United States General Accounting Office 33900

GAO

Report to the Commissioner of Internal Revenue

March 1986

# COMPUTER SECURITY

# Contingency Plans and Risk Analyses Needed for IRS Computer Centers

GAO/IMTEC-86-10

034917 / 129434

GAO

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

Information Management and
Technology Division
B-221001

March 27, 1986

The Honorable Roscoe L. Egger, Jr.
Commissioner of Internal Revenue
Department of the Treasury

Dear Mr. Egger:

We reviewed the Internal Revenue Service's (IRS) plans for ensuring the continuity of its computer operations if any 1 of 12 IRS computer centers is destroyed or significantly disabled for an extended period by a natural disaster, fire, accident, or sabotage. We also reviewed IRS' efforts to assess potential risks (such as fire, flood, unauthorized entry, or ineffective contingency planning) at these centers. We found that IRS

- does not have tested, certified automatic data processing (ADP) contingency plans for its computer centers, and
- has not periodically assessed potential risks to computer operations at these centers, although it has recently started a risk-analysis program that it hopes to complete in 1987.

IRS relies heavily on computers to process tax returns and receipts and to monitor taxpayers' compliance with laws and regulations. Any major loss or damage to its computer assets—equipment, software, or data—would limit IRS' ability to carry out its complex and demanding mission which, in 1984, involved collecting $680 billion in tax revenues and paying $85 billion in tax refunds. A disruption to IRS' data processing capability can have a devastating effect on operations, as is evidenced by the 1985 filing season when, among other things, the shortage of computer capacity resulted in

- millions of dollars of interest being paid on late refunds to taxpayers,
- millions of dollars in overtime payments being made to IRS employees,
- IRS' ability to answer taxpayer inquiries being impaired, and
- inaccurate notices being sent to taxpayers.

If IRS had tested, certified plans, additional computer capacity would have been identified in advance and available for use to meet some of the shortfall that occurred during the 1985 filing season. As discussed later, an essential element of an effective contingency plan is the provision for adequate backup computer capacity.

To reduce the disruption caused by events that prevent normal operation at computer centers, Office of Management and Budget (OMB) Circular A-130[1] and IRS' Internal Revenue Manual require the development maintenance, and testing of ADP contingency plans. To alert agency management to the type and magnitude of risks facing a computer center, and then identify measures to eliminate or mitigate these risks, these same regulations require that risk analyses be conducted at least once every 5 years at each center. The results of risk analyses can be used to help prepare and revise ADP contingency plans. While IRS has taken and continues to take steps in these areas, its efforts have fallen short.

This letter describes our objectives, scope, and methodology; summarizes our findings; and states our recommendations. Appendix I provides more detailed information on our findings.

## Objectives, Scope, and Methodology

Our objectives were to determine (1) whether IRS' ADP contingency plans provide reasonable assurance that IRS computer centers, in the event of a prolonged disruption, can continue critical data processing operations promptly, and (2) whether IRS has implemented a risk-management program to assess and reduce potential threats to computer operations.

We conducted our review at IRS headquarters; IRS' National Computer Center (NCC); and 4 of the 10 service centers that process tax returns and related documents: Andover, Massachusetts; Atlanta, Georgia; Austin, Texas; and Fresno, California. These four were selected because they are geographically dispersed and vary in work-load volume. We did not visit IRS' non-tax-return processing center, the Detroit Data Center, because after obtaining information on it from IRS headquarters, we did not believe that a visit was necessary.

We observed physical and environmental controls for IRS computer rooms, tape libraries, and backup tape storage areas. We also inventoried IRS' backup tapes at the sites we visited. We interviewed appropriate IRS security, internal audit, computer operations, and user personnel at headquarters and at the service centers.

We reviewed governmentwide circulars, regulations, and publications, as well as Treasury Department directives and IRS' Internal Revenue

[1]Effective December 12, 1985, OMB Circular A-130 (Management of Federal Information Resources) superceded OMB Circular A-71, Transmittal Memorandum Number 1, which had been in existence since 1978. The new circular does not change the requirements specified in A-71 for ADP contingency plans and periodic risk analyses.

Manual, to determine applicable standards and guidelines. We also reviewed IRS risk-analysis reports, ADP contingency plans, and related documents and compared them to these standards and guides. In addition, we toured computer facilities at a major commercial bank and the Federal Reserve Board, both in San Francisco, California, and in Washington, D.C., to gain a perspective on security efforts at other types of organizations. We conducted our review in accordance with generally accepted government auditing standards from July 1984 to September 1985.

## Contingency Plans and Risk Analyses Are Required for IRS Computer Centers

IRS' tax return processing system is comprised of two major components—NCC in Martinsburg, West Virginia, which maintains a master file account on each individual and business taxpayer, and the 10 service centers, which receive and control tax returns and subject them to validity and consistency checks and mathematically verify taxpayers' computations. IRS' Detroit Data Center is responsible for IRS' administrative systems, tax analysis systems, and many of its management information systems.

As noted earlier, OMB's Circular A-130 required each agency head to set up an ADP security program. Among other things, each agency is required to do the following:

- Develop and maintain contingency plans that will provide reasonable continuity of data processing support should events occur that prevent normal operations. (These plans should be periodically reviewed and tested.)
- Conduct periodic risk analyses at each computer center to determine the center's vulnerabilities and to effectively use security resources to reduce potential loss. These analyses must be performed before a new center is designed; or whenever a significant change to the physical facility, hardware, or software occurs; or at least every 5 years.

IRS' Internal Revenue Manual also requires that ADP contingency plans be developed, maintained, and tested for each of the 12 IRS computer centers. The manual notes that plans must be developed to respond to fire, flood, sabotage, serious equipment damage or failure, loss of electrical power, bomb threats or explosion, and civil and natural disasters. The manual specifies that each contingency plan must provide for

- backup facilities and computer hardware, i.e., a prearranged location where ADP operations can take place while the damaged facility is repaired;
- backup files of software, data, and documents necessary to continue operations;
- processing priorities, i.e., a list ranking the critical applications to be processed, recognizing that only top-priority, essential functions will be performed in the event of a disaster; and
- other essential requirements, such as personnel, transportation, supplies, office equipment, and security.

The manual also requires that appropriate assistant commissioners review and certify all contingency plans to ensure that (1) workable, technically feasible plans are prepared, and (2) all management levels know of the plans available to protect critical ADP systems. The Assistant Commissioner for Returns and Information Processing must certify the plans for NCC and the 10 service centers, and the Assistant Commissioner for Support and Services must certify the plan for the Detroit Data Center.

## IRS' ADP Contingency Plans Lack Certain Elements

IRS' draft ADP contingency plans are incomplete. Further, IRS has not taken adequate measures to prepare for an emergency. Specifically:

- NCC has no designated backup processing site.
- IRS' Computer Services Office stated that computer capacity problems may make infeasible IRS' currently proposed arrangement for one service center to back up another.
- IRS has not identified the most critical work-load functions, i.e., those that must be performed first in the event of a prolonged disruption to a center's operations.
- Backup tape files containing data and programs necessary to continue operations were not always maintained as required by IRS.
- Testing to ensure the workability of ADP contingency plans has ranged from nonexistent to limited.

As a result, existing ADP contingency plans do not meet IRS' requirements to deal with the basic stages of emergency reaction: emergency response, backup operations, and recovery operations. Regarding backup operations, IRS has not analyzed and ranked the feasibility, costs, risks, and benefits of alternative backup strategies. Because of the high cost and administrative burden of operating a backup facility, IRS

regulations require that all available alternative backup operations be carefully considered.

## Risk-Analysis Program Has Been Resumed

In November 1984 and January 1986, IRS conducted risk analyses at the Brookhaven and Fresno Service Centers, respectively. Also, in January 1986 IRS began a risk analysis at its Memphis Service Center. These are the only such analyses done since IRS suspended its risk-analysis program in 1981. Accordingly, IRS does not know the actual risks facing its other 10 centers, the potential losses such risks could cause (for example, physical damage or lost revenues), or how to most effectively reduce those risks. IRS plans to complete risk analyses at all of its centers by 1987.

Between 1979 and 1981, IRS performed risk analyses at six of its centers, each concentrating on a specific operation. For example, the Philadelphia Service Center analyzed risks to its remittance processing system, and the Austin Service Center analyzed the security of its building and grounds. However, these analyses were never consolidated into an IRS-wide assessment as planned because, in September 1981, IRS decentralized its approach to security. IRS made this change because it believed that controls were firmly in place, managers had become more security conscious, and the need for additional security procedures had diminished. Consequently, IRS placed a moratorium on risk analyses that continued through 1983.

In 1983, the Treasury Department reviewed its internal controls in response to the Federal Managers' Financial Integrity Act of 1982 [31 U.S.C. 3512 (b) and (c)], which requires agencies to report to the President and the Congress annually on how well their internal control systems are working. On December 31, 1983, Treasury reported that information systems security was a "material" (substantial) weakness; as part of the Department's corrective actions, IRS implemented a new risk-analysis program for its 12 centers.

The risk analysis conducted at Brookhaven identified physical security problems similar to those we found at other IRS centers. For example, IRS found that Brookhaven was susceptible to fire and smoke damage because the computer room door did not close; we noted that NCC has no fire door between its two computer rooms. Also, IRS disclosed that the main entrance to Brookhaven's computer room was not secured after hours. We saw the same conditions at the Fresno and Andover Service Centers. IRS also stated that Brookhaven's ADP contingency plan lacked

adequate detail on steps to be taken in emergencies. At the close of t review, IRS prepared an action plan to address the problems identifie this center.

## Contingency Planning and Risk-Analysis Efforts Are Progressing Slowly

ADP contingency planning and risk-analysis efforts at IRS are proceeding—but at a slow pace. In 1986, almost 8 years after OMB's Circ A-71 (now superceded by Circular A-130, which has the same requir ments) required federal agencies to develop, maintain, and periodical review and test ADP contingency plans, IRS still does not have tested, tified plans. As indicated earlier, the circular also required that risk analyses be performed at least every 5 years or earlier if significant changes in facilities, hardware, or software occur. However, IRS has n yet conducted risk analyses at all of its centers, even though significa hardware and software changes have taken place.

In 1977, we reported that IRS' controls over computer operations were not adequate to prevent unlawful disclosure of tax data.[2] We pointed that IRS' weak enforcement of its security regulations occurred becaus responsibility was fragmented among four organizations within IRS. Because these organizations had other functions to perform, they devoted less attention to security matters. We therefore recommended that the Commissioner establish an independent security office respor sible for all facets of IRS' security program. The Commissioner agreed that IRS had not been aggressive in the security area and committed th agency to a vigorous course of improvement that included, among oth things, undertaking a major risk-analysis effort. In April 1978 IRS esta lished a single organization to oversee its security program.

As indicated earlier, in September 1981, IRS believed that its centers were reasonably secure and placed the moratorium on risk analyses t continued through 1983. Treasury revitalized the risk-analysis progra after identifying ADP security as a material weakness in an assessment of its internal control systems.

The need for tested, certified contingency plans became readily apparent to IRS in June 1983 when a fire in a power generator room at Brookhaven shut down the center's computers for a day. Following th disruption, the Assistant Commissioner for Returns and Information Processing questioned the adequacy of disaster recovery plans for IRS

[2]IRS Security Program Requires Improvements to Protect Confidentiality of Income Tax Informati (GGD-77-44, July 11, 1977).

service centers and asked the centers to reevaluate and update their plans.

Because the updated plans contained several problems, the Assistant Commissioner formed a task group in October 1984 to develop a model plan for the service centers. The group is comprised of representatives from the offices of three assistant commissioners—Returns and Information Processing, Support and Services, and Computer Services. In November 1984 the group determined that its task was very complex and would require input from many additional field and national office staff to produce a detailed and adequate plan. It also proposed hiring a consultant to gather information for a model plan. By September 1985, the task group planned to draft a statement-of-work; this document would be used to procure a vendor to prepare a model ADP contingency plan for service centers. IRS has now suspended this effort and is considering establishing a contingency planning office.

In October 1985, IRS reported to Treasury that IRS was not in compliance with OMB Circular A-71 (now A-130) regarding contingency plans and risk analyses. IRS did not say when it anticipated completing its contingency plans, but it did indicate that all risk analyses would be done by September 30, 1987.

## Conclusions

IRS' computer centers are vulnerable to prolonged disruptions caused by accident, fire, natural disaster, or sabotage because the agency does not have adequate contingency plans to continue critical data processing operations. In addition, IRS has not assessed the risks to which its centers are exposed.

Such plans and assessments are required by OMB and IRS regulations. They are critical for IRS because of its mission and how it is carried out—almost entirely with computers. Since IRS computers must process millions of returns involving billions of dollars in revenues and refunds, when computers are not available for an extended period, IRS' ability to efficiently, effectively, and economically achieve its mission is greatly affected.

Accidents do occur, as is evidenced by the fire at Brookhaven. Also, the effects of a disruption to IRS' data processing capabilities were illustrated during the 1985 filing season when IRS paid millions of dollars in interest on late refunds, paid millions of dollars in overtime, and provided poor service to many taxpayers. The disruption caused by these

events might have been reduced if IRS had tested, certified contingency plans requiring adequate backup computer capacity.

IRS has taken some action to correct problems; however, its progress has been slow. IRS initially planned to conduct risk analyses for all its centers in 1986. As of January 1986, only two risk analyses had been completed, with a third in progress. IRS now plans to complete all risk analyses by 1987. In addition, the effort to develop a model ADP contingency plan for all service centers was suspended in November 1985 after a year's work. We believe these actions indicate that contingency plans and risk analyses have not been given a high priority.

The lack of tested, certified contingency plans and the failure to conduct periodic risk analyses are significant control weaknesses because of IRS' heavy dependence on ADP support to achieve its mission. The IRS Commissioner responded to this situation on October 21, 1985, when he reported to Treasury that IRS was not in compliance with OMB Circular A-71 (now A-130).

## Agency Comments and Our Evaluation

IRS generally agreed with our findings and recommendations. IRS said it strongly agreed that a tested contingency plan that would enable the agency to continue processing in the event of a disaster was needed. It also acknowledged that progress in developing such a plan has been slow. In this regard, IRS stated that its Automation Policy Board, after discussing the issues in a draft of this report on December 17, 1985, granted approval to the Assistant Commissioner (Computer Services) to appoint a contingency planning project officer. The officer's initial tasks, to be completed in about 60 days (about the beginning of March 1986), are to develop time frames and estimate resources needed for a contingency planning office. The board will then review these estimates and decide whether to approve such an office. IRS also stated that risk analyses for all computer centers would be completed by 1987.

IRS did not agree that the problems encountered in the 1985 tax filing season could have been avoided or significantly reduced if tested, certified ADP contingency plans existed. It stated that contingency plans address risks of natural disasters, fire, accident, or sabotage, which generally are not applicable to problems that arise when implementing new systems and operations.

While we agree that the risks of natural disasters and those associated with the implementation of new systems are different, a contingency

plan would provide alternative sources for data processing capability that could be used whenever normal operations are disrupted. In the particular case of the 1985 tax filing season, the disruption (among other things, not having enough computer capacity to process the work load) was similar to what could happen if a natural disaster occurred and IRS computers became unavailable. If IRS had had adequate contingency plans, the process of locating and using additional processing facilities might have been easier.

IRS told us that the NCC contingency plan does not currently conform to IRS requirements, but that it is being revised and will soon be submitted for certification. IRS also raised technical and editorial points in our draft report, which we have addressed. IRS' points and our comments regarding their disposition are contained in appendix II.

## Recommendations to the IRS Commissioner

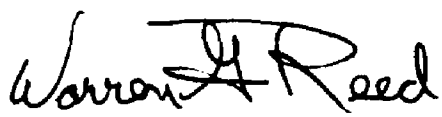
We recommend that you direct the Assistant Commissioner, Support and Services (for the Detroit Data Center), and the Assistant Commissioner, Returns and Information Processing (for all other computer centers), to expedite efforts to

- develop, certify, and periodically test ADP contingency plans for all IRS computer centers according to the criteria and procedures set forth in IRS' Internal Revenue Manual and OMB Circular A-130;
- perform periodic risk analyses to (1) aid in developing and maintaining effective ADP contingency plans, and (2) help assess the internal controls environment, as required by the Federal Managers' Financial Integrity Act of 1982 and the OMB circular; and
- continue to report the lack of contingency plans and periodic risk analyses as material control weaknesses under the Federal Managers' Financial Integrity Act until contingency plans have been developed, certified, and tested, and risk analyses (as well as needed corrective action identified by such analyses) have been completed for all computer centers.

As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement on actions taken on our recommendations to the House Committee on Government Operations and the Senate Committee on Governmental Affairs not later than 60 days after the date of the report. A written statement must also be submitted 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 Director, Office of Management and Budget; the Secretary of the Treasury; and interested congressional committees and subcommittees; and will make copies available to others upon request.

Sincerely yours,



Warren G. Reed
Director

# Contingency Plans and Risk Analyses at IRS

ADP contingency plans are essential to ensure the continuity of IRS' computer operations if any one of the agency's computer centers is destroyed or significantly disabled for an extended period because of a natural disaster, fire, accident, or sabotage. Despite the importance of computers to IRS' mission and the fact that there has been a governmentwide requirement since 1978 that appropriate contingency plans be developed, maintained, and tested, IRS does not have tested, certified ADP contingency plans for any of its centers. In addition, until IRS completed a risk analysis at its Brookhaven Service Center in November 1984, it had not identified the risks and vulnerabilities of any of its centers since 1981. We believe that IRS' slowness in completing contingency plans and conducting risk analyses is due to the agency's placing too low a priority on these tasks. Deficiencies in the agency's contingency plans, its attempts to correct them, and its risk-analysis efforts are described in this appendix.

## Significance of ADP Contingency Plans

Contingency plans can help an organization expedite the recovery of computer operations and minimize recovery costs. For example, in 1982 the minicomputers, online terminals, and communication systems of a major mortgage banking company were destroyed by a fire. Because of a good contingency plan, the bank had relocated, received, and installed replacement equipment, and had returned to business as usual within 4 days. In contrast, in August 1979, water from broken pipes flooded the Census Bureau's computer center and damaged its computers. Without a designated backup facility, Census had no alternative except to acquire dedicated computer time commercially until its own computer equipment was restored—an alternative that cost more than $1.5 million. If prior arrangements for backup had been made with another federal or commercial center, the cost might have been less.

Although IRS has never had a major disaster at a computer center, a 1983 fire in a power generator room at Brookhaven shut down the center's computers for a day. A larger disruption might halt computer operations for a longer time. The loss of an IRS computer center for even several days could, depending on the time of year, result in

- millions of dollars in interest payments to taxpayers caused by delays in processing refunds;
- overtime payments to IRS employees to make up for any interrupted processing;
- lost revenue because collection staff would not have the data to check the accuracy of returns;

- impaired service to taxpayers because of lost records; and
- inaccurate notices to taxpayers, caused by delays in posting data to taxpayers' accounts.

These effects are not unlike those experienced by IRS during the 1985 filing season when, among other things, the lack of sufficient computer capacity of computer systems resulted in interest paid to taxpayers, extra overtime (at least 45 percent more than 1984 figures) paid to IRS employees, and poor service to taxpayers. The effect, however, could be significantly greater if the time required for a computer center to recover became protracted.

## Several Aspects of IRS' ADP Contingency Plans Are Inadequate

Federal requirements for computer centers' ADP contingency plans are set forth in OMB Circular A-130, dated December 12, 1985 (see appendix III). According to this document, agencies should

- develop and maintain contingency plans to ensure that essential functions can continue in the event computer support is interrupted and
- maintain disaster recovery plans at all computer installations in case normal operations are interrupted, and test these plans periodically.

IRS has incorporated the above criteria in its Internal Revenue Manual, which requires that ADP contingency plans be developed, maintained, and tested for critical systems at IRS' 12 computer centers. The manual also requires that the Assistant Commissioner for Returns and Information Processing review the NCC's and service centers' plans and certify their adequacy. The Assistant Commissioner for Support and Services is to certify the plan for the Detroit Data Center.

Under the Brooks Act (40 U.S.C. 759), the National Bureau of Standards is assigned the task of developing technical standards and guidelines for federal ADP activities. The Bureau's guidelines for developing disaster recovery plans appear in the Department of Commerce's Federal Information Processing Standards Publication (FIPS PUB) 87, Guidelines for ADP Contingency Planning (March 1981). This publication identifies the following important areas to be addressed for an effective ADP contingency plan:

- A strategy for backing up computer operations.
- Identification of work-load priorities.
- Safeguarding duplicate copies of essential data and computer programs.
- The periodic testing of the plan.

- Analysis of the risks at computer centers.

A discussion of IRS' progress in each of these areas follows.

## Backup Strategy Does Not Ensure Prompt Continuity of Operations

Both the FIPS PUB 87 and the Internal Revenue Manual stress the importance of ADP backup strategies. FIPS PUB 87 suggests that organizations consider selecting a prearranged backup facility where critical computer center tasks can be performed until a distressed facility is restored. The Internal Revenue Manual states that ADP contingency plans are to provide for such backup facilities and lists three backup options: (1) equipped contingency center—a facility fully equipped with needed hardware; (2) an empty shell—a building suited to the quick installation of computer hardware (raised floor, air-conditioning, power supply); and (3) a paired computer center—an IRS-managed ADP system that is designated to process the critical work load of the distressed center. The manual further states that, since the cost and administrative burden of backup facilities are high, other options should also be considered.

We found that the draft ADP contingency plans for IRS' service centers and NCC do not contain adequate backup strategies to ensure that critical functions will continue promptly after a major ADP disruption. We also found that IRS has not prepared an analysis of the feasibility, costs, risks, and benefits of alternative backup strategies.

The service centers' plans are based on the paired-center approach. Under this approach, a center damaged in a disaster would send its work load to its paired center for processing. This assumes sufficient computer capacity at each center to serve its counterpart. IRS' Computer Service Office questioned the viability of the paired-center approach in light of complaints by service centers of inadequate capacity to process their own work load, let alone additional work from other centers. As long as this situation exists, IRS' ability to recover service center ADP operations after a disaster, using this approach, is in doubt.

NCC's draft plan does not designate a specific backup facility to be used if its facilities are seriously damaged. Under this plan, should a disaster occur, IRS would try to locate space for a backup facility by contacting several designated IRS service centers, the Federal Emergency Management Agency, and the General Services Administration. Should these steps fail to obtain an acceptable center, IRS would then contact other federal data centers and commercial backup facilities.

NCC's plan to find a computer center after a disaster occurs presents several problems.

- The computers at IRS' service centers are not compatible with NCC's computers; therefore, NCC could not run its programs on service center computers.
- NCC has no written agreement with other federal computer centers; nor are the computers at the other federal centers fully compatible. Some may be similar to NCC's, but IRS' programs would at least need revision to run on such computers.
- Finding an acceptable empty shell and identifying and contracting for minimum system requirements could take weeks or even months. The Deputy Regional Administrator for the General Services Administration thought NCC would need more than 30 days to obtain an acceptable site and resume operations.

IRS has considered several options for backing up NCC in the last 5 years (empty shell, letter of agreement with another federal agency), but it has not selected a definite backup location for use with its ADP contingency plan. Nor has IRS prepared an overall evaluation of the relative costs, risks, benefits, and feasibility of various backup strategies for itself or NCC, as required by IRS regulations.

The Detroit Data Center has an ADP contingency plan only for the computer application system that supports the payroll function; it does not have a plan that supports the entire center.

## Work-Load Priorities Have Not Been Identified

The Internal Revenue Manual requires that all ADP contingency plans include a list, in order of priority, of the critical work-load functions to be performed by the system. After a disaster, a computer center would probably not be able to do all its work functions because it would most likely not have a complete complement of computer capacity available. IRS has not identified those work-load functions that are most critical to accomplishing its mission. IRS' draft plans simply list routine processing schedules for all functions. Therefore, in an emergency, IRS would have to take time to decide which work-load functions critical to its continued operation should receive priority.

## Backup Files Have Not Been Safeguarded

FIPS PUB 87 states that it is essential that backup copies of appropriate data and computer programs be adequately secured so that an agency can continue operations if the original versions are destroyed. IRS'

manual requires that all critical systems have backup files and that these files be kept off-site.

Although NCC had stored its required backup tapes at an off-site location, three of the four service centers—Andover, Atlanta, and Fresno—had not done so. However, the Atlanta center has recently contracted to have its tapes transported and stored off-site. We also found that backup tape files for all four service centers were incomplete. The missing files included those containing data on taxes owed, problem taxpayers, overdue returns and payments, and investigations of delinquent taxpayers. These data are important to the support of IRS programs.

We asked Fresno center officials why they did not use an off-site storage area. They replied that, because of problems in transporting tapes to an off-site location and inadequate funds to obtain a vault for that location, a decision was made to store backup tapes in a locked cabinet in a building adjacent to the one housing the computer room tape library. If a natural disaster, such as an earthquake, should strike this computer center, the original tapes and the backup tape files could be simultaneously destroyed.

## Periodic Testing Needed to Ensure Viability of Plans

Testing of ADP contingency plans is essential. FIPS PUB 87 states:

> One of the more important aspects of successful contingency planning is the continual testing and evaluation of the plan itself. Quite simply, a plan which has not been tested cannot be assumed to work.... ...if the ADP contingency plan is not subjected to continual and rigorous management review as well as to in depth testing on a scheduled basis it will fail when needed.

IRS regulations also mandate testing of the plans. The Internal Revenue Manual requires "tabletop testing" (an in-depth talk-through), as well as annual testing of significant portions of the ADP contingency plan. Test results are to be documented and evaluated.

At the four service centers we visited, officials stated that their draft plans were not tabletop-tested. One official said he thought headquarters personnel were responsible for conducting these tests.

According to IRS, it has updated and tested the NCC plan annually. At NCC, officials stated that they tabletop-tested NCC's draft plan in 1984, but they did not document the test. NCC has tested its ability to restore segments of its master files by processing backup tapes from its off-site

storage vault on NCC computers. However, because IRS has not identified a backup site for NCC's operations, NCC has not been able to test its ability to restore operations at an alternate site that may not have fully compatible hardware and software.

The Brookhaven Service Center plan was partially tested in November 1983. Approximately 3,500 quarterly tax deposit returns were shipped from Brookhaven to the Philadelphia Service Center to be processed. In March 1984, a report concluded that the test was successful. However, IRS' Disclosure and Security Division stated it did not consider this exercise to be an in-depth test of those plans because Philadelphia processed only a small portion of Brookhaven's hundreds of thousands of transactions that may need to be processed in a single day.

## Risk Analyses Provide a Useful Tool to Reduce Risk and Aid ADP Contingency Planning

Risk analyses identify the nature and magnitude of risks facing a computer center. Such information can help management decide (1) how to reduce these risks and (2) select an appropriate ADP contingency plan. Several government directives and guidelines focus on the importance of risk analyses for ADP centers. OMB Circular A-130 states that risk analyses should provide a measure of the relative vulnerabilities of the computer centers so that "security resources can be effectively distributed to minimize potential loss." It requires that federal agencies perform risk analyses

- at least every 5 years;
- before approving design specifications for new computer systems; or
- whenever a computer center's physical makeup, hardware, or software changes significantly.

The Treasury Department incorporated these requirements into directives with which IRS must comply: Treasury Directive 10-08, dated January 25, 1979, and Treasury Directive 81-41, dated November 23, 1983, which superceded the prior directive.

Besides the Treasury directives, Federal Information Resources Management Regulation (Amendment 1, December 1984) 201-7.103.2 also requires that agencies perform risk analyses "for each ADP and telecommunications facility to provide an understanding of the probable losses and the effect of these losses."

In addition, FIPS PUB 87 recommends that risk analyses be used as part of the orderly process needed to develop a contingency plan. It notes that:

With relatively few exceptions, the selection of appropriate strategies should follow the risk analysis. Until the risk analysis is done, it is usually difficult to know the critical systems which must be maintained and the demands for resources which will be made to support those critical systems. Thus, it is expected that the strategy can be, at least tentatively, selected immediately after the risk analysis is complete

## Risks Exist at IRS Computer Centers

The November 1984 risk analysis at Brookhaven, done in response to the Financial Integrity Act, and our own review at four centers revealed that risks do exist. For example, the Brookhaven analysis revealed that

- the center was susceptible to fire and smoke damage because the computer room door does not close;
- the main entrance to the computer room was not secured after normal working hours, increasing the risk of entry by unauthorized individuals; and
- smoke detectors in the computer room have produced an excessive number of false alarms to the local fire department, which could slow the response to a real fire.

Weaknesses we found at the other centers include the following:

- At the Andover, Atlanta, and Fresno Service Centers, and at NCC, access doors to the computer room were not always monitored.[3]
- At Andover and Fresno, visitor badges were left unattended, and at Fresno an access button to the computer room doors was not disconnected after duty hours.
- At Fresno, the tape library was left unlocked and unattended after normal working hours, and cleaning personnel were sometimes not monitored.
- At Austin, the tape library had no automatic sprinkler system.

## IRS Risk Analyses Have Been Resumed

Between 1979 and 1981, IRS performed risk analyses at six of its centers. It elected to have each service center concentrate on a different area of operations and analyze physical security conditions/risks. For example, the Philadelphia Service Center performed a physical security analysis on its remittance processing system, and the Austin Service Center analyzed security measures and protection for its building and grounds.

[3]In commenting on a draft of this report, IRS told us the problem with the access doors at NCC would be corrected by December 24, 1985. According to the Security Administrator at NCC the problem still had not been corrected as of February 13, 1986.

According to an IRS official, the results of these risk analyses were to be consolidated into an IRS-wide assessment. However, in September 1981, believing that its centers were reasonably secure, IRS placed a temporary moratorium on facility risk analyses, so no consolidated risk assessment was prepared.

In 1983, Treasury reviewed its internal controls, including those at IRS, in response to the Federal Managers' Financial Integrity Act of 1982. On December 31, 1983, the Secretary of the Treasury reported to the Congress and to the President that information systems security was a material control weakness throughout Treasury. Treasury then directed all of its bureaus, offices, and agencies to conduct a risk-analysis program to identify specific security weaknesses and then correct them. On February 3, 1984, IRS began implementing a new risk-analysis program for its 12 computer centers. A contractor performed the first risk analysis at Brookhaven in November 1984 and the second risk analysis at Fresno in January 1986; the other centers are to follow. IRS intends to act on security weaknesses identified in the Brookhaven analysis and has developed an action plan to make improvements.

In his October 21, 1985, letter, the IRS Commissioner reported to the Secretary of the Treasury that IRS had determined that it was in noncompliance with OMB Circular A-71 (now A-130) regarding security of automated information systems. Specifically, the letter stated that IRS planned to conduct risk analyses for all centers by September 30, 1987, and also to develop contingency plans.

## Internal Studies Have Noted Problems in ADP Contingency Plans

Both IRS' Disclosure and Security Division and Internal Audit Division have identified problems in IRS' ADP contingency plans. In 1981, the Disclosure and Security Division recommended an IRS-wide approach to disaster recovery planning. IRS issued a handbook containing standards for ADP contingency planning and testing in February 1983, but it paid little attention to the subject until the 1983 fire at Brookhaven. As a result, the IRS' Returns and Information Processing Division, in August 1983, asked the service centers to reevaluate and update their existing plans in accordance with the February 1983 handbook. A copy of Brookhaven's updated plan was also submitted to each service center to be used as a guide. Except for the Detroit Data Center, each center submitted an updated plan to IRS headquarters between September 1983 and January 1984.

These plans were sent to the Disclosure and Security Division for review, which concluded in March 1984 that the Brookhaven plan, as well as most of the other centers' plans, omitted almost all of the major elements required by the handbook. The division criticized the plans for not

- including recovery operations procedures,
- specifying a prearranged location for a backup facility,
- listing critical ADP work-load processing priorities,
- stating the minimum number of personnel required to operate the critical ADP systems,
- listing critical amounts and types of supplies and office equipment, and
- addressing how the plans would be tested.

Disclosure and Security also reviewed NCC's plan and concluded that the plan would not work without a designated backup facility, needed to better address critical ADP operations and processing priorities, and required adequate testing to ensure that it would work.

IRS' Internal Audit Division reviewed the security program and issued a report on December 6, 1984, noting that, at the time of its audit work, IRS had no current contingency plans for half of its 12 centers. In addition, the report noted that the six existing plans had not been reviewed by Disclosure and Security and were insufficiently tested to determine their feasibility of implementation or adequacy of protection.

IRS management responded that updated plans for the 10 service centers had been submitted to and reviewed by Disclosure and Security between November 1983 and May 1984. Disclosure and Security concluded that the service center and NCC plans did not conform to IRS requirements and would need improvement to make them workable. IRS management said that, in light of this needed improvement and doubts about the viability of the paired-center approach, a task group, comprised of representatives from the offices of three assistant commissioners, had been set up to develop a model disaster recovery plan for service centers. However, on November 9, 1984, the task group determined that the scope of the problem was so complex that

> ...this project would require input from many additional field and national office staff and would require the full time participation of the task group members to produce a detailed and adequate plan.

The group therefore proposed hiring a consultant to develop the model plan. The work of this task group was suspended in November 1985. On December 17, 1985, IRS' Automation Policy Board granted approval for the Assistant Commissioner (Computer Services) to appoint a contingency planning project officer. The officer's initial task, to be completed about March 1986, is to develop time frames and estimate resources to help decide whether to establish a contingency planning office.

## Contingency Planning and Risk-Analysis Efforts Are Progressing Slowly

ADP contingency planning and risk analyses at IRS are progressing slowly. In 1986, almost 8 years after OMB required federal agencies to develop, maintain, and periodically review and test ADP contingency plans, IRS still does not have tested, certified plans. The circular also required that risk analyses be performed at least every 5 years or earlier if significant changes in facilities, hardware, or software occur. However, IRS still has not conducted risk analyses at all of its centers, even though significant hardware and software changes have taken place.

In 1977, we reported that IRS' controls over computer operations were not adequate to prevent unlawful disclosure of tax data.[4] We pointed out that IRS' weak enforcement of its security regulations occurred because responsibility was fragmented among four organizations within IRS. Because these organizations had other functions to perform, security matters generally received less priority attention. We therefore recommended that the Commissioner establish an independent security office responsible for all facets of the security program at IRS. The Commissioner agreed that IRS had not been aggressive in the security area and committed the agency to a vigorous course of improvement including, among other things, undertaking a major risk-analysis effort. In April 1978, IRS established a single organization to oversee its security program.

In September 1981, however, IRS decentralized its approach to security enforcement and later began reducing the number of security personnel. This change was made because IRS believed that controls were in place, managers were more security conscious, and the need for additional security procedures had diminished. IRS placed a moratorium on risk analyses that continued through 1983.

[4]IRS Security Program Requires Improvements to Protect Confidentiality of Income Tax Information (GGD-77-44, July 11, 1977).

As indicated earlier, Treasury revitalized the current risk-analysis program after identifying ADP security as a material weakness in a December 1983 assessment of its internal control systems. Yet IRS has completed only two risk analyses at two centers as of January 1986.

Furthermore, the need for tested, certified contingency plans became readily apparent to IRS after the Brookhaven fire. However, as of January 1986, over 2 years after this incident occurred, IRS still does not have tested, certified contingency plans for its 12 centers.

# Advance Comments From the Internal Revenue Service

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

COMMISSIONER OF INTERNAL REVENUE

Washington, DC 20224

Mr. William J. Anderson
Director, General Government Division
United States General Accounting Office
Washington, DC 20548

Dear Mr. Anderson:

We appreciate the opportunity to review your recent draft report entitled "Computer Security: Contingency Plans and Risk Analysis Needed for IRS Computer Centers."

We generally agree with the report's findings and recommendations concerning our efforts in this area. The report repeats information that has previously been presented to and considered by Service management as a result of reviews conducted within the Service by both our Internal Audit and Disclosure & Security Divisions.

We strongly agree that a tested contingency plan is necessary to enable us to continue processing in the event of a disaster. We realize that our progress in dealing with this issue has been limited due to the complexity of the task and the lack of available resources to address the problem. In fact, the Disclosure & Security Division submitted these issues as material weaknesses to the Commissioner for inclusion in the A-123 annual assurance letter to the Secretary of the Treasury in September, 1985. We believe that overall we are making good progress in bringing the Service into compliance with OMB regulations and our own Internal Audit recommendations, as well as GAO's conclusions in this report.

Our FY 1986 Annual Plan for Risk Management, which was issued in September, 1985, reflects the Service's awareness that risk analyses at our 12 major sites are needed, but cannot be completed by the end of 1986. This current plan also includes the use of contractor services for at least two sites (with an option to expand to others) and the National Office, as well as a team of Service employees to conduct risk analyses at remaining sites. A copy of this plan was provided to GAO. Consequently, the comments contained on pages 9, 13, and 30 of the draft report which indicate that the Service plans to complete risk analyses at all of its centers by 1986 is inaccurate. The process will not be completed until 1987.

See comment 1.

Department of the Treasury Internal Revenue Service

Mr. William J. Anderson

We do not agree with the statement on page 2 that the problems encountered in the 1985 filing season could have been avoided or significantly reduced if tested, certified ADP contingency plans were in existence. The type of contingency planning contemplated by the review (i.e. plans to address risks of "natural disaster, fire, accident or sabotage") would not be generally applicable to problems that arise in the implementation of new systems and operations.

See comment 2.

We would also like to clarify several portions of the draft report's discussion of the National Computer Center (NCC). NCC has a disaster recovery plan which is updated and tested annually. Although it does not currently conform to the precise requirements of Internal Revenue Manual section 1(16)24, it is being revised and will soon be submitted for certification. A statement on page 24 of the draft report could be interpreted to suggest that NCC's back-up tapes were incomplete. We believe such an interpretation would be incorrect. NCC's back-up tapes were tested quarterly and no deficiencies were found. The weakness in NCC's computer access system, noted on page 29, will be corrected no later than December 24, 1985. On page 32, the draft report comments that NCC was "not storing magnetic media file back-up tapes in designated storage areas." This was true for the on-site tapes, but they would have no bearing on their ability to recover from a disaster because the tapes to be used for disaster recovery are stored off-site, as required. Lastly, a comment on page 33 states that contingency plans were updated and submitted to NCC. This is not correct; plans were actually submitted to the Disclosure & Security Division.

See comment 3.

See comment 4.

See comment 5.

See comment 6.

See comment 7.

Issues contained in your draft report were discussed at a December 17, 1985, meeting of the Automation Policy Board. At that meeting, the Assistant Commissioner (Computer Services) was given approval by the Board to appoint a contingency planning project officer. The officer's initial task, which should be completed in about 60 days, will be to establish time frames and calculate the resources that would be associated with a contingency planning office. The Board will then review these time frames and resource estimates and decide whether or not to officially approve the new project office.

With kind regards,

Sincerely,

Acting Commissioner

The following are GAO's comments on IRS' letter dated December 30, 1985.

## GAO Comments

1. According to IRS' 1986 plan, risk analyses at six service centers and the National Office (IRS headquarters) are scheduled to begin in fiscal year 1986. No completion date was stated. However, IRS now informs us that completion at all centers will be in 1987, which we so note on pages 1, 5, 7, and 19.

2. We added language on page 1 to clarify that the problems encountered by IRS during the 1985 filing season derived in part from computer capacity shortages. See also our comment on pages 8 and 9.

3. Even though IRS said that it updates and tests the NCC plan annually, we have pointed out the weaknesses in its tests on pages 16 and 17. We added a statement to the report on page 9 to acknowledge that IRS is revising the NCC plan and intends to submit it for certification soon.

4. We deleted language that implied NCC backup tapes were incomplete.

5. According to NCC's Security Administrator, the access problem still had not been corrected as of February 13, 1986.

6. In our draft we referred to a December 6, 1984, report issued by IRS' Internal Audit Division, which disclosed that NCC was not properly storing its backup tapes. IRS accurately points out that Internal Audit was referring to on-site backup tapes rather than off-site backup tapes. Because these on-site tapes were not properly stored in tape libraries or in on-site storage vaults, the Internal Audit Division had properly concluded that "the Service [IRS] may be hindered from recovering quickly in the event of a local disaster." (Emphasis added.) While the on-site backup tapes, if properly stored, could be used to recover from a local disaster, IRS correctly points that its off-site backup tapes are maintained to recover from a disaster, whether local or not. Accordingly, we have dropped this point from the report.

7. We revised page 20 to note that plans were submitted to IRS' Disclosure and Security Division.

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

3390

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

Official Business
Penalty for Private Use $300

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100