The Security and Performance of Electronic Tax Return Processing Should Be Improved to Meet Future Goals

June 2000

Reference Number: 2000-20-095

June 14, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
                Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The Security and Performance of Electronic
                Tax Return Processing Should Be Improved to Meet Future
                Goals

This report presents the results of our review of the receipt and processing of electronic tax returns for the 2000 Filing Season, which was consolidated at two locations. In addition, we evaluated the Internal Revenue Service's (IRS) corrective actions on selected issues that were included in a previous audit report.

In summary, we found that the Electronic Management System (EMS) had sufficient communications and processing capacity to receive and store expected tax return volumes during the 2000 Filing Season. However, the Chief Information Officer (CIO) should implement performance and capacity management planning to determine the processing efficiency and future capacity needed to achieve the IRS' goal of receiving 80 percent of tax returns electronically by 2007. In addition, the CIO needs to implement adequate EMS security procedures and project management controls, and complete and test the disaster recovery plan.

We issued a draft of this report to IRS management on May 1, 2000, with a May 31, 2000, response period. However, management's response was not available as of the date this report was released.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions, or your staff may call Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

The Security and Performance of Electronic Tax Return Processing Should Be Improved to Meet Future Goals

Table of Contents

Executive Summary

The Electronic Management System (EMS) is the Internal Revenue Service's (IRS) primary system for receiving electronic tax returns from trading partners.[1] Through April 17, 2000, the EMS received approximately 41 million individual federal and state income tax returns, about 28 percent more returns than in the 1999 Filing Season.

The overall objective of this review was to evaluate the EMS' readiness to process tax returns for the 2000 Filing Season. In addition, we evaluated the IRS' corrective actions on the remote access security policy and security administration issues that were included in the previous audit report, *Evaluation of the Service's Electronic Management System* (Reference Number 074502, dated July 28, 1997). Early in the 2000 Filing Season, we discussed the issues in this report with representatives of the EMS Project Office (EMSPO) so that corrective actions could begin.

Results

During 1999, the IRS assigned a new Project Manager to the EMSPO, acquired hardware and telecommunication links, and revised EMS computer programs and procedures to consolidate the receipt of electronic tax returns at the Austin Service Center (AUSC)[2] and Tennessee Computing Center[3] EMS locations. The consolidated EMS had sufficient telecommunication and processing capacity to receive and store expected tax return volumes during the 2000 Filing Season. However, the following items should be addressed to protect tax returns from unauthorized disclosure and to ensure that tax returns are timely and efficiently processed.

---

[1] For purposes of this report, a "trading partner" is anyone who transmits electronic tax returns to the IRS. This includes tax return preparers and Online Service Providers who provide taxpayers a subscription service to prepare and file their own electronic tax returns.

[2] Service centers are the data input arm of the IRS. Service center personnel input paper tax returns and related tax information, correct errors on paper and electronic tax returns and documents, and forward the data to the computing centers for analysis and posting to taxpayer accounts.

[3] Computing centers house the mainframe tax processing computers that validate tax returns and post the information to taxpayer accounts.

Electronic Management System Processing Should Be Evaluated and Changes Planned

The IRS' *Modernization Blueprint* is currently being revised, but how and when the current EMS will complete its transition to the modernized computer processing environment is not known. In the mean time, the IRS is continuing its marketing and development efforts to significantly increase electronic tax return volumes in order to achieve its goal of receiving 80 percent of tax returns electronically by 2007.

The EMSPO did not have a performance and capacity management plan to determine whether the existing EMS could effectively process anticipated volumes. Stress and integration tests and a capacity assessment completed in 1999 identified risks that the EMS may not have the capacity needed for future volumes.

In addition, the EMS operations could be more efficient. Continuing to locate the EMS at AUSC is not consistent with the IRS' consolidated mainframe tax processing environment. The IRS will need to maintain the current high capacity telecommunication lines between the AUSC and the Martinsburg Computing Center (MCC) and to encrypt tax return transmissions between the two locations. The result will be higher telecommunication costs and less efficient processing than if the AUSC EMS were located at the MCC.

Electronic Transmissions of Tax Returns and Related Tax Information Can Be Better Protected From Unauthorized Disclosure

Most electronic tax returns are transmitted over public telephone and data communication lines between trading partners and the IRS, but the IRS has not implemented encryption procedures for these transmissions. Improved security for electronic tax return transmissions would help protect over 41 million tax returns from being read or altered by unauthorized users.

Security Administration Procedures for Electronic Tax Information Can Be Improved

An EMS security risk assessment report and our audit results showed that the EMS is vulnerable to unauthorized accesses. The EMS computer programs did not require contractors to use smartcards[4] to access the EMS from remote locations to ensure that the accesses were authorized and secure. In addition, the EMSPO had not established a procedure to manage and control the smartcards, including separating custody of the unissued smartcards from EMS computer program maintenance duties.

---

[4] A "smartcard" is a small electronic device about the size of a credit card that verifies the user's identification (authentication) and encrypts the user's transmission.

Electronic Management System Project Management Controls Can Be Improved

The EMSPO did not effectively use project management techniques to ensure timely and effective testing of all system components, and there is no evidence that problems which could have affected the filing season were raised to the IRS Filing Season Readiness Executive Steering Committee.[5] For example, high capacity telecommunication lines needed for the 2000 Filing Season were not installed timely, but this matter was not raised to the IRS Filing Season Readiness Executive Steering Committee. In addition, the EMSPO had assigned a contractor the task of maintaining project planning documentation. However, the EMSPO did not have copies of this documentation, which would have assisted its oversight of the project.

The Electronic Management System Disaster Recovery Plan Should Be Completed and a Recovery Exercise Conducted

The EMS disaster recovery plans have not been updated and tested since 1997. If normal processing at one EMS site is lost, a slow recovery or insufficient processing capacity at the alternate site could delay taxpayers' tax refunds and IRS tax return processing.

Summary of Recommendations

The Chief Information Officer (CIO) should implement performance and capacity management planning and evaluate processing efficiency to determine future EMS computer needs. Also, the CIO should improve the security provided electronic tax returns and tax information during transmissions, improve the security administration at the EMS locations, continue to improve EMS project management controls, and complete and test the disaster recovery plan.

Management's Response: We issued a draft of this report to IRS management on May 1, 2000, with a May 31, 2000, response period. However, management's response was not available as of the date this report was released.

---

[5] The Filing Season Readiness Executive Steering Committee consists of senior IRS management and is chartered to oversee preparations for future tax filing seasons.

Objective and Scope

The overall objective of this review was to evaluate the EMS' readiness to process tax returns for the 2000 Filing Season.

The overall objective of this review was to evaluate the Electronic Management System's (EMS) readiness to process tax returns for the 2000 Filing Season. In addition, we evaluated the Internal Revenue Service's (IRS) corrective actions on the remote access security policy and security administration issues that were included in a previous audit report, *Evaluation of the Service's Electronic Management System* (Reference Number 074502, dated July 28, 1997).

Audit work was performed between December 1999 and January 2000 at the IRS National Office in New Carrollton, Maryland and the Tennessee Computing Center (TCC)[1] in Memphis, Tennessee. We interviewed key personnel and reviewed relevant documentation. This audit was performed in accordance with *Government Auditing Standards*.

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

Background

The EMS is the IRS' primary system for receiving electronic tax returns from trading partners.[2] The EMS also validates and routes these tax returns to the IRS' mainframe tax processing computers and stores acknowledgments for trading partners and state tax returns for state tax agencies. An acknowledgment tells

---

[1] Computing centers house the IRS' mainframe computers that validate tax returns and post the information to taxpayer accounts.

[2] For purposes of this report, a "trading partner" is anyone who transmits electronic tax returns to the IRS. This includes tax return preparers and Online Service Providers who provide taxpayers a subscription service to prepare and file their own electronic tax returns.

the taxpayer that his/her electronic tax return was accepted or rejected by the IRS and, if rejected, explains why.

Through April 17, 2000, the EMS received approximately 41 million electronic tax returns.

Through April 17, 2000, the EMS received and processed 29.6 million individual federal income tax returns (not including 5 million TeleFile returns) and 11.6 million state income tax returns. This is about 28 percent more returns than were received in the 1999 Filing Season.

The IRS Restructuring and Reform Act of 1998 (RRA 98), Pub. L. No. 105-206, 112 Stat 685, requires the IRS to receive 80 percent of all tax returns and information electronically by 2007. The IRS' Electronic Tax Administration (ETA) strategic plan, *A Strategy for Growth*, proposes to improve electronic tax processing by consolidating processing operations at fewer sites.

In November 1999, the IRS reduced the number of locations that receive electronic tax returns from five service centers to the AUSC and TCC EMS locations.

Until November 1999, trading partners electronically transmitted tax returns to five IRS service centers.[3] Since then, the EMS located at the Austin Service Center (AUSC) and the TCC have received all electronic tax returns from trading partners.

Results

In March 1999, the IRS initiated efforts to consolidate the receipt of all electronic tax returns on the EMS located at the AUSC and TCC. In May 1999, the IRS assigned a new EMS Project Manager, with primary responsibility for completing the consolidation and ensuring that the EMS could timely and accurately process all electronic tax returns. Before the 2000 Filing Season started, the EMSPO, its contractors, and other IRS functions:

---

[3] Service centers are the data input arm of the IRS. Service center personnel input paper tax returns and related tax information, correct errors on paper and electronic tax returns and documents, and forward the data to the computing centers for analysis and posting to taxpayer accounts.

- Acquired and installed additional hardware and telecommunication lines.

- Revised the existing EMS and IRS mainframe computer tax return processing programs.

- Revised the EMS Help Desk computer process and procedures previously used only at the AUSC and expanded their use to all locations.

The EMS had sufficient capacity to process tax return volumes expected in 2000. However, the IRS should improve EMS processing in several areas.

The consolidated EMS had sufficient telecommunication and processing capacity to receive and store expected tax return volumes during the 2000 Filing Season. In addition, the EMS consolidation did not significantly affect the IRS' trading partners and state tax agencies, as they were required only to change the telephone number that they use to transmit tax returns. However, the IRS should improve EMS processing in the following areas:

- The performance capabilities of the EMS have not been evaluated to ensure that projected electronic tax return volumes can be timely and efficiently processed until replaced by the modernized computer environment.

- Electronic tax return and tax information transmissions are not encrypted and could result in unauthorized disclosures.

- Security administration procedures that could prevent and detect unauthorized EMS accesses and computer program changes were not properly implemented.

- Project management controls did not timely identify and effectively correct performance problems that could delay tax return processing and allow unauthorized access to the IRS mainframe computers.

- The EMS disaster recovery plan was not completed, and a recovery exercise was not conducted to help assure a prompt recovery from a significant processing interruption.

The follow-up review of the prior audit report recommendations determined that the previously reported non-compliance with the IRS' remote access security policy was corrected in the current IRS security procedures. The IRS' corrective actions on the previously reported security administration weaknesses included improving the audit trails to record all required information about events, establishing a control to ensure that the audit trail files did not exceed the capacity of the tapes, and locking out users who had not accessed the EMS within a specified period.

Early in the 2000 Filing Season, we discussed the issues we identified with representatives of the EMS Project Office (EMSPO) so that corrective actions could begin.

Electronic Management System Processing Should Be Evaluated and Changes Planned

The IRS' *Modernization Blueprint* is currently being revised, but how and when the current EMS will complete its transition to the modernized computer processing environment is not known. In the meantime, the ETA continues its efforts to significantly increase electronic tax return volumes. It is marketing electronic filing, adding tax forms and schedules that can be filed electronically, and expanding the use of technology to simplify electronic filing.

The EMSPO has not initiated performance and capacity testing to determine whether the EMS can effectively process future anticipated tax return volumes.

The IRS has established a capacity planning and management function to assess the ability of systems such as the EMS to keep pace with business requirements. However, the EMSPO did not have a performance and capacity management plan to determine whether the existing EMS could effectively process anticipated volumes. The EMS stress and telecommunication integration tests, conducted in December 1999 and January 2000, indicated limitations on the number of tax returns that the current system will timely and effectively process. Also, an IRS contractor qualified several conclusions in a 1999 EMS processing

and telecommunication capacity assessment report because the AUSC and TCC processing statistics were limited and inconsistent. The contractor recommended that the EMSPO accumulate specific processing statistics to enable in-depth capacity analyses. These analyses should include estimates of the EMS' ability to timely process anticipated volumes, which would form an objective basis for future EMS computer needs.

Locating the EMS at the AUSC is not consistent with the IRS' mainframe tax processing configuration.

In addition, locating the EMS at the AUSC is not consistent with the IRS' mainframe tax processing configuration. The IRS is scheduled to consolidate the mainframe computers that process electronic tax returns at the TCC and MCC by the end of 2000, while all electronic tax returns will be received at the AUSC and TCC. Therefore, the IRS will be required to maintain a high capacity telecommunication link between the AUSC EMS and the MCC mainframe computers, thereby increasing telecommunication costs. The need to encrypt transmissions between the AUSC and MCC will also cause processing inefficiencies.

If performance and capacity tests determine that the EMS does not have the capability to process all electronic tax returns until it has completed transition to the modernized computer environment, the EMSPO will need to make an interim investment decision to acquire additional processing capacity. As part of this decision, the costs and benefits of moving the AUSC EMS computers to the MCC should be considered.

Recommendation

The Chief Information Officer (CIO) should:

1. Evaluate the EMS' performance capability to determine whether it can securely, reliably, and timely process expected future volumes until the EMS completes transition to the modernized computer environment and ensure that interim EMS investment decisions include a cost and benefit analysis for relocating the AUSC EMS computers to the MCC.

Management's Response: We issued a draft of this report to IRS management on May 1, 2000, with a May 31, 2000, response period. However, management's response was not available as of the date this report was released.

Electronic Transmissions of Tax Returns and Related Tax Information Can Be Better Protected From Unauthorized Disclosure

The IRS requires trading partners to ensure the security of all transmitted data. However, it does not require them to encrypt tax return and acknowledgment transmissions.

The ETA strategic plan, *A Strategy for Growth,* indicates that the security of the IRS' electronic systems and the confidentiality of taxpayer information are among the most important responsibilities of the IRS. The IRS issued two Revenue Procedures and other administrative documents to provide guidance to trading partners for electronic filing. The instructions state that trading partners must secure all data transmitted to the IRS but do not provide guidance on how to secure the tax return and acknowledgment transmissions.

Based on opinions from the IRS Office of the Chief Counsel, IRS management has taken the position that the IRS is not legally obligated to protect tax returns until it receives them and, therefore, has not required trading partners to encrypt tax returns being transmitted to the IRS. However, the IRS has mandated other transmission standards that trading partners are required to follow. Since most electronic tax returns are grouped and transmitted in batches over public telephone and leased data communication lines, there is a risk that unauthorized disclosure of tax information could occur during transmissions between trading partners and the IRS. Encryption is an accepted technique that would prevent sensitive information from being read or altered by unauthorized users. The IRS uses encryption for internal transmissions of tax information but has not implemented it for similar transmissions between trading partners, the IRS, and state tax agencies.

To improve security over the 41 million electronic federal and state tax returns that are transmitted to the

IRS and to increase taxpayers' confidence that their tax returns are adequately secured during transmission, additional procedures, including encryption, should be developed and implemented. These procedures would help provide the same level of security over transmissions of returns from trading partners to the IRS as is provided by the IRS in transmitting returns between IRS locations.

Recommendations

The CIO should:

2. Develop and implement improved security standards and procedures, such as encryption, for all electronic tax return transmissions.

3. Integrate the improved procedures for the electronic transmission of tax returns from trading partners into the future IRS modernization architecture.

Security Administration Procedures for Electronic Tax Information Can Be Improved

An EMS security risk assessment and our audit results show that the EMS is vulnerable to unauthorized accesses.

The IRS has established security administration procedures for computer systems that contain tax-related information. These procedures are designed to prevent and detect unauthorized accesses and disclosures. They include: 1) authorized personnel who remotely access IRS systems must use appropriate user authentication and encrypt all transmitted information, 2) access to authentication devices and encryption programs must be controlled, 3) security administration duties must be separated from computer programming and operations duties, and 4) audit trail reports and logs must be reviewed and questionable actions reported to management.

Our audit results showed that the EMS is vulnerable to unauthorized accesses. A December 1999 report on the results of a contractor's review of EMS security over

electronic tax information had the same results. The more significant weaknesses included:

Remote access authentication and encryption procedures (smartcards) were not properly implemented.

- Selected contractor employees access the EMS from remote locations over public telephone networks to maintain the computer programs. They are supposed to use an IRS-supplied authentication and encryption device (smartcard).[4] The smartcard ensures that the access is authorized and the transmission is not tampered with. However, the smartcards were not properly implemented, as:

  - ♦ The EMS security settings did not deny system administrator access to employees who did not use a smartcard to access the EMS from a remote location. The risk assessment identified one contractor who did not install smartcard readers on its computers. The audit determined that this contractor's employees used their assigned user names and passwords to access the EMS over unencrypted public telephone lines. Unencrypted remote transmissions could be vulnerable to interception and tampering that could result in the EMS computer programs being improperly altered or destroyed.

  - ♦ The EMSPO had not established a procedure to manage and control access to the smartcards. The smartcards must be accounted for because they contain the EMS authentication and encryption codes.

  - ♦ Another contractor maintained physical custody of the unissued smartcards and also maintained EMS computer programs. Inadequate separation of these duties could result in the unauthorized use of the smartcards.

---

[4] A "smartcard" is a small electronic device about the size of a credit card that verifies the user's identification (authentication) and encrypts the user's transmission.

The IRS did not effectively implement the procedures that would detect unauthorized accesses so that they can be investigated.

- Security administration procedures were established to collect and review system access reports and audit trail information. However, the IRS did not effectively implement the procedures that would detect unauthorized accesses so that they could be investigated. Security administrators did not review the EMS security reports that were designed to identify unauthorized accesses to the computer systems.

As of January 2000, IRS management had not corrected the weaknesses identified in the security risk assessment. Without strong security controls, there is an increased risk of unauthorized accesses to the EMS computer programs and stored taxpayer information.

Recommendations

The CIO should:

4. Ensure that the EMS security settings require the use of smartcards to access the system from a remote location, that procedures are established to manage and control the smartcards, and that unissued smartcard custody duties are properly separated from computer programming and operations duties.

5. Ensure that EMS security administrators appropriately restrict access to audit trail information and review EMS security reports and audit trails.

Electronic Management System Project Management Controls Can Be Improved

The IRS' system development life cycle guidelines require that project planning documents be prepared and updated to track the status of all planned tasks. These documents serve as a basis for ensuring that all required work is identified, planned for, and completed before new computer systems are implemented. These guidelines also require that all aspects of the system be

tested to determine whether the system is functioning as intended and that any problems be corrected before the system is implemented. Problems that cannot be effectively dealt with at the Project Office level should be elevated to senior IRS management, including multi-functional groups such as the IRS Filing Season Readiness Executive Steering Committee, to assure proper resolution.

EMSPO project oversight did not ensure timely testing of all system components.

The EMSPO properly prepared a project plan and issued Statements of Work[5] to contractors to develop, document, and test the computer hardware and programming changes needed for the 2000 Filing Season. However, EMSPO project oversight did not ensure timely testing of all system components. Also, there is no evidence that problems which could have affected the filing season were raised to the IRS Filing Season Readiness Executive Steering Committee.

Centralization of all electronic tax return receipts at two locations during 1999 required the IRS Telecommunications function to obtain high capacity telecommunication lines between the AUSC EMS and the Ogden Service Center and the MCC[6] mainframe tax processing computers. These lines were originally scheduled for installation in October 1999, but installation was not completed and integration with the EMS was not tested until the second weekend of January 2000. When stress and integration testing was completed, there were indications that peak volume file transfers would take significantly longer than planned and these slow transfers could interfere with other IRS tax processing traffic on this network.

---

[5] A Statement of Work provides requirements and specifications to the contractor about a service or product that the IRS needs and establishes due dates for deliverables (documents or products) and milestones (critical actions).

[6] Until the IRS' mainframe computer consolidation project is completed in 2000, mainframe processing of electronic tax returns will also be conducted at the Austin and Ogden Service Centers.

EMS personnel implemented a different file transfer process to address the performance problems. However, the substitute process bypassed security controls that the contractor evaluated during the EMS security risk assessment. The risk assessment was the basis for the EMS Interim Authority to Operate.[7]

The EMSPO did not have copies of all project planning documentation and did not elevate problems that could have affected the 2000 Filing Season to the Filing Season Readiness Executive Steering Committee.

These problems occurred, in part, because EMSPO personnel had assigned one contractor the task of maintaining overall project planning documentation, but the EMSPO did not have copies of all of this documentation to assist its management oversight of the project. In addition, each contractor prepared periodic status reports for its tasks and held meetings with EMSPO personnel, but the reports and meetings did not identify the performance problems discussed above, determine their cause, or initiate changes to effectively correct the problems. In addition, Information Systems management did not elevate the delayed telecommunication link delivery and testing as a concern to the IRS Filing Season Readiness Executive Steering Committee.

Closer monitoring of project management documentation and tasks to assure all critical items are timely completed and prompt involvement of upper level management in problem areas would help prevent critical delays in the project development and testing process.

Recommendations

The CIO should:

6. Ensure that EMS project management is improved by preparing and maintaining project management documents, including project and test plans, and

---

[7] An Interim Authority to Operate is a memorandum signed by senior IRS managers that permits a system to process tax information while security testing and the certification process are ongoing.

strengthening oversight of the contractors' development and testing of future changes.

7. Assure that critical development or testing delays (e.g., computer program or equipment installation) that could affect tax processing are timely raised to the IRS Filing Season Readiness Executive Steering Committee for resolution.

The Electronic Management System Disaster Recovery Plan Should Be Completed and a Recovery Exercise Conducted

IRS personnel did not complete the EMS disaster recovery plan or conduct a full exercise.

IRS information systems security guidelines require disaster recovery plans to be developed, tested, implemented, and maintained for major computer systems. The plans should be routinely reviewed, tested, and updated to provide for reasonable continuity of information system support and to reduce downtime.

Since 1997, EMS disaster recovery plans have not been updated or tested. The EMSPO identified this situation and began revising the plans in November 1999. EMS and contractor personnel also demonstrated the recovery procedure in early January 2000. However, they did not complete the EMS disaster recovery plan or conduct a full disaster recovery exercise (simulates a recovery using the disaster recovery plan) before the 2000 Filing Season started.

The full disaster recovery exercise was not conducted because the EMSPO, contractor, AUSC, and TCC personnel needed to conduct it were assigned to develop, test, and implement the EMS processing changes that were required for normal tax processing. The EMSPO expects to complete the disaster recovery plan and conduct an exercise by mid-2000.

There is a significant risk that a disaster recovery effort could delay tax return processing.

There is a significant risk that a disaster recovery effort could delay tax return processing as the EMS and associated telecommunication links may not have sufficient capacity to timely transfer all electronic tax

returns to the IRS mainframe tax processing computers. In addition, if normal processing at one EMS site is lost, a slow recovery or insufficient processing capacity at the alternate site could delay taxpayers' tax refunds and IRS tax return processing. A successful recovery plan exercise would provide management a level of assurance that EMS processing could continue at one site if the other site experienced a disaster.

Recommendation

The CIO should:

8. Ensure that the EMS disaster recovery plan is completed and periodic recovery plan exercises are conducted.

Conclusion

The EMS had sufficient telecommunication and processing capacity to receive and store expected tax return volumes during the 2000 Filing Season. However, the CIO should improve the EMS security and project management controls, complete and test the disaster recovery plan, and implement performance and capacity management planning to determine EMS computer needs.

Detailed Objective, Scope, and Methodology

The overall objective of our review was to evaluate the Electronic Management System's (EMS) readiness to process tax returns for the 2000 Filing Season. We also evaluated Internal Revenue Service (IRS) management's corrective actions on security and taxpayer privacy issues that were included in the previous audit report, *Evaluation of the Service's Electronic Management System* (Reference Number 074502, dated July 28, 1997).

I. To determine whether the EMS Project Office (EMSPO) management's oversight activities ensured that the consolidated EMS was effectively tested and critical problems identified by the tests were resolved, we:

   A. Reviewed the EMS operational and capacity test plans and schedules and determined whether tests were conducted in a simulated production environment and included volumes typical of filing season patterns.

   B. Reviewed the EMS operational and capacity test status reports and results and determined whether critical problems encountered during testing were effectively resolved.

   C. Determined whether the EMSPO management's oversight of the completed tests included their certification that the EMS was ready for production.

II. To determine whether EMSPO management's oversight activities ensured that disaster recovery plans were developed and effectively tested and critical problems were resolved, we:

   A. Reviewed the EMS disaster recovery and business resumption plans and determined whether the plans were fully documented, completed prior to the start of the 2000 Filing Season, and contained current information.

   B. Reviewed the EMSPO communications and processing capacity assessments and determined whether the EMS has sufficient redundant capacity to implement the disaster recovery plans.

   C. Reviewed the disaster recovery test plans and results and determined whether the tests were conducted in a simulated production environment and used the production systems and whether any problems encountered during testing were effectively corrected.

III.   To determine whether the EMSPO management's oversight activities ensured that the necessary steps were completed to certify the consolidated EMS' compliance with IRS security requirements and follow-up on the IRS' corrective actions on previous audit recommendations, we:

    A.   Determined whether the EMSPO completed the necessary security certification documentation required to obtain Interim Authority to Operate and whether the documentation complied with security certification guidelines.

    B.   Reviewed the security certification documentation prepared for the consolidated EMS and determined whether the IRS' corrective actions on previous audit recommendations brought the EMS in compliance with:

        1.   The IRS' and Department of the Treasury's security requirements for access to computer systems containing sensitive information.

        2.   The IRS' Secure Dial-In Policy for access to IRS computer systems from remote locations.

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Danny Verneuille, Audit Manager
Nelva Blassingame, Senior Auditor
Frank Greene, Senior Auditor
Steven Gibson, Auditor
Olivia Jasper, Auditor

Report Distribution List

Chief Information Officer IS
Chief Operations Officer OP
Deputy Chief Information Officer, Operations IS
Deputy Chief Information Officer, Systems IS
Director, Enterprise Operations IS:E
Director, Systems Development IS:S
Assistant Commissioner (Electronic Tax Administration) OP:ETA