United States General Accounting Office

GAO

Report to the Commissioner of the Internal Revenue Service

September 1993

IRS INFORMATION SYSTEMS

Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information

149978

GAO/AIMD-93-34

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-253798

September 22, 1993

The Honorable Margaret Milner Richardson
Commissioner
Internal Revenue Service

Dear Ms. Richardson:

This report discusses weaknesses in general controls over the Internal Revenue Service's (IRS) computerized information systems. General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include the organizational structure, operating procedures, software security features, and physical protections designed to ensure that only authorized changes are made to computer programs, that access to data is appropriately restricted, and that back-up and recovery plans are adequate to ensure the continuity of essential operations. Such controls are critical to IRS' ability to safeguard assets, maintain the confidentiality of taxpayer data, and ensure the reliability of financial management information.

We reviewed IRS' computer general controls as part of our audit of IRS' fiscal year 1992 financial statements. IRS is 1 of 10 agencies required by the Chief Financial Officers Act (Public Law 101-576) to develop such financial statements and have them audited. This report is one of a series resulting from our audit. Appendix I contains a list of our previously issued reports.

Results in Brief

Our review identified two significant areas of weakness in the general controls over IRS computer systems that have increased the risk of fraud and diminished the reliability of IRS' financial management information. First, IRS did not adequately restrict access to taxpayer data to only those computer support staff who needed it and did not adequately monitor the activities of thousands of employees who were authorized to read and change taxpayer files. As a result, IRS did not have reasonable assurance that the confidentiality and accuracy of this data were protected and that the data were not manipulated for purposes of personal gain. IRS internal reviews have identified instances where IRS employees (1) manipulated taxpayer records to generate unauthorized refunds, (2) accessed taxpayer records to monitor the processing of fraudulent returns, and (3) browsed taxpayer accounts that were unrelated to their work, including those of

friends, relatives, neighbors, and celebrities. IRS has recognized that its current controls over access to taxpayer data are not adequate and is developing a more effective means of identifying inappropriate access activity.

Second, controls did not ensure that IRS used only authorized versions of its computer programs. This is a systemic problem that permits programmers to introduce unauthorized software changes either inadvertently or deliberately and, thus, increases the risk that taxpayer and other data may not be processed as intended by management policies. Ultimately, it can (1) impair the reliability of all data processed, (2) result in costly processing interruptions and errors and destruction of programs and data, and (3) allow fraudulent acts to occur and remain undetected.

Also, in case of an unexpected interruption in operations at its primary computer center, IRS' ability to maintain taxpayer accounts on a current basis may be impeded. This is because the capacity of the computers at its backup site is not adequate to run all of the primary and backup sites' critical applications at the same time. Also, IRS has not tested the effectiveness of its recently revised disaster recovery plan. IRS plans to obtain needed computer resources at its backup site during fiscal year 1994 and test its disaster recovery plan before the end of fiscal year 1993.

Background

As the federal government's tax collector, IRS reported $1.1 trillion in tax revenues for fiscal year 1992. To process and account for these revenues, IRS relies on extensive data processing operations. IRS' centralized master files of taxpayer information are maintained at its Martinsburg Computing Center (MCC), in Martinsburg, West Virginia. A second computing center in Detroit, Michigan, processes primarily administrative data, other than that associated with payroll, and serves as a backup processing facility for MCC operations. IRS also operates 10 service centers that process tax returns, remittances, and transactions associated with collection activities and 70 district and regional offices that can also access taxpayer data. IRS' Chief Information Officer is responsible for designing, acquiring, testing, and maintaining computer hardware at IRS' computing centers, service centers and district offices. The Information Systems Management Office, which is under the Chief Information Officer, is responsible for developing most of the software used by the IRS systems that account for taxpayer data.

Controls associated with computing or service center operations and the general data processing environment are key factors in attaining the basic

control objectives of ensuring that data are processed as authorized and are adequately protected from unauthorized change or disclosure. Such controls, which are referred to as general controls, typically relate to computer hardware, operating systems,[1] security software, security administration, software change controls, disaster recovery, and other facility-wide controls. General controls do not include controls that pertain to specific computer applications, for example, edit checks to reject input which is incomplete or has been determined to be unreasonable for a specific application. Many applications may operate within a single data processing facility, and the general controls in place at that facility affect the integrity of all of those applications.

Objective, Scope, and Methodology

Our objective was to evaluate and test the effectiveness of IRS' general controls over its computerized operations. Specifically, we evaluated IRS' general controls for ensuring that

- data and programs were protected from unauthorized access;
- only authorized changes were made to application and system software; and
- essential operations could be continued in case of an unexpected interruption.

To focus our work on the most significant controls, we performed preliminary risk assessments of IRS' general controls at the Martinsburg and Detroit Computing Centers, the Philadelphia and Cincinnati Service Centers, and IRS headquarters in Washington, D.C. At the conclusion of this preliminary work, we contracted with the public accounting firm of Price Waterhouse to gather additional information and evaluate general controls at MCC, the Philadelphia Service Center (PSC), and IRS headquarters. These evaluations included reviews of related IRS policies and procedures, tests and observations of controls in operation over all of the systems in use at these locations, and discussions with officials at the locations visited. We determined the scope of our contractor's audit work, monitored its progress at all key points, and reviewed the related workpapers to ensure that the resulting findings were adequately supported.

We discussed our findings and IRS' short-term corrective actions with responsible officials at MCC, PSC, and IRS headquarters. However, we did not assess the controls that IRS plans to incorporate into its long-term Tax

[1]The operating system is the set of programs that provides basic instructions to the computer and allows it to run various applications.

Systems Modernization effort, which is not expected to be complete until after the year 2000. Our review was performed from October 1992 to May 1993 in accordance with generally accepted government auditing standards.

IRS provided written comments on a draft of this report. These comments are summarized and evaluated at the end of this report and are reprinted in appendix II.

Inadequate Controls Over Access to Data and Programs

A basic internal control objective for any management information system is to protect data from unauthorized changes and to prevent unauthorized disclosures of confidential data. Although we found that IRS had implemented various policies, procedures, and physical controls to protect taxpayer data, IRS did not adequately (1) restrict access by computer support staff to computer programs and data files or (2) monitor the use of these resources by computer support staff and users. As a result, personnel who did not need access to taxpayer data could read and possibly use this information for fraudulent purposes. In addition, unauthorized changes could be made to taxpayer data, either inadvertently or deliberately for personal gain, for example, to initiate unauthorized refunds or abatements of tax.

Access Authority Was Not Adequately Restricted

Agencies can reduce the risk that unauthorized changes or disclosures occur by (1) granting employees authority to read or modify only those programs and data that are necessary to perform their duties and (2) periodically reviewing this authority and modifying it to reflect changes in job responsibilities and terminations of employment.

Although IRS had procedures in place to formally grant, document, and review most employees' access capabilities, these procedures were not always effective in appropriately limiting access to only those employees who needed it to perform their duties. IRS had not established a policy requiring periodic reviews of programmers' access authority to ensure that the authority they had originally been granted was still needed. Also, officials at IRS headquarters did not review access authority granted at service centers and district offices to determine if managers at these locations were making consistent judgments regarding which employees should be authorized access and the extent of their access. The ability of IRS headquarters to comprehensively review the access authority of service center and district office personnel is limited because IRS' systems have

not been programmed to generate lists of personnel with specific access authority. However, such reviews could be performed for a sample of employees, since information on individual employees' access authority is available.

Both IRS and we have identified instances of inappropriate access authorizations. In its December 1992 report to the President and the Congress required under the Federal Managers' Financial Integrity Act (FMFIA) (31 U.S.C. 3512(d)), Treasury reported that IRS personnel who approve manually processed refunds were inappropriately authorized to both initiate and approve such refunds through IRS' computers. Also, at MCC, we identified two secretaries who had no need to access sensitive computer files but had been granted such access because authority had been granted to the entire group of employees that they worked with, rather than on an individual employee basis.

Additionally, we identified computer support staff at both PSC and MCC who had been granted broad access to programs and data that was beyond that needed to perform their routine duties and, in some cases, did not provide an appropriate segregation of duties. For example,

- 15 personnel at MCC had broad access authority to both operating system and application programs, which allowed them to independently initiate and execute application program modifications that could result in changes to taxpayer data, and several could also suspend, or turn off, the security features that provided a record of their user identification and the date of their access;
- 20 computer systems analysts at PSC, responsible primarily for installing new computer programs, had been granted broad access to all programs and taxpayer data at that location even though they did not all require such extensive access; and
- 6 security officers at PSC, who were primarily responsible for granting and modifying access authority to other service center personnel and conducting security training, had unlimited access to taxpayer data through IRS' primary system for accessing taxpayer accounts even though they did not need such access to perform their duties.

IRS officials told us that these employees had been granted broad access to facilitate support of the centers' 24-hour a day operations. However, by carefully analyzing the duties of these employees, IRS could have limited their access authority without impeding their ability to do their jobs and thus reduced the risk of inappropriate activity. Also, other techniques,

such as an emergency password, could have been implemented to provide temporary access authority when needed.

Access Activity Not Adequately Monitored

PSC did not adequately review the actual access activities of its employees. The greatest risk involved IRS' Integrated Data Retrieval System (IDRS), which is the primary computer system for accessing and adjusting taxpayer accounts. Thousands of IRS employees can read and alter sensitive tax information in IDRS through computer terminals located throughout each service center and at district offices.

Monitoring the access activities of employees, especially those who have the ability to alter sensitive programs and data, can help identify any significant problems and deter employees from inappropriate and unauthorized activities. However, when thousands of transactions are involved, reviews cannot be effective unless reports are available to managers that highlight activity that is unusual or suspicious so that it can be investigated. In the absence of such reports, managers can periodically review the appropriateness of a sample of transactions. Regardless of the technique used, active oversight can help ensure that problems are deterred or detected.

The reports used by PSC's 340 unit security representatives, who usually were unit heads, did not provide a means of effectively monitoring the activities of the 5,034 PSC employees who had access to IDRS as of December 1, 1992.[2] This was because the reports, which were provided on either a weekly, monthly, or quarterly basis, did not identify most types of unusual or suspicious activity, such as frequent attempts to access one individual's account. Instead, they summarized thousands of accesses and highlighted only a few types of suspicious or unusual activity, such as accessing a spouse's or another employee's account. Although these reports were useful in identifying accesses by unauthorized personnel, they did not highlight many other indicators of potentially inappropriate activity by authorized personnel, such as repeated access to a specific taxpayer's account, browsing trends, or large-dollar transactions. In addition, PSC had not established procedures for monitoring the accesses of its 340 security representatives.

[2]IDRS provides personnel at each service center access to the files related to the returns that their respective center has processed. Nationwide, there are about 56,000 IDRS users.

An October 1992 internal audit report on IDRS security[3] identified the lack of useful security reports as a servicewide problem and reported that various internal audit reviews and projects have identified instances where employees used IDRS for non-business reasons without being detected by management. For example, by analyzing employees' accesses through the use of a command code that allows the user to read certain information in a taxpayer's account, IRS' internal auditors identified 368 employees who had used IDRS for non-business purposes without management's knowledge. Of these, 79 were referred to IRS' internal security for investigation of potential criminal activity. According to the October 1992 internal audit report, 6 cases had been referred to the Department of Justice for prosecution for preparing fraudulent returns and then monitoring the related accounts on IDRS. Some employees had used IDRS to issue fraudulent refunds or browse taxpayer accounts that were unrelated to their work, including those of friends, relatives, neighbors, and celebrities. While these and other non-routine internal reviews have identified instances of fraud, such reviews cannot be relied on to routinely prevent or detect unauthorized access to taxpayer data.

IRS has recognized that its current controls over access to data through IDRS are not effective, and Treasury reported this in its December 1992 FMFIA report. To address this problem, IRS is developing a computerized capability to monitor employee access activity. As planned, this new tool will automatically search for and report numerous combinations of IDRS command code use that IRS deems to be suspicious or that have been used for fraudulent purposes in the past. This should provide IRS with a much more effective means of identifying inappropriate access activity. According to IRS headquarters officials responsible for this project, as of May 1993, IRS was in the process of developing the software for this project and procuring the related computer hardware. These officials said that they expect this new capability to be available in early fiscal year 1994.

Two other areas where access was not adequately monitored involved fewer employees; however, their activities were potentially more damaging because they had unlimited access to both taxpayer data and programs at PSC. Access activities of PSC's six IDRS security officers were not required to be reviewed, and the activities of the center's 20 computer system analysts were not adequately reviewed because PSC's security administrator did not distribute the weekly reports on the analysts' access activities to the analysts' supervisors. PSC's security administrator told us that he usually looked over the reports and then threw them away. As a

[3]"Review Of Controls Over IDRS Security," (Reference No. 030103) October 23, 1992.

result, the analysts' supervisors, who were most familiar with the analysts' responsibilities and activities in any given week, did not have an opportunity to (1) examine the reports, which sometimes listed several hundred accesses for an individual analyst, or (2) compare new reports with previous reports to identify trends in suspicious or inappropriate accesses.

Software Security Features Not Optimized at MCC

MCC was not taking full advantage of various optional security features available through the computer system software that governed access to IRS' master files of taxpayer data and to programs being developed by headquarters. Although these features were built into the system software by the software manufacturer, MCC was responsible for deciding which features to use and for activating them. Some of these built-in security features were not being effectively used because MCC had not prescribed the conditions under which they were to activate or identified data tapes in a way that would allow the computer to recognize the tapes and determine which controls to apply. For example,

- tapes, including those on which most master file data were stored, were not restricted from unauthorized access or modification because the related software security features had not been implemented and the tapes had not been labeled so that the software could recognize them for this purpose and
- MCC had not activated features that would have automatically (1) suspended or revoked user identifications that had not been used within a specified period and (2) ensured that copied files were subject to the same software access controls as the original versions.

Physical Security Not Effective at PSC

At PSC, physical controls were inadequate over the tape library containing taxpayer records and a terminal with unlimited access to sensitive data and programs. These tapes and the terminal were contained in a room to which access was controlled by a card key system. However, this system was not effective because procedures for initially authorizing and reverifying cards were informal and inconsistent. For example, official request forms were not used to request card key access and there were no periodic reviews of all cardholders to determine if they continued to need access. Various persons who should not have had access to taxpayer data held card keys, such as employees of the security vendor that installed the system. In addition, one user had three card keys and two other users had two card keys each.

Even if the card key system had effectively limited access to this room, the numerous tape librarians who needed access to the tape library did not also need access to the IDRS terminal, which was used primarily by computer system analysts to install new software. For this reason, instituting mechanisms for separately controlling access to these resources would have provided greater assurance that they were not used by unauthorized personnel.

Inadequate Software Change Controls

Although IRS had implemented various controls over the development and implementation of computer programs used to access and process taxpayer data, we identified weaknesses in two areas. First, centrally developed programs that had been modified and approved were not adequately controlled to ensure that only authorized and properly tested program versions were used to process and access taxpayer data. Also, PSC exercised little or no control over the use of locally-developed programs. Because of these weaknesses, IRS risked implementing unauthorized programs, which could result in improper processing of taxpayer data or allow malicious programming changes that could interrupt data processing or destroy data files and programs. Also, as with access control weaknesses, inadequate software change controls could permit deliberate attempts to improperly modify taxpayer data.

Centrally Developed Programs Not Adequately Controlled

IRS' Information Systems Management Office had not implemented effective procedures to ensure that programs that had been reviewed and approved were the same versions of programs that were used to process taxpayer data at MCC and the service centers and that programs were consistently reviewed by IRS' independent quality assurance group. The Information Systems Management Office is responsible for developing and modifying all IRS computer programs used to process taxpayer data and for developing related software control standards.

Programmers had uncontrolled access to programs after they had been approved by supervisors because IRS had not developed procedures requiring them to go through a program librarian[4] to obtain programs. Because of this, programmers could, either inadvertently or deliberately, change previously approved programs or substitute an unauthorized program for the approved version before such programs were put into production. By making such changes or substitutions, an individual could

[4]Program librarians maintain the program libraries, which contain groups of programs. Typically, program libraries are organized according to the programs' status and purpose, such as programs in use or programs that are being tested.

provide a means to access or manipulate data without being detected or to destroy programs and data. In addition, if unauthorized changes had been detected, it would have been difficult to identify when, how, and by whom such changes had been made because a history, or audit trail, of this information was not maintained. Controlling access through a program librarian could have minimized the risk of unauthorized changes by (1) restricting access to only those programmers who could show that they had been authorized to change a program, (2) ensuring that only one programmer at a time had access to an individual program, and (3) maintaining prior versions of approved programs to provide an audit trail of changes.

Also, because IRS' independent quality assurance group focused its reviews on program changes that were made as part of IRS' semi-annual program change cycle, changes that were not part of this cycle were not subject to the same level of review. Therefore, they had an increased risk of containing programming errors. Quality assurance reviews are to be conducted after changes have received supervisory approval and are intended to ensure that changes comply with authorized change requests. Although the majority of program changes were made as part of the semi-annual cycle, IRS officials said that some significant changes were made outside of these cycles.

No Formal Control Over Locally Developed Programs at PSC

Much broader change control weaknesses existed regarding programs used at PSC to enhance local operations and measure service center productivity. Such programs had either been developed at PSC or obtained from other service centers and had been implemented without any formal review, documentation, or approval, even though such steps are required by IRS procedures. This lack of control over locally developed programs increased the risk that (1) taxpayer data could be inappropriately altered or disclosed, (2) local management reports could be incomplete, inaccurate, or misleading, and (3) malicious program changes could be introduced. Inappropriate accesses to and modifications of data could have been detected after they had occurred through reviews of reports on access activity. However, as previously discussed, such reviews were not an effective tool for identifying such improprieties.

After we brought this weakness to the attention of IRS headquarters officials, they told us that they plan to review operations at other service centers to determine if they have adequate controls over locally developed programs.

Disaster Recovery Plans Incomplete

In November 1992, IRS finalized an updated disaster recovery plan intended to ensure that taxpayer accounts could be maintained on a reasonably accurate and current basis if MCC's operations were unexpectedly interrupted. In case of such an emergency, IRS plans to temporarily transfer MCC's essential operations to its Detroit Computing Center. However, IRS officials told us that (1) the data processing capacity of Detroit's computers was not adequate to run all of MCC's and Detroit's critical applications at the same time and (2) IRS had not performed a complete test of Detroit's ability to handle MCC's operations since 1989. In addition, IRS officials said that a formal analysis to determine which of MCC's computer applications were critical had not been performed since 1988. Performing such analyses and tests periodically, perhaps every year or two, can help identify any modifications that may be needed due to changes in management policies, computer software and hardware, and personnel.

IRS officials told us that they plan to conduct a complete test of MCC's disaster recovery plan before the end of 1993. In addition, they said that IRS planned to purchase new computers during fiscal year 1994 that would provide the Detroit center with the data processing capacity needed to handle both MCC's and Detroit's critical applications.

Conclusions

IRS has not adequately instituted certain basic controls over its computerized operations. Such controls are especially important at IRS because of the large amount of funds involved and because of IRS' responsibility for maintaining the confidentiality of taxpayer data. Weaknesses in IRS' general controls increase the risk of fraud, unauthorized change or disclosure of taxpayer data, and interruptions in critical data processing operations. By automating its process for reviewing access to taxpayer data, IRS is taking steps to better detect inappropriate accesses to data maintained in IDRS. Also, IRS plans to test its disaster recovery plan and supplement its backup data processing capacity. However, additional actions are needed to limit access authority granted to computer support staff and better control software modifications.

Recommendations

We recommend that you direct the Chief Information Officer and the regional commissioners, as appropriate, to

- limit access authorizations for individual employees to only those computer programs and data needed to perform their duties and periodically review these authorizations to ensure that they remain appropriate;
- monitor efforts to develop a computerized capability for reviewing IDRS user access activity to ensure that it is effectively implemented;
- establish procedures for reviewing the access activity of unit security representatives;
- use the security features available in MCC's and PSC's operating system software to enhance system and data integrity, especially regarding controls over tapes containing taxpayer data;
- require that programs developed and modified at IRS headquarters be controlled by a program librarian responsible for (1) protecting such programs from unauthorized changes, including recording the time, date, and programmer for all software changes, and (2) archiving previous versions of programs;
- establish procedures requiring that all computer program modifications be considered for independent quality assurance review;
- formally analyze MCC's computer applications to ensure that critical applications have been properly identified for purposes of disaster recovery,
- test the disaster recovery plan prior to the end of 1993, as planned, and
- monitor service center practices regarding the development, documentation, and modification of locally developed software to ensure that such software use is adequately controlled.

In addition, we recommend that you direct the Philadelphia Service Center Director to

- review the current card key access system to ensure that only users who need access to the facilities protected by the system have access and that authorized users each have only one unique card key and
- establish physical controls to protect computers with access to sensitive data that are not protected by software access controls.

Agency Comments and Our Evaluation

In commenting on a draft of this report, IRS agreed with the concerns we reported and discussed planned corrective actions. Regarding controls over employees' access to computer programs and taxpayer data files, IRS stated that it is revising written guidelines, strengthening management reviews, and enhancing audit trail systems to better report employees' activities. Regarding controls over centrally and locally developed computer programs, IRS stated that it has formed a team to identify needed controls, is testing off-the-shelf computer software that contains program version controls, and is strengthening documentation and scheduling requirements for locally developed computer processes. IRS also provided some details regarding its efforts to strengthen its disaster recovery capabilities.

IRS' comments indicate that it is in the process of addressing the control weaknesses described in our report. However, many of the related details have not been either formulated or implemented. We plan to further review these efforts and assess their effectiveness in conjunction with our audit of IRS' fiscal year 1993 financial statements.

This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement on actions taken on these recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Operations no later than 60 days after the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of the report.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Governmental Affairs; the Senate Committee on Finance; the House Committee on Government Operations; the House Committee on Ways and Means; the Subcommittee on Commerce, Consumer, and Monetary Affairs, House Committee on Government Operations; the Subcommittee on Oversight, House Committee on Ways and Means; and the Joint Committee on Taxation. We are also sending copies to the Secretary of the Treasury, the Director of the Office of Management and Budget, and other interested parties. Copies will be made available to others upon request.

This report was prepared under the direction of Gregory M. Holloway, Associate Director, Civil Audits, who may be reached on (202) 512-9510, if you or your staff have any questions. Major contributors to this report are listed in appendix III.

Sincerely yours,

Donald H. Chapin
Assistant Comptroller General

Contents

Letter 1

Appendix I Reports Resulting From GAO's Audit of IRS' Fiscal Year 1992 Financial Statements 18

Appendix II Comments From the Internal Revenue Service 19

Appendix III Major Contributors to This Report 21

Abbreviations

FMFIA	Federal Managers' Financial Integrity Act
IDRS	Integrated Data Retrieval System
IRS	Internal Revenue Service
MCC	Martinsburg Computing Center
PSC	Philadelphia Service Center

Reports Resulting From GAO's Audit of IRS' Fiscal Year 1992 Financial Statements

Financial Management: IRS Lacks Accountability Over Its ADP Resources (GAO/AIMD-93-24, August 5, 1993).

Financial Audit: Examination of IRS' Fiscal Year 1992 Financial Statements (GAO/AIMD-93-2, June 30, 1993).

Financial Audit: IRS Significantly Overstated Its Accounts Receivable Balance (GAO/AFMD-93-42, May 6, 1993).

Federal Tax Deposit System: IRS Can Improve the Federal Tax Deposit System (GAO/AFMD-93-40, April 28, 1993).

Comments From the Internal Revenue Service

COMMISSIONER

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

AUG 0 3 1993

Mr. Donald H. Chapin
Assistant Comptroller General
Accounting and Financial Management Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Chapin:

Thank you for the opportunity to comment on the GAO draft report IRS INFORMATION SYSTEMS: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information. This draft is one of several we expect to receive as GAO continues the audit of our Fiscal Year 1992 financial statements.

We agree with the concerns noted in the draft report. We also appreciate the recognition in the report of the actions the Service has already taken or is planning to take to address these concerns.

The report identified weaknesses in controls over access by computer support staff to computer programs and data files, and weaknesses in monitoring the use of these resources by computer staff and users. We are placing much stronger emphasis on the implementation of procedures and guidelines related to access controls and monitoring. We are revising our internal management documents to strengthen these guidelines where needed, and we are strengthening management reviews to ensure compliance. Also, we are enhancing the audit trail systems to better report activity of users and computer support personnel.

The report identified weaknesses in controls of centrally developed programs which ensure that correct versions are in operation, and controls over programs developed locally at Field sites. We formed a team to identify requirements for automated procedures and related guidelines to provide change and version controls, and are now testing off-the-shelf software packages which contain version control features. We will revise our internal management documents to strengthen documentation and scheduling requirements of all locally developed computer runs.

The report identified weaknesses in the testing of our disaster recovery plan to ensure that the Service's Master File records would be reasonably accurate and current in the event of major interruption of operations. Disaster recovery guidelines were approved and distributed in February 1993. This has

Mr. Donald H. Chapin

elevated the Service's recovery posture for the computing centers. We are procuring computer systems during 1994 and additional space and facilities in mid-1995, for a total Corporate Contingency operation at each of our computing centers if necessary. A complete test of the disaster recovery plan for our Master File computing center will be finished in 1993. Additional major recovery tests are planned between our computing centers.

We look forward to continuing our work with you in this important area of automated information systems.

Sincerely,

for Margaret Milner Richardson

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Robert F. Dacey, Senior Assistant Director
Jean L. H. Boltz, Assistant Director

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1000
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066.

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100