICIAL USE" and also warrants protection under the Freedom of Information Act due to the sensitive information contained in the responses to your recommendations.

Recommendation # 1

The Office of Security Standards and Evaluation (SSE) in coordination with other IRS offices should develop an overall IRS plan, which includes standards and a schedule for completion of disaster recovery and business resumption plans. The SSE should monitor completion of plans for each major IRS location.

Assessment of Cause

The IRS must make sure that plans are developed and have all the important elements. Requiring plans to be in place within a specific time frame will help in setting the priority of this important task. For example, all 10 service centers were given specific dates for completing business resumption plans by the EOSCO and all service centers completed plans. However, the Assistant Commissioner (Service Center Operations) (sic) has not given service centers specific dates for completion of disaster recovery plans and four service centers have yet to complete these plans.

Corrective Action

In its oversight and guidance role, SSE—which is now called the Office of Security & Privacy Oversight (SPO)—will continue coordinating with the organizations that are responsible for the plans and working with the affected organizations to complete the individual and overall plans. SPO's Office Of Security Evaluations & Oversight will also assist in developing standards and a schedule for completing the disaster recovery and business resumption plans.

The IRS has taken several steps towards standardization of the business continuity plans. Through the Executive Officer for Service Center Operations (EOSCO), the Andover Service Center developed and distributed a prototype business resumption plan for customization by each service center. Northeast Region developed a prototype plan for district office business resumption that was distributed to all District Offices. SPO's Office Of Security Evaluations & Oversight installed a generic version of the Fresno Service Center disaster recovery plan at each service center for customization to their individual site. The Office of Security Evaluations & Oversight also distributed the Comprehensive Business Recovery planning software to each site and provided training to the identified staff at the sites.

Summary of Action for ITC

The Office Of Security Evaluations & Oversight will coordinate with the responsible officials (see below) and will issue a memorandum for the completion of an overall IRS plan, which will include standards and a schedule for completion of disaster recovery and business resumption plans to include minicomputer applications (See Recommendation #10).

Implementation Date

December 2000

Responsible Officials

Assistant Commissioner (Forms & Submission Processing)
Assistant Commissioner (Customer Service)
Assistant Commissioner (National Operations)
Executive Officer for Service Center Operations
Director, IS Service Center Operations
Directors, District Offices (33)
Director, IS Field Operations

Recommendation # 2

The Chief Operations Officer and the Chief Information Officer should include disaster recovery and business resumption in the performance rating process for senior management and information officers at computing centers, service centers, and districts.

Assessment Of Cause

Despite the importance of having both business and disaster recovery plans at each major facility, many critical IRS facilities lack either one or both types of plans. The IRS must make sure that plans are developed and have all the important elements. Overall, IRS management has not emphasized timely plan development or assigned responsibilities to one office nationally for plan completion. Requiring plans to be in place within a specific time frame will help in setting the priority of this important task. For example, all 10 service centers were given specific dates for completing business resumption plans by the EOSCO and all service centers completed plans. However, the Assistant Commissioner (Service Center Operations) has not given service centers specific dates for completion of disaster recovery plans and four service centers have yet to complete these plans.

Corrective Action

SPO will keep the COO and CIO apprised of the efforts by responsible senior managers and information officers to implement disaster recovery and business resumption plans. These efforts will be factored in the performance rating process.

Summary of Action for ITC:

The COO and CIO will factor in the efforts of responsible senior managers and information officers to implement disaster recovery and business resumption during the performance rating process.

Implementation Date

October 2000

Responsible Official

Chief Operations Officer
Chief Information Officer
Director, Security and Privacy Oversight

Recommendation # 3

The Assistant Commissioner (Support Services) should purchase generators for service centers that do not have adequate generator capacity or establish agreements to lease generators during times of need.

Assessment Of Cause

Five service centers did not have electrical generators needed to continue operations in the event of a power outage (one of these did have a dual power source and may be able to continue operations if the outage affected only one source).

Corrective Action

As discussed with the audit staff, we will continue to evaluate the business need associated with acquiring emergency generator systems in our Atlanta, Cincinnati, Fresno, Kansas City, and Philadelphia Service Centers. However, this is not a high priority item given its high cost and limited benefits. In this regard, mainframe consolidation has reduced the demand on the Centers' battery backup capabilities, which in turn provide enough capacity for an orderly shutdown of the systems. It is important note, that the generators in our service

centers were acquired to support major computer systems—not service center operations. Acquiring costly generators to run an entire Service Center would significantly drive up costs, including costs associated with building systems upgrades. For example, significant space would have to be provided for the generators along with a secure and safe area for storing large quantities of fuel. In essence, the IRS would be in the power plant business. Electrical distribution systems would probably require extensive retrofitting to accommodate the new power requirements, which would be needed to keep the computers running and to power building support systems such as lighting, heating, ventilation, air conditioning and security systems.

Whereas, the IRS agrees that essential functions need to continue during and after power outages, it does not believe that a big investment in large backup generator systems is necessarily the best answer for all its facilities. The recommendation is not based on identified government and industry guidelines, which do not typically recommend that disaster recovery and business resumption plans be bound to specific types of equipment and supplies that can be used to restore important information systems and business processes. Instead, approaches need to be based on practical considerations including feasibility and cost. For example, with 10 service centers the IRS is able to minimize the effects of a power outage by rerouting critical work to unaffected centers. At this time, we believe that this is a reasonable and responsible approach. However, as workloads and systems continue to change across the IRS, we will continue to evaluate the business need associated with acquiring emergency generator systems.

Summary of Action for ITC

Current conditions cannot support a business case to implement the recommendation, which is being closed.

Implementation Date

N/A

Responsible Official

N/A

Recommendation # 4

The Assistant Commissioner (Support Services) should develop an IRS-wide memorandum of understanding with the General Services Administration which specifies service center alternate space needs in the event of a disaster.

Assessment Of Cause

TIGTA reviewed plans at five sites and found that these plans did not have all necessary information and did not cover all the important information systems and resources. Two service centers and a district office did not provide for alternate space needs in case of disaster.

Corrective Action

Whereas, this recommendation appears to be a good idea, it is not clear that it is a high priority for the IRS to pursue at this time, given other priorities and the low risk, if any, associated with not implementing this recommendation. In natural disasters like hurricanes and earthquakes, an alternative site may not be feasible, especially if the site is also damaged or destroyed. In a scenario, where a facility has been significantly destroyed, there may not be anything available from the original facilities to support a recovery process. We agree that having alternate space available is an approach that can work for some disasters, but it does not always appear to be the most appropriate or cost effective strategy for the Service. Again, the IRS has the ability to reroute work and to move resources into a disaster area—like we have done in the past—to continue operations and assist victims. Whereas it is important to have backup facilities available for critical systems and operations during a disaster, with over 1,000 facilities we currently have backup capabilities to handle the workload of our facilities ourselves. We also can quickly assess the damage and mobilize the specific resources needed to disaster areas. In this regard, the IRS is ready to procure alternate space and resources if needed and our plans address doing this following emergencies. We do not see the cost effectiveness of relying on prior commitments that would be necessary for all types of emergencies. The leasing of emergency space needs to be done in an appropriate and cost effective manner, with our primary focus on restoring essential functions within the constraints of the Service's limited resources.

Summary of Action for ITC

Current conditions cannot support a business case to implement the recommendation, which is being closed.

Implementation Date

N/A

Responsible Official

N/A

Recommendation # 5

Martinsburg Computing Center management should ensure personnel up-date the Payer Master file disaster recovery plan to include files needed for recovery prior to the first update. Personnel should ensure these files are sent offsite beginning in the year 2000.

Assessment Of Cause

Backup data files stored offsite are critical to disaster recovery planning. If backup data files are not taken offsite, important tax information could be damaged if a disaster occurred at a primary facility. The IRS was not always storing important data files offsite. The Payer Master file must be reestablished each year. However, the data files created when reestablishing the Payer Master file were not stored offsite. These files are necessary to restore the Payer Master file until current year processing begins in approximately May of each year. Martinsburg personnel were unaware files were not being stored offsite because disaster recovery tests were conducted after the Payer Master file was restored. Once TIGTA found this problem, Martinsburg personnel identified the backup data files that are needed to recover the Payer Master file for January through April and they plan to send the files offsite beginning in January 2000.

Corrective Action

File Identification/Program Updates have been completed. The Martinsburg Computing Center identified the January through May data files that are needed to create the current year Payer Master file. The file names will be provided to the Master File Scheduling Section for program updates to ensure creation of a backup copy for offsite storage purposes. The backup file names will then be added to the Martinsburg Computing Center Payer Master file portion of the Disaster Recovery Plan. A review of the files will be made during the annual plan review to add additional files or correct existing files. The identified files will be stored offsite during the January through May timeframe. Martinsburg Computing Center personnel will review the Martinsburg Computing Center Offsite Security Storage reports in March 2000, to ensure files needed for creation of the Payer Master file are being stored offsite with the correct retention. The status of this action will be reported monthly to the Chief, Program Planning Division

Implementation Dates

Files will be stored offsite starting in January 2000.

Responsible Official

Director, Martinsburg Computing Center

Summary of Action for ITC

Identify the data files needed as input to create the current year Payer Master file. Provide file names to the Master File Scheduling Section for program updates to ensure creation of backup copy for offsite storage. Backup file names will be added to the Martinsburg Computing Center Payer Master file portion of the Disaster Recovery Plan. Review of the files will be made during annual plan review to add additional files or correct existing files. Identified files will be stored offsite during the January through May time frame. Personnel will review the Martinsburg Computing Center's Offsite Security Storage reports in March 2000, to ensure files needed for creation of Payer Master file are stored offsite with correct retention.

Recommendation # 5

The Assistant Commissioner (National Operations) should update procedures to ensure that information systems programmers notify computing centers of program changes which affect offsite backup files. Programmers should identify new file names so that the proper files are sent offsite when program changes are made.

Assessment of Cause

Martinsburg Computing Center personnel determined that the Debtor Master file was not stored offsite when they were preparing for the annual disaster recovery test. This happened because of a redesign of the database that was not reflected in the backup procedures. In addition, computer programmers do not notify computing center personnel when changes are made to databases or programs, which affect files, needed to be stored offsite. As a result, computing center personnel responsible for sending files offsite must try to identify these files by reviewing all program changes.

Corrective Action

National Office and Computing Center staff worked together to develop procedures to correct this situation. These procedures went into effect September 1999 and will be included in the next revision of the Information Systems Operations Support Handbook IRM 2.2.8

Implementation Date

September 10, 1999 (Corrected)

Summary of Action for ITC

Completed - National Office and Computing Center staff worked together to develop procedures to correct this situation. These procedures went into effect September 1999 and will be included in the next revision of the Information Systems Operations Support Handbook IRM 2.2.8

Responsible Official

Director, Martinsburg Computing Center

Recommendation # 7

The Assistant Commissioner (National Operations) should ensure computing centers maintain security profile data for all 10 service centers on line.

Assessment of Cause

Security and Communications System (SACS) - controls all IRS employee on-line access to taxpayer accounts. Consolidation of SACS is complete for all 10 service centers. As consolidation is completed (two service centers in 1999 and five in 2000), computing centers' disaster recovery and offsite backup files become increasingly important. In case of failure, the IRS could lose mainframe computer systems for five service centers at a time. To avoid this potential, the IRS plans to have computing centers back up each other for disaster recovery purposes, which should enable the 5 affected service centers to recover within 36 hours. TIGTA reviewed offsite backup files for IRS consolidated mainframe systems at both computing centers. The Martinsburg Computing Center was not sending any files for consolidated mainframe systems off site and the Tennessee Computing Center was only sending 38 of 118 needed database files (32 percent) offsite

One of the important files that was not sent offsite contained SACS security profile data, which controls all IRS employees' access to taxpayer information. At the time of our review, the Martinsburg and Tennessee Computing Centers each had security profile data for its five service centers. Since consolidation for the SACS system is complete, the fact that neither computing center was storing security profile data offsite created the risk of having half of all IRS employees without access to taxpayer information and unable to input information, if a disaster occurred. To be better prepared for a disaster, computing centers should maintain the security profile data for all 10 service centers on line.

Corrective Action

This weakness has been mitigated by revising the disaster recovery plan for SACS that now requires that the computing centers back up the SACS database nightly and electronically transmit the data to each other. The data is then stored on tape cartridges in automated tape libraries (tape silos) at each reciprocating computing center.

Implementation Date

July 1999 (Actions to respond to the recommendation were completed. The SACS procedures calling for daily backup were revised and implemented.)

Responsible Official

Director Enterprise Operations

Summary of Action for ITC

The recommendation was closed. The procedures calling for daily back up were revised and implemented July 1999.

Recommendation # 8

Computing Center management should establish specific procedures to implement disaster recovery offsite procedures, follow specific backup procedures for consolidated mainframe systems, and take all disaster recovery backup files offsite.

Assessment of Cause

At the time TIGTA completed this audit, the disaster recovery save and restore procedures and the tape storage plans for the consolidated platforms at the two computing centers were still being revised and had not been fully implemented.

Corrective Action

Each center now has tested its daily and weekly disaster recovery save procedures for the back up of its consolidated mainframe data files. The computing centers are currently following these procedures.

Currently each center has implemented an offsite storage policy for disaster recovery backups. This shipment included tapes that were created over the weekend and represent a disaster recovery backup for a full weekend. Incremental backups are made each night. The Tennessee Computing Center currently ships it disaster recovery backups daily.

Each center creates a shipping log for the tapes that are shipped and stored off site. Computer operators and computing center management can review copies of those logs each day to validate the fact that the center's disaster recovery tapes were moved to the off site location.

Implementation Date

November 1999 (Completed)

Responsible Officials

Director, Martinsburg Computing Center
Director, Tennessee Computing Center

Summary of Action for ITC

The recommendation was closed. Actions were completed at the two centers in June and November 1999.

Recommendation # 9

Monthly, Computing Center and Service Center management should verify that all critical system files are backed up and sent offsite.

Assessment of Cause

The IRS needs to establish procedures to verify all needed backup files for critical systems are being completed and stored offsite monthly to avoid missing files in the event of a disaster.

Corrective Action

The Computing and Service Centers will continue to perform annual inventories of offsite files. The Centers will conduct a review of existing procedures to determine actions that can be taken to improve the verification process. This review will include assessing the feasibility of monthly verifications.

Implementation Date

March 2000

Responsible Official

Director, Martinsburg Computing Center
Director, Tennessee Computing Center
Director, Service Center Operations

Recommendation # 10

The Assistant Commissioner (National Operations), in coordination with SSE, should develop a consolidated listing of offsite storage requirements for minicomputer applications

Assessment of Cause

The IRS does not maintain a consolidated listing of minicomputer applications with specific requirements for offsite storage. The IRS does have general guidance (not listed by specific application) in the IRM for all "multi-user systems" and guidance for each individual system in contingency plans. However, this information is not consolidated into one document that could be used by tape librarians or system administrators to easily verify all backup files for minicomputer systems are being stored offsite.

Without procedures for offsite storage, minicomputer data could be lost if a disaster occurred. After TIGTA identified this problem, Tennessee Computing Center personnel and Andover Service Center personnel began storing needed minicomputer backup files offsite.

Corrective Action

The IRS currently requires a Technical Contingency Planning Document for all systems requiring security certification. This Technical Contingency Planning Document is used as the basis for providing the necessary documentation for listing of offsite storage requirements for minicomputer applications. However, assurance that minicomputer system recovery requirements are met in disaster recovery plans will be reinforced as part of the corrective action for Recommendation #1. In addition, the Office of Security Evaluations & Oversight will include ongoing verification of this requirement in its site reviews. These reviews will verify the accuracy of information within the Technical Contingency Planning Document with offsite storage locations.

Summary of Action for ITC

Assurance that minicomputer system recovery requirements are met in disaster recovery plans will be reinforced as part of the corrective action for Recommendation #1. In addition, the Office of Security Evaluations & Oversight will include ongoing verification of this requirement in its site reviews. These reviews will verify the accuracy of information within the Technical Contingency Planning Document and offsite storage for minicomputer applications.

Implementation Date

Completed

Responsible Official

Director, Enterprise Operations
Director, IS Service Center Operations
Director, Field Operations

Recommendation # 11

The Office of Security Standards and Evaluation should develop guidance to assist managers in developing sufficient plan testing and maintenance procedures. This guidance should include, but not be limited to:

- Ensuring tests are based on offsite data or other resources that would reasonably be available in the event of a disaster.
- Ensuring any assumptions included in the test are reasonable (e.g., availability of information systems).
- Verifying that alternate support service organizations can provide necessary services or facilities.
- Ensuring tests are of sufficient depth to identify plan limitations or areas needing clarification or revision.

Assessment of Cause

Disaster recovery and business resumption plans must be tested and updated to ensure plans remain current and complete. Otherwise, plans can quickly become obsolete, particularly in a changing business operations and information systems environment. Tests must be sufficient to identify:

- Weaknesses in each plan's procedures and
- Missing resources needed to implement these plans.

Additionally, maintenance procedures must include provisions for:

- Incorporating necessary modifications discovered during testing and
- Continuous plan updates as IRS processes or personnel change.

Corrective Action

The Office of Security Evaluations & Oversight has developed and issued "Procedural Guide to Exercise Plans", a guide to disaster recovery plan testing. IRM 2.1.10.6 identifies the Head of Office as being responsible for testing of the business continuity plans. The Office of Security Evaluations & Oversight through its oversight responsibilities will ensure that tests are conducted. It will also monitor their results.

Implementation Date

November 15, 1999 (Closed)

Summary of Action for ITC

The Office of Security Evaluations & Oversight will ensure that tests are conducted in adherence to the Procedural Guide to Exercise Plans. It will also oversee the results.

Responsible Official

Director, Security Evaluation & Oversight

Recommendation # 12

The Office of Security Standards and Evaluation should develop consolidated mainframe systems test plans that test disaster recovery at both computing centers using only backup files stored offsite.

Assessment of Cause

The Martinsburg Computing Center has not developed a disaster recovery plan for consolidated mainframe systems, nor has it approved and tested a business resumption plan.

The Tennessee Computing Center's plans and testing are not adequate because it has not developed (a) an incident management plan to coordinate activities of the center's functions, (b) a disaster recovery plan for minicomputer systems, or (c) a business resumption plan.

The IRS performed one disaster recovery test of its consolidated mainframe systems in September 1998 at the Tennessee Computing Center. This test was performed to demonstrate that the Martinsburg and Tennessee Computing Centers could act as recovery sites for each other. However, that test did not use offsite backup files that were being regularly prepared under normal operations, but instead included special procedures to ensure all necessary data files were available. . [NOTE: This information is incorrectly reported. The test was at the Martinsburg Computing Center for the recovery of the Tennessee Computing Center consolidated platform. The scope of this test was to determine if the operational procedures for system recovery, including file identification for offsite storage was complete. Subsequent tests, as noted below, did utilize an offsite tape inventory for test execution.]

Corrective Action

The disaster recovery test of the consolidated mainframe systems conducted at the Martinsburg Computing Center in June 1999, was developed by the Office Of Security Evaluations & Oversight and included the use of backup files from offsite. Future tests developed by the Office Of Security Evaluations & Oversight will continue to use files from offsite storage. When the operational responsibility for the tests are moved to the computing centers, the Office Of Security Evaluations & Oversight will ensure that the tests are conducted using files from offsite storage.

The Office of Security Evaluations & Oversight hired three analysts in March 1999. Their oversight responsibility includes assisting in the development of test plans, which will include the use of files from offsite storage.

Implementation Date

June 1999. This recommendation is closed.

Summary of Action for ITC

IRS is conducting these tests using files from offsite storage.

Responsible Officials

Director, Enterprise Operations
Director, IS Service Center Operations