BY THE U.S. GENERAL ACCOUNTING OFFICE

Report To The Secretary Of The Treasury

Unreliable Evaluations Detract From Treasury's Progress To Implement The Financial Integrity Act

Again this year, GAO conducted reviews of 23 federal agencies' efforts to implement the Federal Managers' Financial Integrity Act of 1982. The act is intended to help reduce fraud, waste, and abuse in government operations through annual agency self-assessments of internal controls and accounting systems.

This report discusses how Treasury's efforts in closely following existing guidelines resulted in continued progress in its implementation of the act. Notwithstanding the progress that was made, Treasury needs to improve its evaluation process in certain areas to better assure that the process can be relied on to determine the adequacy of Treasury's internal controls. Treasury's managers are confused regarding the vulnerability assessments, a crucial element of the evaluation process, which caused the assessments to be unreliable. Treasury needs to develop guidance that reduces the present complexity and subjectivity of the assessments. GAO recommends several actions designed to do this.

UNITED STATES GENERAL ACCOUNTING OFFICE

GAO/GGD-86-10
OCTOBER 10, 1985

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

GENERAL GOVERNMENT
DIVISION

B-216946

The Honorable James A. Baker III
Secretary of the Treasury

Dear Mr. Secretary:

This report concerns Treasury's efforts to implement the requirements of the Federal Managers' Financial Integrity Act of 1982. The report highlights the progress made and problems encountered by Treasury in implementing the act. The report focuses on

--the status of actions taken to correct identified weaknesses,

--the quality of critical evaluations which have comprised the bulk of Treasury's efforts under Section 2 of the act,

--improvements needed in evaluating ADP controls, and

--improvements needed in accounting system reviews.

The report contains recommendations to you on pages 16, 32, 42, 54, and 55. 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 Senate Committee on Governmental Affairs and the House Committee on Government Operations not 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 the report to the Director, Office of Management and Budget; the Internal Control Management Officer for each of Treasury's 13 organizational units; and interested committees of the Congress.

Sincerely yours,

W.J. Anderson

William J. Anderson
Director

EXECUTIVE SUMMARY

The Treasury Department acts as the government's financial agent, manages the public debt, collects taxes, handles a cash flow of $6 billion daily, and makes up to 700 million payments annually. Because of these important missions, GAO reviewed Treasury's fiscal 1984 progress in evaluating the adequacy of its internal controls and accounting systems under the Federal Managers' Financial Integrity Act.

BACKGROUND

The act requires that executive agencies evaluate their systems of internal accounting and administrative controls relative to standards prescribed by the Comptroller General to determine whether they provide reasonable assurance that (1) obligations and costs comply with applicable law; (2) funds, property and assets are safeguarded; and (3) revenues and expenses are properly accounted for. Agency heads must report annually to the President and the Congress on the results of these evaluations. Each agency must also report on whether its accounting systems conform to the Comptroller General's principles, standards, and related requirements.

RESULTS IN BRIEF

Treasury is making progress in correcting the two departmentwide material weaknesses identified in fiscal 1983 and the numerous weaknesses identified by its bureaus. Treasury is also bringing its accounting systems into conformance with the act's requirements.

In 1984, Treasury reported (1) it did not have any departmentwide material weaknesses, (2) it had reasonable assurance that the act's objectives were achieved, and (3) 6 of its 26 accounting systems fully conformed to the act's requirements. However, GAO believes Treasury does not yet have a sufficient basis to determine whether its internal control and accounting systems comply with the act because:

--critical evaluations (vulnerability assessments) were unreliable,

--all significant ADP systems and controls were not assessed, and

--accounting system evaluations were of insufficient depth and scope.

PRINCIPAL FINDINGS

Corrective Actions

Treasury is developing a uniform system to safeguard its personal property and is correcting weaknesses in the security of its ADP systems--the two material internal control weaknesses it reported in fiscal 1983. Also, the bureaus have completed about 40 percent of the corrective actions planned to address 140 weaknesses identified by the bureaus in fiscal 1983 and 1984. For example, one bureau improved the security of monthly shipments of $10 million in savings bonds and government checks. Other significant reported weaknesses still need to be corrected. For example, one bureau needs to implement security improvements in its electronic transfers of $4.5 billion annually. (See pp. 7 to 9.)

Treasury has also begun many improvements to bring 20 accounting systems into conformance with the act's requirements. For example, a major redesign is underway of the Public Debt Accounting System, which processes several trillion dollars of transactions annually. (See pp. 45 and 46.)

Inadequate Evaluations

Treasury's internal control and accounting system evaluations, however, need to be improved to reasonably assure that material weaknesses are being identified.

Vulnerability assessments are critically important because they identify which agency functions are most vulnerable to problems. They also are the basis for determining where internal control reviews, which test suspected controls in operation, and other corrective actions should be directed. (See pp. 17 and 18.)

Treasury's vulnerability assessments were unreliable. There were major differences in how managers of the same function rated like variables in the assessment, and managers frequently did not consider major operations of an assessed function. For example, the Internal Revenue Service's Information Returns Program is used to verify income reported by taxpayers. IRS managers overlooked operations involving income information received on magnetic media tape--which accounts for 80 percent of all program documents received. (See pp. 22 to 28.)

Furthermore, although Treasury established a risk management program to evaluate ADP systems, significant ADP systems and important internal controls were not assessed. For example, the Office of the Comptroller of the Currency had eight ADP systems that were not evaluated under the program or through vulnerability assessments. Also, important controls over data input validation and editing, which are needed to assure that erroneous data is detected before processing, were not assessed. (See pp. 36 to 40.)

A New Approach

Treasury's Customs Service is developing an approach which may improve the reliability of future vulnerability assessments. Also, Treasury needs to modify its risk management program to assure coverage of all ADP systems and controls. (See pp. 28 and 36.)

Accounting Systems

Treasury reported 6 of its 26 accounting systems conformed with the Comptroller General's principles, standards, and related requirements; 2 systems did not conform; and 18 systems conformed in all material respects, except for a limited number of instances of nonconformance. To address these problems, corrective actions have been taken or planned, including some major system redesigns. Although Treasury is making progress, its accounting system evaluation program can be improved by ensuring that (1) all major systems are tested in operation and (2) regional/field accounting operations are evaluated. (See pp. 45 to 56.)

RECOMMENDATIONS

GAO recommends that the Secretary of the Treasury take several actions. These actions include (1) testing Customs' planned assessment approach on a sample basis at other bureaus to ascertain the desirability of adopting it departmentwide, (2) requiring bureaus making vulnerability assessments before completion of the above tests to take certain actions to improve the reliability of the assessments, and (3) expanding accounting system examinations and testing. (See pp. 16, 32, 42, 54 and 55.)

AGENCY COMMENTS

Treasury commented that, overall, GAO's technical analyses reinforced some of its conclusions about the Department's process. Treasury concurred with some of GAO's recommendations, but had reservations about others. Department reservations and GAO's evaluations are detailed at the end of each chapter.

Although concurring with GAO's analyses and many of GAO's recommendations, the Department expressed particular concern with GAO's conclusion on its ability to assert reasonable assurance in its required annual statements to the President and the Congress. Treasury expressed this concern because (1) its vulnerability assessments were not the sole basis for its assurance statements and (2) it has adhered to OMB instructions.

GAO acknowledges that the assessments were not the sole basis for Treasury's assurance statements; however, they comprised the bulk of Treasury's efforts and formed the foundation of its process. Also, GAO has previously recommended that OMB revise its guidance for the year-end reporting statement. For these and several other reasons, GAO believes its conclusion is sound. (See pp. 14, 32, 42 and 55.)

Contents

TABLES

TABLES

ABBREVIATIONS

ADP	Automatic Data Processing
FIA	Federal Managers' Financial Integrity Act
GAO	General Accounting Office
IRS	Internal Revenue Service
OCC	Office of the Comptroller of the Currency
OMB	Office of Management and Budget

CHAPTER 1

INTRODUCTION

In September 1982, the Congress enacted the Federal Managers' Financial Integrity Act of 1982 (P.L. 97-255) in response to continuing disclosures of waste, loss, unauthorized use, and misappropriation of funds or assets across a wide range of government operations. The goal of this legislation is to help reduce fraud, waste, and abuse and to improve management of federal operations. The act provided, for the first time, the necessary governmentwide discipline to identify and remedy internal control and accounting systems problems that hamper effectiveness and accountability, potentially cost the taxpayer needless dollars, and diminish the public's confidence in the government. The Department of the Treasury is 1 of 23 agencies included in our review of the status of federal agencies' efforts to implement the act during the second year.

FRAMEWORK ESTABLISHED TO IMPLEMENT THE ACT

The Federal Managers' Financial Integrity Act (FIA) reiterated the concept first incorporated in the Accounting and Auditing Act of 1950 that the primary responsibility for adequate systems of internal control and accounting rests with management. The act has two primary sections to address this concept--section 2 and section 4.

Section 2 requires that agency systems of internal accounting and administrative control must comply with internal control standards prescribed by the Comptroller General and must provide reasonable assurance that

- --obligations and costs are in compliance with applicable law;
- --funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and
- --revenues and expenditures are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

Agency heads are required to prepare annual statements to the President and the Congress on whether their internal control systems fully comply with the act's requirements. To the extent that the systems do not comply, the act requires the identification of any material weaknesses in their systems together with plans for corrective actions.

Section 4 of the act further requires that agency heads make another annual statement on whether the agencies' accounting systems conform to the Comptroller General's accounting principles, standards, and related requirements. These encompass internal controls.

To provide the framework for implementation, as prescribed by the law, the Comptroller General issued standards in June 1983 for agencies to meet in establishing their internal control systems. The standards apply to program management as well as to traditional financial management areas and encompass all operations and administrative functions.

The Office of Management and Budget (OMB), in consultation with us, issued guidelines in December 1982 for agencies to use in evaluating, improving, and reporting on their internal control systems. In short, OMB's guidelines provide that agencies segment their programs and functions into assessable units which are then assessed for vulnerability to fraud, waste, and abuse; take corrective actions for vulnerable units (such as through detailed internal control reviews which evaluate and test the adequacy of controls in place); and identify, report, and correct all known material control weaknesses.

TREASURY'S ORGANIZATION AND OPERATIONS

The Department of the Treasury has a wide range of diverse and critical duties. These include (1) formulating domestic and international financial, economic, and tax policy; (2) serving as the financial agent of the government; (3) manufacturing coins and currency; (4) managing the public debt; (5) collecting federal revenues through various taxes; and (6) enforcing various laws related to such matters as firearms and explosives, imports and exports, counterfeiting, and tax evasion. Overall, Treasury accounts for a cash flow of about $6 billion daily and makes an estimated 600 to 700 million payments annually.

Treasury has about 116,000 employees in 13 major bureaus and offices (hereafter referred to as bureaus). Eight of these bureaus have field offices to carry out their responsibilities. The 13 major bureaus are listed below:

- --Bureau of Alcohol, Tobacco and Firearms
- --Internal Revenue Service (IRS)
- --U.S. Secret Service
- --Bureau of Engraving and Printing
- --Financial Management Service (formerly Bureau of Government Financial Operations)
- --Office of the Secretary
- --U.S. Customs Service
- --Bureau of the Public Debt
- --Office of Revenue Sharing
- --Office of the Comptroller of the Currency (OCC)
- --U.S. Mint
- --U.S. Savings Bonds Division
- --Federal Law Enforcement Training Center

Overall responsibility for directing, coordinating, and reporting on the internal control evaluations was assigned to the Assistant Secretary (Management). Internal control officers appointed by bureau heads are in charge of day-to-day administration of the internal control evaluation, improvement, and reporting processes.

The Assistant Secretary (Management) and the Fiscal Assistant Secretary were responsible for the evaluations of the administrative and fiscal accounting systems, respectively. Day-to-day responsibility was delegated to a specially created task force which established policies, procedures, and guidelines for evaluating accounting systems and reporting on the results.

OVERVIEW OF TREASURY'S 2-YEAR EFFORTS

Treasury issued its first report under the act on December 27, 1983. Treasury reported that its evaluation process indicated that, on the whole, its system of internal controls complied with the objectives of the act.[1] Also, Treasury reported that it found no indication of serious problems with the operational integrity of its accounting systems. The annual report identified two major categories of departmentwide weaknesses--information systems security and personal property management. Because weaknesses in data processing, office automation, telecommunications, etc. were frequently acknowledged by the bureaus, Treasury's annual report recognized that its separate program of risk assessment and control over ADP resources must be improved. Similarly, Treasury reported that efforts were underway, both on a bureau and department basis, to improve accountability for personal property.

The report further stated that in 1984 the Department would require the bureaus to resegment their operations into assessable units and perform vulnerability assessments on the new units to overcome recognized deficiencies. The Department also planned to revise various policy memorandums, update information to the bureaus, and issue an Internal Control Handbook to provide more complete guidance on implementing the program. Additionally, the Department planned to strengthen its training program by (1) preparing instructional films for the bureaus and (2) developing training modules or courses on the various phases of the program. Finally, the Department planned to improve monitoring of the bureaus' activities by completing an automated tracking system and having teams make periodic visits to the bureaus to assess the quality of their efforts.

---

[1]We reported that problems with Treasury's internal control evaluation process prevented a conclusive assessment of its internal controls (GAO/GGD-84-66, May 25, 1984).

Treasury's second report, issued on December 31, 1984, said that its evaluation process indicated that, taken as a whole, Treasury's systems of internal accounting and administrative control provide reasonable assurance that the objectives of the act were achieved. Unlike 1983, Treasury did not identify any significant material weaknesses in its systems of internal control. However, reference was made to continuing progress in remedying deficiencies reported in 1983. Also, Treasury reported that it had taken the necessary measures to assure that the evaluations of its accounting systems were conducted in accordance with the standards prescribed by the Comptroller General in a memorandum to agency heads dated April 18, 1983.

OBJECTIVES, SCOPE, AND METHODOLOGY

We reviewed Treasury's implementation of the act because of the high priority given by the President and the Congress to improving the government's internal controls. We did not attempt to evaluate Treasury's internal control systems, the results of actions taken by Treasury to improve those systems, or the extent to which Treasury's accounting systems comply with the Comptroller General's principles and standards.

The objectives of our review were to

--evaluate Treasury's second year progress in implementing its internal control and accounting system evaluation processes;

--determine whether Treasury bureaus were taking necessary corrective actions;

--assess the reasonableness of Treasury's second annual assurance reports; and

--determine whether the vulnerability assessments (required evaluations of the susceptibility of Treasury's programs or functions to waste or loss) were reliable.

We conducted audit work at all of Treasury's bureaus and offices involved with the process except for the Federal Law Enforcement Training Center. We did not evaluate the center's efforts because of its location (Glynco, Georgia) and small size. Our work involving the internal control process (section 2) consisted of interviewing the designated internal control officers and their staffs in each bureau, Inspector General staff, selected program managers, officials responsible for ADP and Risk Management Program (a Treasury ADP evaluation effort), and representatives of the management consulting firm of McManis Associates, Inc. (which assisted Financial Management Service in conducting its internal control reviews). Moreover, we examined and analyzed relevant correspondence; directives and procedures, including those for the Risk Management Program; and internal control reviews and their accompanying documentation. We also determined the status of corrective actions at all bureaus and examined several specific actions at four bureaus.

Although we obtained information on all the bureaus' efforts to complete the accounting system (section 4) evaluation process, we examined in more detail 12 accounting system evaluations at four bureaus--the Bureau of the Public Debt, Financial Management Service, IRS, and Customs Service. These bureaus were selected because they provide financial management services essential to government operations and/or control significant amounts of revenues. These 4 bureaus operate 14 of Treasury's reported 26 accounting systems.

Specifically, we reviewed (1) the bureaus' identification of accounting systems subject to FIA to assure that all such systems were identified; (2) the actual accounting system evaluations by interviewing bureau staff and reviewing evaluation documentation and testing performed; and (3) internal audit or Inspector General workpapers and reports.

We also observed system evaluations conducted by contractors engaged by the Financial Management Service. We reviewed their work at the Financial Management Service's disbursing offices in Washington, DC; Philadelphia, PA; Austin, Texas; and San Francisco, CA. We selected these locations because these regional disbursing offices were being evaluated by Treasury for the first time under FIA.

Our review was conducted between May 1984 and March 1985 and was performed in accordance with generally accepted government auditing standards.

To address the reliability of vulnerability assessments, we reviewed 818 vulnerability assessments made by four bureaus (IRS, Customs, Mint, OCC). These bureaus accounted for about 80 percent of Treasury's assessable units and about 88 percent of the vulnerability assessments made in 1984. (See table I.1, app. I.)

Given the diversity of bureau missions and the need to acquire a working knowledge of the assessable units reviewed, most of our fieldwork was on the assessments of the Customs Service. We selected Customs because its assessments closely followed OMB guidelines and it is the second largest bureau. Our field work was conducted in four of Customs' seven regions, and it involved the regional assessments made for seven different functions. A total of 22 assessments were reviewed. These units were selected because of the wide ranges in the vulnerability ratings assigned by the various regions. (See table I.2, app. I.)

In addition, supplemental fieldwork was also done for two IRS assessments and one Financial Management Service assessment. The IRS assessments were for two assessable units of its Information Returns Program: (1) returns and information processing and (2) examinations. This work was done at IRS' Central Region's Service Center and Midwest Regional and District office, respectively. At Financial Management Service's Philadelphia Regional Financial Center, our work concerned the assessment for Treasury's Financial Communications System unit. We examined these assessments (1) because of their relation to a major federal program and (2) to examine an assessment which appeared to have overlooked major internal control weaknesses.

CHAPTER 2

TREASURY CONTINUED TO MAKE PROGRESS IN IMPLEMENTING THE FINANCIAL INTEGRITY ACT

Treasury made progress in correcting the material weaknesses identified in 1983 and 1984 by the bureaus. Also, Treasury continued to develop an agencywide method to evaluate internal controls in conformance with the act. The bureaus issued needed guidance, conducted about 1,500 new vulnerability assessments, and completed 42 internal control reviews in fiscal year 1984. Notwithstanding the progress that was made, material weaknesses identified by the bureaus remain to be corrected and departmentwide staffing has been insufficient for effective monitoring of the bureaus' processes.

CORRECTIVE ACTIONS HAVE BEEN TAKEN TO ADDRESS PROBLEMS

Treasury is working to correct both departmentwide and bureau related weaknesses identified by its internal control evaluation efforts in 1983 and 1984. Based on an analysis of the bureaus' reported weaknesses, Treasury reported in 1983 two major categories of departmentwide material weaknesses: personal property management and information systems security. In 1984, Treasury reported considerable progress in developing, adopting, and implementing a standardized property management and control system. For example, a uniform bar coding identification has been designed to improve inventory control of property assets.

To address the material weakness in information systems security and criticisms of its 1983 evaluation of ADP controls, Treasury instituted an ADP Risk Management Program. According to OMB, Treasury's program is one of the few programs which formalizes requirements for assessing risk in ADP systems throughout a federal agency. While this is a step in the right direction, information systems security weaknesses still exist and improvements are needed in Treasury's evaluation of ADP internal controls. This is discussed further in chapter 4.

Material weaknesses and corrective actions reported by Treasury's bureaus tend to be concentrated in several Treasury bureaus and offices which are smaller in size and scope of mission. They also tend to concern administrative rather than operational issues. According to Treasury, as of September 30, 1984, the bureaus completed 45 of the 82 corrective actions planned to address the 51 material weaknesses reported to the Department by the bureaus in fiscal year 1983. Twenty-nine of these weaknesses were reported by the U.S. Mint, Office of Revenue Sharing, and the Office of the Secretary. These three components completed 23 of their 43 proposed corrective actions.

According to Treasury's 1984 report, the bureaus completed 46 actions (36 percent) of the 127 corrective actions planned to address the 89 material weaknesses reported to the department in fiscal year 1984. Two bureaus--the Comptroller of the Currency and the Federal Law Enforcement Training Center--accounted for 55 of these reported material weaknesses. These two bureaus completed 24 of their 77 proposed corrective actions.

Many of the reported weaknesses for fiscal years 1983 and 1984 (about 75 percent in our judgment) concerned administrative matters, such as outdated or no operating manuals; inadequate policies and procedures; insufficient staffing, training, and other personnel matters; and reorganization problems. Other reported weaknesses were more closely aligned to actual operations. Some examples of completed corrective actions follow.

In 1983, Public Debt reported that it needed to improve security for the $10 million in savings bond stock and government checks shipped monthly from the manufacturer's plant to its vault in Washington, D.C. Public Debt took corrective actions, including providing for armed guards to accompany the shipments.

In another instance, the U.S. Mint better controlled its access to the ADP area at the Philadelphia Mint to ensure adequate security over the processing of payroll checks, and it improved the safeguarding of its shipments of coin dies. If stolen or lost, the dies could be used to make counterfeit coins.

Customs Service reported in 1983 that it lacked an accountability system for its seized property program, which involves millions of dollars in assets seized in its enforcement operations. It established a task force to recommend policy changes and address problems and designed a property management system in February 1984. Customs Service also established a steering group to recommend and implement short- and long-term improvements. Implementation of the new seized property management system began in March 1984 and is expected to be completed in December 1985.

While Treasury has made progress in correcting the material weaknesses identified by the bureaus, reported weaknesses still exist. For example, the Savings Bonds Division needs to implement a comprehensive property management system.

Among the weaknesses remaining to be corrected are several that directly affect bureau missions or operations. For example, the Office of Revenue Sharing noted that the potential for fraud existed in its transfer of funds ($4.5 billion annually) through the Federal Reserve Direct Deposit System. The Office has been participating in a departmentwide study of electronic fund transfers and is planning to improve the security of its electronic transfer of funds by December 1985. Public Debt is studying ways to improve controls over agents and employees involved with the sale and redemption of savings bonds because of a theft of about $450,000 in unissued bond stock. In addition, Customs Service has established a task force to identify options for enhancing controls over its payments of overtime to inspectors. In fiscal year 1983, overtime amounted to about $85 million.

OTHER SECOND YEAR EFFORTS: CONTINUED PROGRESS

Treasury bureaus continued the momentum initiated in the first year. In addition, Treasury has responded to suggestions offered last year by OMB, the Inspector General, and GAO regarding the evaluation of its internal controls.

Ten of 12 bureaus we reviewed assigned additional employees to their quality assurance efforts in fiscal 1984. This represents an increase of about 6 full-time and 83 part-time employees over fiscal 1983 staffing levels. Also, Treasury issued its revised internal control directive on November 7, 1983, to recognize the subsequent enactment of the Financial Integrity Act, OMB guidance and GAO standards. Four Treasury bureaus (Customs; Savings Bonds; Alcohol, Tobacco and Firearms; and Engraving and Printing) issued their own internal control directives, and three other bureaus (IRS, Public Debt, and the U.S. Mint) had a draft internal control directive to augment OMB's and Treasury's guidance.

Nine of the 12 bureaus resegmented their operations into smaller assessable units, increasing their units from 534 in 1983 to over 2,100 assessable units in 1984. The resegmentation generally included increased participation from program and field managers. The resegmentation resulted from concerns we raised last year that assessable units were too broad and bureaus with field operations (five of eight) did not involve field managers.

Treasury's 1984 vulnerability assessments were done in accordance with OMB guidelines. All of the Treasury bureaus reviewed, except Office of Revenue Sharing, Office of the Secretary, Financial Management Service, and Bureau of the Public Debt, conducted new vulnerability assessments for a majority of the assessable units in fiscal year 1984. These four bureaus remained on the 2-year cycle adopted by Treasury in 1983 and plan to perform their second round of vulnerability assessments in fiscal year 1985.[2]

[2] Public Debt did perform vulnerability assessments on three new assessable units.

Treasury's bureaus also organized and conducted internal control reviews of suspected internal control weaknesses. The bureaus had completed 42 as of September 30, 1984. Twenty-eight of the internal control reviews were done in Financial Management Service; Bureau of Alcohol, Tobacco and Firearms; and Bureau of the Public Debt. The bureaus' reviews were generally conducted on units rated as highly vulnerable and were usually done by managers or staff members in the areas being reviewed and done in accordance with OMB guidelines. However, Financial Management Service contracted with the management consulting firm of McManis Associates, Inc., to perform its internal control reviews.

PARTS OF PROCESS NEED IMPROVEMENT

Treasury needs to provide better departmentwide oversight of its bureaus' efforts. Also, certain aspects of two bureaus' efforts need to be improved.

Better departmental oversight needed

Because of recognized deficiencies in its first year efforts, Treasury essentially started over in fiscal 1984. Treasury's bureaus resegmented their operations, provided training, and made additional vulnerability assessments and internal control reviews. In light of all the new work, Treasury's departmental oversight team should have more effectively monitored the bureaus' efforts. OMB's guidelines state:

> "It is critical that an Executive agency, whether large or small, carefully organize and assign responsibilities in a manner that ensures that the evaluation, improvement, and reporting on internal controls is conducted in an efficient and effective manner. This includes providing for quality assurance over the entire process."

For fiscal 1983, Treasury had a team which (1) visited each bureau to determine the status and commitment of its efforts, (2) reviewed some of each bureau's vulnerability assessments for compliance with OMB requirements, and (3) provided feedback to each bureau on its overall efforts.

For fiscal 1984, the Department planned to monitor the bureaus' activities by having teams make periodic visits to ensure that bureau procedures would produce quality products on which the Secretary could rely. The teams were to prepare reports for the departmental internal control coordinator to serve as a basis for follow-up action to address problems discovered in the visits. However, due to shifting departmental priorities, these objectives were not met.

FIA staff at 11 bureaus told us that the 1984 departmental quality review visits consisted of discussing the status of the bureaus' programs. Department oversight involved checking on the number of vulnerability assessments, internal control reviews, and corrective actions completed, rather than the quality of the work. In addition, Treasury's Internal Control Handbook, which was to provide more complete guidance on the various steps of implementing its program, was never completed and was issued as a draft.

FIA staff at nine bureaus stated they received very little feedback from Treasury on the quality of their FIA efforts in 1984. They said this created an impression among bureau managers and FIA staff that Treasury was not overly concerned with the results of the process, but rather in meeting its milestones and completion dates. They also said that the way FIA was being implemented resulted in a paperwork burden. In addition, FIA bureau officials expressed concern that the program could become a self-perpetuating effort with only lip service being provided to the program's true objectives.

For fiscal 1984, the Department also planned to monitor the bureaus' activities through the Treasury Internal Control System. This tracking system is intended to be an automated data base management system which would maintain a complete inventory of Treasury's assessable units, including a record of the results of all vulnerability assessments, internal control reviews, and actions taken to correct deficiencies.

Our review of the Department's tracking system's information printout for seven bureaus showed that the system was not fully operational in fiscal year 1984. The information was outdated and incomplete. New assessments had been performed; but the data had not been captured, and the results of all internal control reviews, Inspector General reports, and corrective actions had not been included. For example, the results of 16 vulnerability assessments and proposed corrective actions at the Bureau of Engraving and Printing were not listed on the tracking system printout. In addition, the information from two internal control reviews and an Inspector General report conducted at Public Debt were not listed. Treasury officials stated that problems with system programs and hardware caused the operating delay.

Individual bureaus have implemented their own manual or computerized tracking system to monitor progress and results, and they are providing information to the Department. The bureaus have been waiting since December 1983 for the departmentwide system to become fully operational. One bureau commented that the system is not accessible, and the bureau derives no benefit from the system. In addition, one bureau official stated that its vulnerability assessments were completed 8 months ago and that being required now to provide updated information on these assessments raises questions as to how much use the Department is making of the tracking system.

The change in Treasury's fiscal year 1984 oversight can be attributed to two factors. First, the Department had a turnover in 1984 of its three senior FIA officers. Personnel changes occurred with Treasury's Assistant Secretary (held by three different persons) and Deputy Assistant Secretary and with the Director of the Office of Management and Organization--the office responsible for directing and overseeing implementation of the act at Treasury. Second, the staff assigned to oversee Treasury's departmentwide implementation were also assigned responsibility to implement the act for the Office of the Secretary--1 of Treasury's 13 organizations.

For the first year, Treasury assigned several individuals to implement the process in the Office of the Secretary and to oversee Treasury's departmentwide efforts. The Office of the Inspector General, in its report on the Office of the Secretary's first year FIA implementation, cited that the staff assigned was insufficient to perform both the Office of the Secretary implementation and departmental oversight. Our report also identified departmental staffing as insufficient. For the second year effort, Treasury assigned fewer staff than in 1983 and again assigned them to oversee the Office of the Secretary internal control efforts for the period April to August 1984. In August, the responsibility for the process was shifted to the Office of Financial Management in the Office of the Secretary.

The insufficient staffing at the department level has lessened Treasury's ability to provide the oversight necessary to assure that the bureaus' assessments are of good quality. The unreliability of the bureaus' vulnerability assessments discussed in the next chapter indicates that the bureaus can benefit from more effective departmental oversight.

Treasury officials have stated that the quality assurance program at the department level will be improved. They plan to assign several new professionals to the internal control staff, hold frequent meetings with bureau personnel, issue a simplified Internal Control Handbook, and conduct periodic seminars on internal controls.

Aspects of two bureau programs need to be improved

We also noted other improvements needed in bureau internal control processes.

- --Secret Service needs to include its field personnel and certain headquarters assessable units in the vulnerability assessment process and to resolve a potential conflict of audit independence.

--IRS needs to circulate its moderate and high vulnerability assessments to all regions so that the regions are made aware of the assessments' results.

Secret Service

Again in 1984, about 2,000 Secret Service employees located in 62 field offices did not participate in the vulnerability assessment process. Headquarters personnel made the assessments without field input. One of the act's purposes is to increase agency managers' awareness of the adequacy of their internal controls so such controls can be improved when warranted. Such increased managerial awareness and improved internal controls can be most effectively achieved by having field managers who daily carry out agency missions and programs meaningfully participate in the FIA process.

In addition, the Secret Service's inventory of assessable units did not include the Service's safety program, the Office of Inspection, and the Management and Organization Division. Consequently, vulnerability assessments were not done on these units as required.

Finally, the Service should resolve the conflict of audit independence resulting from the same official implementing and auditing the act. The Service's internal control officer, who is responsible for directing and coordinating the implementation of FIA, is also the head of the Service's Office of Inspection, which includes the investigative and internal audit functions. Over the last 2 years, this individual has audited the Service's implementation of FIA as part of a Treasury-wide Inspector General audit, while at the same time being responsible for implementing the act. The official's dual position represents a conflict of independence in carrying out the auditing role. An official from an office other than the Office of Inspection should be responsible for the FIA program, or auditors other than those from the Office of Inspection should be assigned to audit the Service's FIA implementation.

Internal Revenue Service

Each of IRS' 7 regions conducted about one-seventh of the 87 regional vulnerability assessments that were done. IRS then sent a listing of the assessment ratings (low, moderate, high) to each region. We believe IRS' regions would benefit by being able to review the basis for the vulnerability assessment ratings, including internal control weaknesses which may be applicable to their own units.

For example, our review of a vulnerability assessment done on the Information Returns Program at the Central Region's Service Center revealed that an identified weakness in internal control was not made known to the other regions. The

Information Returns Program is IRS' program for identifying taxpayers underreporting income and/or not filing tax returns. All taxpayer information (e.g., W-2 and 1099 interest and dividend forms) is compared to actual taxpayer income tax returns for discrepancies. The Central Region's vulnerability assessment identified a weakness in its internal controls. Branch personnel could exclude certain incoming tax documents, such as those of relatives or friends, to avoid verification that the income was reported in their tax returns. The other regions were not made aware of that information, although they follow the same policies and procedures as the Central Region.

We discussed our views on the desirability of distributing the sample assessments to all regions with the Service's FIA staff. They agreed to circulate the high and moderate vulnerability assessments to all regions.

CONCLUSIONS

Treasury made progress correcting internal control weaknesses identified during the first 2 years under the act. However, other identified weaknesses still need to be corrected. Further, departmental oversight and certain aspects of one bureau's efforts need to be improved.

AGENCY COMMENTS AND OUR EVALUATION

Of the four recommendations in this chapter, Treasury concurred with one, disagreed with two and did not comment on the fourth. We continue to believe the Secretary should implement all four recommendations.

Areas where Treasury concurs with GAO

Treasury agreed with our recommendation to improve departmental monitoring. Treasury said it has expanded its quality assurance program by (1) adding additional staff, (2) meeting quarterly with bureau internal control staffs, (3) developing a simplified set of guidelines, and (4) holding seminars. Treasury also noted that its automated information system has been updated and possible enhancements are being studied.

These actions appear to be responsive to our recommendation. However, we wish to emphasize that a primary purpose of our recommendation was to improve Department oversight by directing it more towards evaluating the results (quality) of bureau efforts rather than merely tracking the amount of activity that has occurred.

Areas where Treasury did not concur with GAO

The Department also stated that the Secret Service did not concur with two of our recommendations. These recommendations were to involve Secret Service's field offices in the vulnerability assessment process and to add three assessable units to its inventory of activities subject to the Financial Integrity Act. No comments were made on our third recommendation to the Service concerning the need to resolve a conflict of audit independence in evaluating their internal control process. For the following reasons, we believe all three recommendations to the Secretary should be implemented.

Field offices should make assessments

Secret Service contends that it is not necessary to have its field offices make vulnerability assessments. Essentially, the Service stated that all of its functions are highly centralized and this mandates the performance of all vulnerability assessments by headquarters personnel, all policies and procedures are developed in headquarters which controls and routinely monitors field office activities, and there is little possibility of undetected deviations from established policies and operational strategies by its field offices.

The Financial Integrity Act's ultimate objective is the establishment and maintenance of effective systems of internal control. The act and its accompanying evaluation process are intended to increase managers' awareness of the adequacy of internal controls over their operations and activities. Whether an organization is highly centralized or not, its delivery of services and performance of activities and functions are usually done in widely dispersed locations. It is in delivering these services and performing these activities and functions where internal control problems occur. We, therefore, believe that field managers who each day are involved in delivering services and carrying out the agency's activities and functions should participate in the FIA evaluation process.

This concept is incorporated in OMB's evaluation process. Circular No. A-123, revised, which prescribes policies and standards to be followed by the executive agencies in complying with the act, states that all levels of management should be involved in assuring the adequacy of internal controls. The Circular also states the performance agreements for Senior Executive Service and Merit Pay or equivalent employees with significant management responsibility should include fulfillment of assigned internal control responsibilities. Secret Service has 2,000 employees in its field locations, including merit pay or equivalent officials. Consequently, we disagree with Secret Service's position that field managers need not participate in the internal control evaluation process.

Other functions should be assessed

The Service also contended that it was not necessary to do assessments of its safety program, Office of Inspection, and Management and Organization Division as we recommend. The Service said it considered these activities when developing its inventory of assessable units and excluded them because they were policymaking functions which can be excluded in accordance with OMB guidelines.

Not all of the functions in these programs are policymaking. The Office of Inspection's duties include inspecting various Service offices (headquarters and field) at regular intervals to ensure procedures are being followed; the Management and Organization Division has management analysts who evaluate Service operations; and the Administrative Operations Division operates a safety program that involves making workplace surveys and checks for various hazards. These kinds of functions are subject to evaluation under the act and OMB guidelines.

RECOMMENDATIONS

We recommend that the Secretary of the Treasury:

--Improve departmental monitoring, including requiring departmental FIA staff to periodically visit the bureaus to review various phases of the process and to provide feedback to the bureaus on their FIA efforts.

--Require auditors other than those from Secret Service's Office of Inspection to be assigned to audit the Service's implementation of the act or assign the Service's FIA implementing responsibility to another Service office official.

--Require Secret Service to involve its field personnel in its vulnerability assessments.

--Require Secret Service to conduct vulnerability assessments on those units which were omitted from the process.

CHAPTER 3

UNRELIABLE VULNERABILITY ASSESSMENTS UNDERMINED TREASURY'S PROCESS IN 1984

Vulnerability assessments are the mechanism an agency uses to determine the relative potential for problems among its programs and functions. They must be done consistently throughout the agency because they rank the potential vulnerability of agency functions relative to each other. Although Treasury's managers closely followed OMB's guidelines, there were major inconsistencies in their assessments. Also, it appears that their assessments frequently did not consider major aspects of their unit's operations.

The assessments are a crucial part of OMB's internal control evaluation process. About 1,500 assessments were done in 1984, which comprised the bulk of Treasury's 1984 evaluation efforts. Because the assessments were unreliable, we believe Treasury and its bureaus did not have an adequate basis to conclude that their internal control systems provide reasonable assurance the FIA objectives were achieved.

Treasury's assessment problems largely stem from the nature of the OMB guidelines which provide a logical but, because they apply governmentwide, general assessment framework. Treasury needs to further develop the OMB evaluation concepts to reduce the present subjectivity of the vulnerability assessments. Such adjustments to the process are allowed and encouraged by OMB. In this regard, the Customs Service is working on an approach that appears to address many of the problems we identified.

VULNERABILITY ASSESSMENTS: A CRUCIAL PART OF THE PROCESS

The basic guidance on how federal agencies are to implement the governmentwide process to evaluate and improve their internal controls is contained in OMB's Internal Control Guidelines. The guidelines are the initial product of a pioneering effort to establish a governmentwide evaluation approach from a diversified body of literature on internal controls and evaluation methodology. Although such a methodology has long been used by the accounting profession, it has never before been applied on the broad scale called for by the Financial Integrity Act--covering, with few exceptions, all federal programs and operations.

The guidelines detail a phased approach which consists of (1) organizing the process by assigning responsibilities to proper persons; (2) segmenting the agency into smaller components (assessable units) that can be more readily evaluated; (3) assessing vulnerability of these units (high, moderate, or low) to develop a priority list of units where internal control weaknesses do or may exist; (4) correcting problems or conducting internal control reviews of units designated as highly or moderately vulnerable on the priority list; and (5) reporting yearly on the status of internal controls. Each phase in the approach is built upon and follows the completion of the previous phase. Thus, proper performance of initial phases is essential to the success of the entire process.

Vulnerability assessments form the foundation of OMB's internal control evaluation process. According to OMB's guidelines, the assessments are the mechanism which an agency uses to determine the relative potential for waste, loss, unauthorized use, or misappropriation among its programs and the basis for establishing priorities for corrective action, including the scheduling of internal control reviews which test suspected internal controls in operation. The assessments are important because (1) their purpose is to focus efforts to improve internal controls to where they are most needed; (2) they cover all agency programs and functions (except matters such as statutory development, rulemaking, and policymaking); and (3) they are the one point in the entire OMB process that involves the greatest number of agency managers, thereby achieving a primary purpose of the act--making managers more aware of the adequacy of internal controls over their operations.

Vulnerability assessments must be reliable to achieve the purposes set for them by OMB. Unreliable assessments will likely (1) result in an inaccurate and incomplete listing of the relative vulnerability of units, (2) cause resources to be misdirected on internal control reviews of units inaccurately designated as highly or moderately vulnerable, and (3) ultimately undermine the process by discouraging the cooperation of agency managers who perceive it as a meaningless exercise.

ASSESSMENT GUIDANCE IS GENERAL

OMB guidelines state that a vulnerability assessment consists of three steps: (1) an analysis of the general control environment, (2) an analysis of the inherent risk, and (3) a preliminary evaluation of safeguards. The guidelines also identify variables and forms which can be used in making and documenting the assessments. In all, there are 27 variables that can be considered and rated. (See app. II.)

Like the overall phased approach, we believe the topics considered in OMB's three assessment steps are sound. The steps address pertinent relationships of internal control systems. Specifically, controls exist to minimize risks inherent to an operation and they function in an environment that can increase or decrease the degree of the risks. However, guidance on how to perform vulnerability assessments is very general.

First, the guidelines do not have sufficient criteria or benchmarks to describe how the variables should be considered relative to an assessable unit. For example, the guidance for the variable "organizational structure" states:

> "The identification of organizational units to perform the necessary functions and the establishment of appropriate reporting relationships."

This guidance offers no criteria for a manager to judge the conditions that would indicate reporting relationships that are appropriate or inappropriate. For the variables "budget level" and "degree of centralization," the guidelines state respectively that operations involving large amounts of money are more susceptible to waste and loss than those involving small amounts and that different degrees of centralization are appropriate for different types of activities. Again, no criteria are presented relative to what constitutes a large or small amount of money or what types of activities would indicate that more or less centralization is desirable.

General guidance requires each manager to create his or her own criteria and leads to inconsistent and highly subjective ratings. These results can be seen in the ratings for the variable "purpose and characteristics" for Customs' assessments of its payroll function. Except for some organizational variances in the level of centralization, this function is consistent throughout Customs. OMB guidelines list several matters to consider for this variable of the inherent risk analysis. Customs made each of these matters a part of the assessment and had its managers answer either yes or no as to the relationship of each matter to the assessable unit. Table 3.1 shows the responses of its eight assessable unit managers.

Table 3.1:

Matters Considered at Customs
When Assessing "Purpose and Characteristics"

Matters for consideration	Number of manager responses[a] Yes	No
Broad/vague legislative authority or regulations	2	5
Cumbersome legislation or regulatory requirements	2	5
Broad or vague mission goals or objectives	0	6
High degree of complexity	7	1
Existence of third party beneficiaries	2	5
Activities involve payment of entitlement monies	3	3
Activities operate under severe time constraints	7	0
Activities involve handling cash receipts	0	6
Activities involve approval of applications, licenses, permits etc.	0	6

[a]Does not always total to eight because some of the regions did not address all the matters.

Table 3.1 shows that without sufficient criteria the same conditions get interpreted differently. For example, the same legislation was perceived by two managers as broad or vague and by five managers as not. The differences in addressing these matters led to two managers rating the variable as highly vulnerable, four managers as moderately vulnerable, and two as lowly vulnerable.

This kind of result is not unique to the purposes and characteristics variable. Twenty-one of the 27 variables lack sufficient benchmarks to produce consistent evaluations. Two other examples for the functions "air passenger examination" and "overtime" are shown in table 3.2. These functions involve the clearing of passengers entering the United States and the authorization and use of employee overtime.

Table 3.2:

Further Examples Showing How
Similar Conditions Were Rated Differently

Assessable unit	Factor	Region ratings A	Region ratings B	Rating explanations: Region A	Rating explanations: Region B	GAO observations
Air passenger examination	Impact outside Customs	High	Low	The rating states significant, wideranging effect upon others	The rating states little impact on public or other agencies	Narratives and ratings are opposite; operations are similar
Overtime	Competent personnel	Moderate	Low	The rating states that staff are fully trained and qualified with a reasonable rate of turnover	The rating states that staff are well qualified and properly trained	Narratives are very similar; but ratings are different

Similarly, the guidelines do not adequately describe to managers how to make a preliminary evaluation of safeguards--the third assessment step. There are no criteria to assist managers in applying GAO's internal control standards to their assessable units. The guidelines devote two paragraphs to this step. The first paragraph essentially states that the purpose of the evaluation is to consider whether controls are in place to prevent loss, waste, or misuse of resources. The second paragraph states that an in-depth review of controls is not appropriate at this stage and that the evaluation should be based on the manager's working knowledge and judgment of the existence and functioning of safeguards.

In addition to these 2 paragraphs, a standard checklist form, listing 11 of GAO's internal control standards by name, is provided. The form requires a judgment (yes/no) about whether the standards are met and explanatory comments for the judgment. The form, however, contains a footnote which governs four of these standards. The footnote states that sufficient analysis will probably not have been done to judge compliance with these particular standards (control objectives, control techniques, recording transactions, executing transactions). Thus, they did not have to be considered.

Treasury's 1984 guidance required that vulnerability assessments be done in accordance with its own handbook and the OMB guidelines. Although Treasury's handbook was issued in draft, it was made available to the bureaus and it closely paralleled OMB guidelines. The handbook detailed the same 27 variables and the same forms OMB suggests be used. The nine bureaus making vulnerability assessments in 1984 closely complied with the OMB-Treasury guidance.

TREASURY'S 1984 VULNERABILITY ASSESSMENTS ARE NOT RELIABLE

In 1984, Treasury and its bureaus reported that on the basis of an evaluation conducted in accordance with OMB's guidelines, its systems of internal control, taken as a whole, provide reasonable assurance that the act's objectives were achieved. According to OMB, reasonable assurance is based on several factors, including (1) results of vulnerability assessments and internal control reviews, (2) assurances by agency officials, and (3) other available information such as Inspector General and GAO reports. Treasury's guidance specified that managers consider previously reported Inspector General and GAO findings during their vulnerability assessments. In 1984, Treasury completed about 1,500 vulnerability assessments and 42 internal control reviews. Thus, vulnerability assessments comprised the bulk of Treasury's efforts and were a significant, if not the primary, basis for the bureaus' and Treasury's reasonable assurance statements.

Our review of Treasury's assessments disclosed a number of shortcomings. Our analysis of 818 assessments made by 4 bureaus showed a pattern of widespread inconsistencies in the ratings. Further, supplemental field audit of 22 assessments revealed that managers frequently (1) did not consider the vulnerability of major aspects of their assessable units and (2) were confused by the assessment methodology. Taken together, these shortcomings seriously undermine the reliability of the assessments.

Significant inconsistencies in vulnerability ratings of common groups

Vulnerability assessments must be done consistently, because the assessments' purpose is to rank assessable units relative to one another. This purpose requires that all assessable units be judged against the same evaluation criteria. Indeed, OMB's guidelines recognize this principle by stating that care should be taken to ensure the ratings are done consistently.

For vulnerability assessments to be done consistently, some basic conditions need to be met. First, agency managers need to evaluate their assessable units against the same variables. As noted earlier, Treasury had its bureaus all follow OMB guidelines and, thus, met this condition. Another vital condition is that the evaluation criteria should be sufficient to govern the application of the variables to the assessable units so that reasonably consistent results are obtained when like situations are assessed by different managers. This latter condition was not met.

We reviewed four bureaus (IRS, Customs, OCC, and U.S. Mint) that made multiple assessments for the same function. For example, "air passenger examination," the processing of persons traveling into the United States by air, is a Customs Service function. Customs' seven regions and its headquarters have responsibilities associated with this function. Thus, eight different managers made vulnerability assessments for this function. As shown in table 3.3, we analyzed a total of 704 vulnerability assessments for 134 groups of common functions.

Table 3.3:

Scope of Vulnerability Assessment Analysis

Bureau	Common groups	Assessments GAO analyzed
Customs	49	393
U.S. Mint	13	60
OCC	12	73
IRS	60	178
Total	134	704

Our analysis identified the consistency of the ratings for some variables which we believed should be rated reasonably consistent by a group of managers who assessed the same function. For example, bureau officials told us that policies and procedures for a given function are the same throughout the organization. Thus, if the assessments were reliable, managers of the same function should be reasonably consistent in rating the variable "policies and procedures."

Our analysis, however, showed that when managers of common groups assessed like conditions, they often did not arrive at reasonably consistent ratings (i.e., at least one manager of the function rated the variable high while at least one other rated it low or not applicable).

At Customs, for example, at least 1 manager of a function rated the variable "impact outside agency" as highly vulnerable, and at least 1 other manager of the same function rated it as lowly vulnerable in about 65 percent of the 49 common groups. Taking one specific instance for the assessable unit air passenger examination, five managers concluded that "impact outside agency" should be rated high, one rated it moderate, and two rated it low. The significance of the difference is that it is not justifiable. Air passengers being cleared when entering the United States are affected about the same at every airport. They all file declarations on merchandise being brought into the country, answer inspector questions, are subject to having their baggage searched, and face the possibility of arrest or having their property seized if the law is violated.

As shown in table 3.4, rating swings of high to low in the same variable by managers of the same function occurred frequently among the 134 common functions analyzed. They ranged from a high of 49 percent for the purpose and characteristics variable to a low of 20 percent for the organizational checks and balances variable. The frequency at which managers of the same function reached opposite conclusions (i.e., high versus low vulnerability) in rating these variables shows that the assessments were not done reasonably consistently throughout the bureaus. Thus, they do not reliably rank functions by their vulnerability.

Table 3.4:

Percent of Major Inconsistencies in Variable Ratings Among Common Groups of Assessments

Variables rated	Treasury bureaus: Customs (49 groups)	U.S. Mint (13 groups)	OCC (12 groups)	IRS (60 groups)	Variable average (134 groups)
	(percent)				
Organizational structure	45	46	0	a	30
Policies and procedures	37	46	17	a	33
Budgeting and reporting practices	39	31	33	a	34
Organizational checks and balances	22	38	0	a	20
ADP consideration	31	0	42	a	24
Purpose and characteristics	80	54	33	30	49
Impact outside agency	65	23	25	22	34
Age and life expectancy of function	29	31	25	17	25
Degree of centralization	49	8	8	42	27

[a]IRS did not characterize their ratings for these variables as high, moderate, or low like the other three bureaus.

Inconsistencies in determining overall vulnerability ratings

There were also inconsistencies in the way managers determined overall ratings of assessable units from the results of the three assessment steps. Neither OMB's nor Treasury's guidance describes how the overall vulnerability rating is to be determined. For example, there is no discussion regarding whether each of the three steps is of equal weight or whether any particular step is more important and should be given greater weight.

As would be expected, identical combinations of ratings for the three assessment steps led to inconsistent conclusions about an assessable unit's overall vulnerability rating. Taking one specific instance, the 3-step rating combination of low, high, low occurred in 69 assessable units and resulted in 45 managers concluding the overall vulnerability was low, 23 that it was moderate, and 1 that it was high.

Overall, about 14 percent of the ratings were inconsistent. (See app. III.) Our analysis, however, is conservative and somewhat understates the problem. We believe a better measure would be to eliminate the results for the two extremes found in the analysis (i.e., where the three-step ratings are all low and where they are all high). In our opinion, these two conditions almost mandate that a manager reach the same conclusion (low or high) for the overall vulnerability rating. With the two extremes thrown out, the rate of inconsistency increases to 24 percent.

The inconsistencies in determining the overall ratings occurred because the guidelines do not describe how to factor the results of the three assessment steps together to arrive at an overall vulnerability rating. The guidelines simply state that the three steps permit a manager to assess the (1) adherence of the program or function to at least some of the prescribed standards and (2) its vulnerability.

The limited guidance created confusion about determining the overall assessment rating. For example, if a manager rates a function's inherent risks as highly vulnerable, but the safeguards as being good, should the overall vulnerability rating be (1) high vulnerability, because of the risks inherent in the program or (2) low vulnerability, because the safeguards are believed to be good? The guidelines do not specifically answer this question and caused the inconsistencies in Treasury's overall assessment ratings.

Major unit operations
were not considered

Our field audit of 22 Customs assessments revealed that in 11 assessments the managers did not consider major aspects of the units' operation (see app. IV). The omissions occurred because the assessable unit descriptions were not sufficiently detailed to assure that the managers would be aware of all important operations which needed to be assessed. Like Customs, seven of the eight other bureaus making assessments in 1984 identified their assessable units by name only. Thus, it is likely that other Treasury managers also may have omitted major operations from their assessments. Indeed, our limited field review of two IRS assessments identified the same problem.

Without a clear understanding of the operations included in an assessable unit, managers (1) could assume a particular operation, common to several assessable units, was covered elsewhere; (2) might not think of an operation while doing the assessment; or (3) may not be in a position to evaluate all aspects of the unit.

Customs' assessment of its "seized, forfeited, and abandoned property" unit demonstrates the type of oversights that occurred. Customs district and port offices obtain various types of property in the course of their duties. For example, Customs officers can seize contraband and other goods which are not properly declared upon arrival into the country or are in violation of law. Ultimately, such property can be either returned after proper payment of duties, penalties, and reimburseable costs; or, it can be forfeited to the government through administrative process or by court order. After forfeiture, such property can be sold, destroyed, or used by the government.

From an internal control perspective, this assessable unit has several inherent risks. For example, the property (which can include cash, vehicles, narcotics, etc.) could be lost or misappropriated without chance of detection, or the value of property which is not maintained or properly managed can deteriorate or diminish.

The assessments did not consider the potential vulnerability of controls in place to handle these major operating risks. The managers did not consider how the various districts and ports maintained inventory control, separated the duties of physical custody from recordkeeping, physically secured the property, accounted for costs associated with the seized property, and managed the cash and other valuable property that is seized. Rather, the assessments primarily involved a consideration of the controls in place to assure that (1) certain types of forfeited property[3] were allocated to best meet various government resource needs and (2) commercial storage space for seized property was properly procured--a small part of seized property operations.

When major operations within an assessable unit are overlooked, potential problems can be missed. We identified indications of potential internal control problems during our review.

For example:

--In one district office, revenue collections averaging about $2 million each day were not always deposited on the day of receipt (a fundamental internal control practice). Backlogs in entry processing caused some collections to remain at cashier units for several days

---

[3]For example, vehicles valued over $25,000.

before they could be deposited. Even when there was no backlog, we were told that daily collections were not deposited until the following day. This increases risks associated with controlling cash. Also, untimely deposits increase government costs (in lost interest revenue and/or increased public debt interest expense).

--Another common set of internal control weaknesses that were not always identified concerned inadequate separation of duties in the payroll assessable unit. We identified several types of weaknesses, including persons entering their own time and attendance data into the payroll system and different payroll clerks using the same computer access code.

Like Customs, all but one Treasury bureau did not describe the operations within assessable units. Thus, assessable unit managers at these bureaus faced the same conditions as their counterparts at Customs. Indeed, one of the two IRS assessments that we examined in some detail did not consider 80 percent of the unit's operations.

We reviewed the assessments for IRS' Information Returns Program. The program acts as an accuracy check by comparing taxpayer reported income against independently submitted income information documents supplied to IRS by banks, brokers, etc. Information returns documents are either received as paper documents or on magnetic media tape (computerized). Currently, about 80 percent of the information returns documents are received on magnetic media tape and 20 percent are processed as paper documents. There was no assessment of the magnetic media tape portion of this process in the Central Region. Service Center officials stated they considered only the paper documents in performing the assessment.

Beyond overlooking the handling of 80 percent of the program's information, the coverage for the part assessed was inadequate. The paper documents operation has six major functions through which tax information is processed to establish a data base that will identify taxpayers who are potentially underreporting income. The Service Center assessment did not consider the potential vulnerability of the last function in the process--sending the taxpayer a letter of inquiry regarding tax discrepancies.

Confusion throughout the assessment process

Our field work also disclosed that most managers who made the assessments voiced confusion with the process. Of the 15 managers who made the 22 assessments we reviewed,[4] 3 said the

[4]Some managers made several assessments.

guidelines were adequate; 3 did not specifically comment on the guidelines; and 9 said they were confused by the terminology, categories, and/or complexity of the guidelines. Listed below are some of the managers' comments to illustrate the confusion encountered in making the vulnerability assessments.

Region A

One manager told us that he thought the approach was a paper exercise. He felt the process was too arbitrary and subjective and did not even help to identify vulnerability. Another manager stated he basically wrote down bureaucratic jargon that he knew upper management would accept. He said the generalities of his comments made the assessment useless. He did not think the vulnerability assessment process had any value at all.

Region B

One manager thought the guidelines for making the vulnerability assessments were general in nature. He said he had difficulty understanding the terminology. Another manager in the region also said that he could not understand the guidance.

The confusion expressed by the managers is evidenced in the assessments. The assessments are characterized by general and conflicting or nonresponsive comments. For example, one of the seized property assessments stated that there were no internal controls. However, in other parts of the assessment, it stated that (1) substantial documentation existed to track the handling of seized property, (2) authorizations of transactions involving seized property were clearly defined in policies, (3) there was a clear and precise sequence of reviews of transactions, and (4) effective checks and balances were built into the program. These latter comments all represent internal controls.

A PROMISING APPROACH FOR DEVELOPING OMB EVALUATION CONCEPTS

Despite the problems with the assessments, Treasury's decision to closely follow OMB guidelines was reasonable. OMB's guidelines were developed pursuant to the Financial Integrity Act and were the initial federal guidance on how to implement the act. Further, the basic criticism of Treasury's initial efforts in 1982 and 1983 by OMB, GAO, and the Inspector General was its failure to follow OMB guidelines. As with many new and wide-ranging initiatives, it is not surprising that startup problems exist and need to be corrected.

Basically, adjustments need to be made to further develop the OMB evaluation concepts. OMB advised agencies in August 1984 that adjustments to its process are allowed and encouraged. OMB stated that its guidelines are intended to assist agencies in developing their process. However, agencies can combine, revise, or otherwise alter the specific steps to develop their evaluation process as long as the objectives of the phases are maintained.

Customs Service's experience has spurred the development of an approach that offers considerable promise to address many of the problems encountered in 1984. Customs' FIA staff recognized that its managers were having problems following the OMB assessment guidelines. The staff reviewed the assessments and found that there were inconsistencies in the ratings and in what was evaluated. They identified a number of specific problems that are closely related to those we previously discussed. For example:

--The assessable units were not well defined.

--The terminology and prescribed procedures were confusing to its managers. Managers did not understand what they were evaluating.

--The term vulnerability was imprecise and highly charged because it implied that managers were being negligent in their duties.

--The evaluation process did not address operating risks adequately nor consider the aspect of compliance with existing controls.

--Many managers who lacked technical skills could not adequately assess automated data processing controls.

As a result, the staff concluded that the assessment results were of questionable value. Customs' officials recognized these concerns and properly qualified the overall results of its efforts in its 1984 assurance letter to the Secretary. Customs' FIA staff began early to address these problems with the assessments. By mid-1984, Customs began to develop a fundamental plan to make the process more understandable and meaningful to its managers.

The plan involves identifying four elements for each assessable unit: (1) the event cycles (major operations or processes), (2) the specific inherent risks in each event cycle, (3) the control objectives for handling each risk, and (4) the basic control techniques used to achieve the control objectives. Each assessable unit's elements would then be circulated among appropriate headquarters and field managers for review and comment. (See app. V for an example.) We believe this proposed approach can address the problems that caused Treasury's vulnerability assessments to be unreliable.

First, it addresses the relationship of all the fundamental factors that comprise the concept of internal controls. Specifically, to develop a methodology for assessing the potential vulnerability of a unit's operations, it is necessary to understand the basic factors involved with internal controls and their relationship to each other. There are three basic and interrelated factors: inherent risks, internal control objectives, and internal control techniques.

Internal controls exist to manage operating risks. Thus, any assessment of vulnerability hinges on a clear understanding of the particular risks each assessable unit faces. Because risks are inherent to an activity, they usually cannot be fully eliminated. Rather, management must establish goals (control objectives) to define how the risks are to be managed. Control techniques are then developed to achieve the control objectives and mitigate the inherent risks.

Customs' proposed approach addresses these basic factors and relationships. When making a vulnerability assessment, an assessable unit manager needs to answer the following types of questions.[5]

--Do I believe all of the inherent risks have been identified?

--Do I believe that the control objectives established for managing these risks are reasonable and adequate?

--Do I believe that the basic control techniques have been identified, are followed, and accomplish the control objectives?

Customs' approach--once the assessable unit's risks and control objectives and techniques have been identified--simplifies the method for making the assessments and complies with OMB guidelines. It focuses the manager's attention on the fundamental internal control concepts. It requires consideration of the above questions in relation to the major activities of the assessable unit, rather than 27 general variables. It also addresses the basic intent of OMB guidance for doing the assessments. An assessable unit manager must consider inherent risks, the specific control techniques, and the environment where they operate. We believe Customs' approach is consistent with the phased approach described in OMB guidelines.

---

[5]These questions are answered on the basis of the manager's knowledge and experience with the assessable unit. They cannot be "answered" in the absolute sense of the word, unless the unit's internal controls are actually tested in operation, and such testing is not part of a vulnerability assessment.

Customs' approach also lends itself to addressing several other issues that have arisen with regard to implementing this process. First, the adequacy of documentation of an assessment has been a common problem reported at Treasury. This matter was discussed in six of the nine Inspector General reports on bureaus making assessments in 1984. It is very difficult for a supervisor or reviewer to examine the present assessments and determine the basis for the ratings, because the comments focus on the variables and these are not assessable unit-specific. If documented as planned, the manager's views under Customs' approach should be focused on how well the unit's specific risks are handled. A manager's rationale for the judgments made should become much more apparent.

Second, Customs' approach would more specifically define the assessable units. This should reduce the problems of major operations not being considered. It also should aid in deciding which layers of the organization's managers need to be involved with the assessments.

Third, much of the confusing terminology associated with the process is eliminated. Internal controls are described in simpler terms of risks, objectives, and techniques. This addresses Customs' concern about the highly charged nature of the term "vulnerable."

We believe the Customs' approach complies with OMB requirements and commend the Customs Service's FIA staff for demonstrating a high degree of creativity, initiative, and commitment to developing the plan.

CONCLUSIONS

The vulnerability assessments made in 1984 comprised the bulk of Treasury's evaluation efforts and were a significant, if not primary, basis for the bureaus' and Treasury's reasonable assurance statements. However, the inconsistencies, omissions, and confusion which characterize the vulnerability assessments make them unreliable. As a result, we believe Treasury and its bureaus did not have an adequate basis to conclude that their internal control systems provide reasonable assurance the objectives of the Financial Integrity Act were achieved.

Treasury's assessment problems largely stem from the nature of OMB guidelines, which provide a logical but, because they apply governmentwide, general assessment framework. Treasury needs to further develop the OMB evaluation concepts to reduce the degree of subjectivity present in its assessments. Such adjustments to the process are allowed and encouraged by OMB. In this regard, the Customs Service is developing an approach which we believe offers promise in addressing the problems discussed in this report. Customs' approach should be tested to determine whether it improves the reliability of these crucial assessments and can be used by other Treasury bureaus.

RECOMMENDATIONS

We recommend that the Secretary of the Treasury:

--monitor Customs Service's implementation of its alternative vulnerability assessment approach and, once its feasibility is proven, test the approach on a sample basis at several bureaus to determine whether it should be adopted departmentwide; and

--require bureaus conducting vulnerability assessments in fiscal 1986 to detail how they plan to assure that their assessments are reliable and to evaluate the adequacy of such plans relative to the problems discussed in this report.

AGENCY COMMENTS AND OUR EVALUATION

Overall, Treasury agreed with our analyses of its vulnerability assessments. Further, Treasury concurred with our recommendations, but indicated several matters are hindering their full adoption. Treasury did, however, express concern about our conclusion that its unreliable assessments did not provide an adequate basis to conclude it had reasonable assurance. Our evaluation of Treasury's specific comments follows.

Treasury concurs with our analyses and recommendations

Treasury stated that our technical analyses of its vulnerability assessments reinforced some of its own conclusions. Treasury stated that the report provides insights and information that will be of great value to its future internal control initiatives.

Treasury also stated that it concurred with both of our recommendations for improving its vulnerability assessments. Treasury noted, however, that Customs is still developing its approach. Thus, Treasury said it will monitor Customs' progress with its new process, but will refrain from testing it in other bureaus until its feasibility is proven. Given that Customs is still developing its approach, we believe Treasury's response is reasonable and have modified our original proposal.

Treasury also concurred with our recommendation to require its bureaus conducting assessments in fiscal year 1986 to detail how they plan to assure how their assessments are reliable and to evaluate these plans relative to the findings in this report. Treasury indicated, however, that its agreement was conditioned on being able to establish a reasonable standard for reliability. Treasury also said that caution must be exerted to ensure the assessments do not become more complicated and paper intensive.

We agree that vulnerability assessments should not be made more complicated or paper intensive. Indeed, our report favorably discusses Customs' efforts to simplify the process. However, we are concerned that Treasury's future assessments will again be an unreliable paper exercise if it continues to use the 1984 assessment approach (as its comments indicate it is going to do).

Regarding Treasury's conditional agreement being based on establishment of a reasonable standard for reliability, we believe our report provides a starting point for developing such a standard. Our report describes several problems with Treasury's assessment process. These were

--the lack of sufficient benchmarks or criteria in Treasury's guidance to aid managers (1) in rating the numerous evaluation variables and (2) in determining how to arrive at an overall vulnerability rating from these variable ratings,

--the failure to define assessable units to ensure adequate coverage of all important activities within the unit, and

--the confusing terminology and guidance.

Because Treasury plans to use the same assessment approach in the future, we believe it imperative that Treasury address these problems in order to increase the reliability of its assessments.

Treasury's concern about our conclusion on reasonable assurance

Although Treasury did not disagree with our conclusion that its vulnerability assessments were unreliable, it expressed concern over our opinion that it lacked an adequate basis to conclude it had reasonable assurance. Treasury said its vulnerability assessments were not the sole basis for its assurance statements to the President and the Congress. Treasury said that its bureaus are requested to review the results of its vulnerability assessments, internal control reviews, audit reports, reviews of internal control under section 4 of the act, management reviews, contractor studies and other source material in preparing reports and assurance letters.

Treasury also said its review process adheres to OMB instructions. Treasury noted that OMB has not established minimum evaluation criteria for agencies to meet before making a reasonable assurance statement. Finally, Treasury noted that OMB guidance states that the sum and substance of all information available to management is to be considered in making a reasonable determination.

In response to Treasury's comments, we emphasize that our report does not state that vulnerability assessments were the sole basis for Treasury's reasonable assurance statement. Rather, on pages 17 and 22, we stated that the assessments comprised the bulk of Treasury's evaluation efforts. Specifically, Treasury bureaus completed about 1,500 vulnerability assessments and 42 internal control reviews during the reporting period. Also, the report states on pages 17 and 18 that the assessments are a crucial part of the OMB process which Treasury followed and are the one point in the process where systematic, departmentwide evaluations are done.

Regarding Treasury's comment that its bureaus were required to review other factors (audit reports, management reviews, contractor studies etc.) in making their reasonable assurance statement, these factors were considered as a part of the vulnerability assessments.

--Treasury's Internal Control Handbook required bureaus to evaluate the variable "prior audits and reviews." The handbook defined this variable as prior audit reports by the Inspector General, bureau audit staffs, GAO and others; internal management reviews and evaluations; congressional reports; and consulting reports. Thus, managers considering the variable "prior audits and reviews" included them in the vulnerability assessments--assessments that our analyses showed to be unreliable. Other than at this point in the process, no evidence of a systematic attempt to consider the types of reviews and studies referred to by Treasury exists.

--Treasury's bureau assurance letters do not clearly state the basis for their reasonable assurance statements. Their statements are made on the basis of their internal control evaluations (used in a broad, generic sense). The description of their internal control evaluation efforts are primarily related to the vulnerability assessments. References made to other reviews or reports tend to be limited and vague. For example, in terms of its 13 bureaus, 10 made no reference to GAO reports, 4 made no reference to Inspector General reports, 9 made no reference to contractor reviews, and 7 made no reference to management reviews. Overall, general references were made to 3 GAO reports, 30 Inspector General reports, 4 contractor reviews and 12 management reviews.

Further, Treasury's instructions to its bureau heads for preparing their annual assurance statements also indicated the assessments were important. Treasury's memorandum to its bureau heads emphasized two specific matters that were particularly important: corrective actions taken by the bureaus on previously reported weaknesses, and the review or verification of each bureau's segmentation and schedule for conducting the second cycle of vulnerability assessments.

In summary, we recognize that management judgment is involved in reaching a conclusion that the internal control systems, taken as a whole, provide reasonable assurance that the act's requirements have been met. In deciding whether their systems provide reasonable assurance, we believe agencies need to consider four factors collectively:

--the comprehensiveness and quality of the evaluation work performed,

--the significance of the weaknesses disclosed,

--the status of corrective actions, and

--the extent to which accounting systems conform to the Comptroller General's requirements.

In our opinion, unless the agency's key accounting systems and internal controls over major programs and functions are adequately evaluated and tested, the agency head does not have an adequate basis to conclude whether the systems, taken as a whole, provide reasonable assurance. Evaluations and corrective actions needed to address the act's requirements may take several years to complete. An agency may be making good progress toward that goal, yet not have progressed to the point where reasonable assurance can be provided.

In Treasury's case, we found that the vulnerability assessments were not reliable, its accounting systems were not sufficiently tested, and its ADP systems were not sufficiently evaluated. Under these circumstances, we cannot agree that Treasury had an adequate basis at the time of its 1984 annual statement to conclude that its internal control systems, taken as a whole, fully comply with the act's requirements.

We recognize that Treasury reached its judgment in accordance with guidelines disseminated by OMB. In our report on first-year implementation of FIA (GAO/OCG-84-3), we recommended that OMB clarify and revise its guidance on what should be contained in the year-end reporting statement. The House Committee on Government Operations, in its August 2, 1984, report on first-year implementation of the act, also recommended that OMB revise its guidance concerning annual reporting. The Committee suggested that it would be more practical for some agencies to report they "have reasonable assurance except..." and identify areas where they do not have assurance. However, OMB took no action on these recommendations. This issue will be discussed further in our overall report on second-year implementation of the act which is to be issued later this year.

CHAPTER 4

IMPROVEMENTS NEEDED TO EVALUATE ADP AND CORRECT ADP SECURITY PROBLEMS

Better guidance and coordination are needed for Treasury to improve its evaluation of ADP controls. In 1984, neither of Treasury's evaluation methods (vulnerability assessments required by the Financial Integrity Act and risk analyses required by OMB's circular on ADP security) adequately evaluated ADP. Both overlooked pertinent systems, facilities, and controls. If Treasury is to achieve its goal of using the Risk Management Program to meet the requirements of the Financial Integrity Act, certain systemic inconsistencies between the two need to be addressed.

Treasury should also provide fuller disclosure about the status of its corrective actions. In 1984, Treasury reported no material weaknesses. Yet, we noted that problems still exist relative to last year's reported material weaknesses on information systems security and that the proposed corrective action--the Risk Management Program--is not yet fully implemented.

ADP CONTROLS WERE NOT ADEQUATELY ASSESSED

Treasury is highly dependent upon ADP to carry out its mission and administrative functions. Many bureau missions or functions would be impossible to perform without the aid of computers, and others could only be performed in a highly degraded mode. For example, without computers, IRS would find it impossible to process the millions of tax returns filed each year and to effectively use the information contained in these returns. IRS' Information Returns Processing system alone is expected to process well over a billion documents by 1986.

Because of ADP's importance, Treasury needs to thoroughly evaluate ADP internal controls. The quality of ADP controls affects Treasury's ability to give reasonable assurance that its systems of internal controls are effective and operating as intended. ADP controls are generally composed of two types:

--<u>ADP general controls</u> govern overall functions, such as organization and management, application system development, and computer operations, and affect the quality of services rendered to ADP users. The scope of general controls is quite broad, affecting most ADP hardware and application software systems.

--<u>ADP application controls</u> are part of individual software application systems and control the quality of data origination, input, processing, and output. Application controls are narrower in scope than general controls, because such controls are tailored to meet the specific control objectives established for each software system.

In 1984, Treasury primarily evaluated the status of its ADP controls in two ways--vulnerability assessments and risk analyses. In our opinion, neither way adequately evaluated Treasury's ADP controls.

Vulnerability assessments did not cover pertinent controls or facilities

Treasury provided limited guidance on how managers should evaluate their ADP internal controls when performing vulnerability assessments. The guidance consisted of the brief OMB definition of the general control environment variable "ADP considerations" and two suggested items to consider: (1) were ADP reports/products timely and (2) did the ADP system comply with the requirements of OMB Circular A-71. This OMB circular required agencies to develop management controls to safeguard personal, proprietary, and other sensitive data in automated systems. It required agencies to implement a computer security program and defined a minimum set of controls to be incorporated into these computer security programs. Treasury's guidance did not describe ADP internal controls nor explain who is responsible for assessing them. As a result, the assessments were adversely affected in several ways.

As shown in the previous chapter, there were major inconsistencies in how managers of the same function rated this variable. For example, at Customs, opposite ratings occurred for the variable "ADP consideration" in 31 percent of the groups of managers rating the same function. Taking one specific example, of the eight managers rating this variable for the function "revenue collections," four managers rated it high vulnerability while four other managers rated it low vulnerability. Given that the same ADP system(s) were rated, it is difficult to determine what such opposite ratings signify. (See p. 24.)

Further, managers did not adequately assess ADP controls in some vulnerability assessments of operations that rely heavily on ADP support. In at least three of the four Customs Service regions included in our review, ADP application controls were not adequately evaluated in assessing Treasury's Payroll/ Personnel Information System. For example, in one region, assessors stated that they gave little, if any, consideration to ADP controls; and, in another region, the assessor did not evaluate controls at the districts and ports where time and attendance data is entered into the system.

The Risk Management Program needs to be developed to achieve its dual objectives

Treasury developed the Risk Management Program in 1983 with the intention of satisfying the requirements of both the Financial Integrity Act and OMB Circular A-71, Transmittal Memorandum No. 1, on the security of Federal automated information systems. The program requires each bureau to (1) inventory all covered[6] information systems and facilities, (2) perform a risk analysis and certification of covered systems once every 3 years, (3) develop a yearly schedule to accomplish the risk analyses and certifications, and (4) appoint a computer security official for each information system facility.

Each bureau inventoried its systems and facilities in 1984 and most had named security officers for their information system facilities. However, risk analyses completed in 1984 covered only 2 of more than 80 ADP systems and facilities identified in approved[7] risk management plans. In addition, three bureaus--Customs Service, Bureau of the Public Debt, and Office of the Secretary (including Office of Revenue Sharing)--did not have approved risk management plans. The chart in appendix VI illustrates the extent of bureaus' implementation during 1984.

We believe the Risk Management Program is a positive step towards evaluating Treasury's ADP controls. However, several significant problems need to be resolved to achieve Treasury's objective of having the program satisfy the requirements of both the Financial Integrity Act and OMB Circular A-71.

First, the Risk Management Program covers only "certain" ADP systems. In contrast, the Financial Integrity Act and its implementing guidance require that all ADP systems be evaluated. In addition, different Treasury organizational units direct the Risk Management Program and the internal control evaluation process. The two efforts should be coordinated to assure that the objectives and requirements of each are achieved and to prevent potential duplication of effort in examining ADP operations. However, activities under the two efforts were not

---

[6]The program applies to certain automated decisionmaking systems, sensitive systems, and major systems critical to fulfilling the organization's mission and to data processing installations with a capital asset value over $1 million or that process any of the above three types of information systems.

[7]While the risk management directive does not require risk management plans to be formally approved, the Department had an informal approval process in 1984 to assure that bureaus were implementing the directive as intended.

adequately coordinated in time to benefit Treasury's 1984 FIA work. Treasury did not provide guidance on how the Risk Management Program should be used to satisfy the requirements of the FIA assessment process.

For example, some ADP activities that were not assessed under the program were also not evaluated under the act during 1984. Customs Service did not conduct risk analyses or vulnerability assessments of its two data centers or regional data facilities in 1984. Also, eight ADP systems and facilities listed in the Office of the Comptroller of the Currency risk management inventory were not included in a risk analysis and were not assessed under the act during the year. For example, the Regional Bank Information System, which supports ongoing monitoring, analysis, and supervision of 140 large regional banks, was not included.

We also noticed that the two evaluation methods caused confusion in some components and a potential for duplication of effort. For example, a Bureau of Engraving and Printing official believed the FIA process required a vulnerability assessment and the Risk Management Program required a risk analysis. To satisfy both requirements, Engraving and Printing hired a contractor to provide two separate documents under a single contract. The two documents contained identical weaknesses, all but one of which were in the ADP general control categories. The only significant difference between the reports was that the vulnerability assessment report also included the standardized Treasury forms and the risk analysis report associated dollar values with the weaknesses.

A second problem concerns the timing of these ADP evaluations. Systems covered by the Risk Management Program are evaluated on a 3-year cycle. In contrast, vulnerability assessments are to be made on a 2-year cycle. This timing difference together with the lack of coordination and guidance, creates the possibility of coverage gaps and duplication like the examples just discussed.

Third, even though all controls are to be assessed under the act, neither evaluation method adequately describes the ADP controls to be considered. This creates the potential for assessors to overlook controls during vulnerability assessments and risk analyses. For example, Risk Management Program guidance identifies a number of ADP internal controls which assessors should consider to determine the level of risk present in ADP systems or operations. These include (1) access controls, which restrict access to computer rooms, equipment, and critical documents and (2) systems software maintenance controls, which ensure that system software changes are properly documented, tested, and approved before being implemented. However, the following were among several important ADP internal controls not adequately addressed.

Table 4.1:

Important ADP Controls Not Covered in Risk Management Program Guidance

Control	Objective of control
System acceptance	To assure that the ADP system was properly designed, developed, and tested before implementation.
Separation of duties	To assure that key duties and responsibilities are performed by different individuals to reduce the risk of errors, waste, or wrongful acts.
Source document origination	To assure that documents are prepared properly and only by authorized personnel.
Data input validation and editing	To assure that erroneous data is detected before processing.
Data processing validation and editing	To assure that erroneous data is detected during processing and reported for investigation.

In addition, most of the discussion of ADP internal controls appears in parts of the guidance provided for illustration and which assessors are not required to use.

Treasury officials have recognized the need to cover additional ADP systems and ADP internal controls and for greater coordination between the Risk Management and Financial Integrity Act programs. They agreed to modify the Risk Management Program to assure adequate coverage of ADP systems and operations and ADP internal controls. Treasury officials also stated that they would amend their Internal Control Handbook to include information on the Risk Management Program and how it fits into the internal control process. They also agreed to amend the Risk Management Handbook to clarify the relationship between the two programs.

Finally, in October 1984, Treasury established a four member working group to address the problem of overlap and possible duplication between the internal control evaluations and accounting system reviews required by the Financial Integrity Act and information system risk analyses required by OMB Circular A-71. According to two members of the working group, as of July 1985, the group had held only one meeting. A third member of the group stated that the group had also met informally "about half a dozen times." The three officials stated that the group's progress to date has been limited to drafting revisions to the directives. They also stated that the major obstacle which they have faced is simply finding the time to pursue the group's objectives.

RISK MANAGEMENT PROGRAM HAS NOT YET CORRECTED ADP SECURITY PROBLEMS

In 1983, Treasury reported material weaknesses in its information systems security. In 1984, Treasury reported no material weaknesses but reported that (1) it instituted the Risk Management Program to address these weaknesses, (2) all bureaus were in compliance with the program, and (3) 12 ADP risk analyses were being conducted.

We believe Treasury's report is confusing about the status of corrective actions to address these reported material weaknesses and that Treasury should have continued to report their existence in 1984. First, the Risk Management Program is not yet fully implemented. As previously discussed, problems exist in the extent of its coverage (systems, facilities, and controls). Further, most of the systems identified as covered by the program have not yet been evaluated nor will they be for at least 3 years.

Additionally, it is clear that problems still exist with Treasury's information systems. For example, the Federal Law Enforcement Training Center reported in 1984 that it has no backup for ADP equipment or systems and that ADP personnel are inadequately trained. The U.S. Mint reported a "significant risk environment" in the ADP area as well as "possibilities for breaches of systems integrity." The Office of Revenue Sharing reported that its annual electronic transfer of $4.5 billion is vulnerable to fraud.

Also, in 1984, a Customs Service clerk used one of the Service's ADP systems--Customs Accounting and Management Information System--to issue fraudulent checks worth over $155,000. According to a Customs memorandum, the fraud was "a result of breakdowns in internal control checks." Weaknesses in the ADP application controls of data input (data conversion and entry) and data output (output balancing and reconciliation) contributed to the fraud.

In addition, IRS' internal audit staff has recently identified significant information systems security problems. In a December 1984 internal audit report on the IRS Security Program, the IRS internal audit staff identified numerous problems, including

--inadequate storage and control of vital, irreplaceable magnetic tape files;[8]

--lack of current contingency plans for 6 of the Service's 12 ADP centers; and

--no assurance that appropriate security requirements are included in new ADP procurements or in major modifications to existing systems.

These conditions indicate that problems still exist in Treasury's ADP systems and that the Risk Management Program has not yet examined or resolved them. Thus, Treasury should have clearly reported the continuation of this material weakness.

CONCLUSIONS

Although Treasury made progress in developing a Risk Management Program to evaluate ADP internal controls, the program was not adequately coordinated with the agency's FIA evaluation process to include all ADP systems and all important ADP internal controls. As a result, ADP systems were not adequately evaluated. Treasury has recognized these problems; however, the working group established to resolve them has done little. Treasury needs to eliminate the gaps and omissions which exist in its risk management and FIA evaluations. Furthermore, because previously identified ADP weaknesses have not yet been corrected, Treasury should have clearly indicated the continuation of this weakness in its 1984 annual report.

RECOMMENDATIONS

We recommend that the Secretary of the Treasury:

--Define the ADP facilities, systems, and controls which are to be evaluated through the Risk Management Program and/or the FIA evaluation process.

--Continue to report all previously identified material weaknesses in the Department's annual report until they are fully corrected.

---

[8]One of the much publicized problems of IRS' Philadelphia Service Center is related to this situation. Because of poor controls over processing a replacement tape on Federal Tax Deposit payments, 26,000 business taxpayer accounts were not properly credited for 3 months. This caused incorrect billings, erroneous enforcement actions, and a multitude of other incorrect transactions within those taxpayer accounts, according to an IRS internal audit report.

AGENCY COMMENTS AND OUR EVALUATION

Treasury agreed with the majority of our comments on its coverage of ADP during its 1984 FIA implementation and concurred with our two recommendations. Treasury also acknowledged that the Risk Management Program was not fully implemented in 1984, its first year of operation, and that the first year's efforts were expected to be uneven at best. Treasury believes it will take 2 to 3 years for a program such as this to mature. It also stated that it had not meant to imply in its 1984 letter of assurance that the program had already corrected the 1983 departmentwide material weakness in information systems security.

Treasury said that our criticism concerning the current level of coordination between the Risk Management Program and Financial Integrity Act program may be true. However, it stated that we did not specify how much coordination between the programs is enough. Although we did not specify how much coordination is enough, the following actions--which Treasury recognized were needed--should resolve the problems we identified. As discussed on page 40, Treasury planned to:

--Modify the Risk Management Program to assure adequate coverage of ADP systems and operations, and ADP internal controls.

--Amend their Internal Control Handbook to include information on the Risk Management Program and how it fits into the internal control process.

--Amend the risk management handbook to clarify the relationship between the two programs.

Further, as we pointed out, the four member working group established to address the problem of overlap and possible duplication between (1) the internal control evaluations and accounting system reviews required by the act and (2) information system risk analyses required by OMB Circular A-71 have met rarely. We believe implementation of the above identified actions and effective fulfillment of the working group's objectives would provide enough coordination to resolve the problems we identified.

Treasury is also concerned that we do not recognize the important role of its Office of Inspector General as a control over the Risk Management Program. Treasury Directive 81-41, the Information Systems Risk Management Program, under the section "responsibilities," states

> "The Inspector General shall be responsible for maintaining a central repository for inventories, plans, risk analyses, and certifications, for evaluating the Department's implementation of the risk management program and for using the program in preparing its annual audit plan."

We agree that strong oversight by the Office of Inspector General can be an effective control to assure that a program's requirements are being implemented. However, while the activities required of Treasury's Inspector General by its directive may identify weaknesses in implementing the Risk Management Program, the activities will not necessarily assure that the program includes all controls or that adequate coordination exists.

Treasury also stated that the facts do not support our statement that a potential for duplication existed in a Bureau of Engraving and Printing contract which provided for three ADP related vulnerability assessments and a risk analysis of ADP facilities. Treasury stated that, while the end products of the contract may appear to be similar, the assessments and analyses were necessary to provide adequate coverage from both the OMB Circulars' perspective (A-123 Internal Control Systems and A-71 ADP systems). Further, both are performed using different methodologies and guidelines.

We recognize that the vulnerability assessment and the risk analysis have different methodologies and guidelines, and their objectives are different. Vulnerability assessments rank programs and functions for conducting subsequent internal control reviews while risk analyses rank the degree of risk so security resources can be properly apportioned. Further, by design, vulnerability assessments provide a broader coverage of ADP activities, whereas risk analyses provide indepth, comprehensive coverage of a specific ADP activity. Nevertheless, they both assess controls and security, and work conducted under each effort may meet some of the evaluation requirements of the other. For example, work performed during a risk analysis will address many of the ADP general controls concerning physical security. When a risk analysis adequately identifies strengths and weaknesses concerning an ADP systems' physical security, a separate evaluation of this area would not be necessary under FIA. To eliminate the confusion and the potential for duplication of effort, we believe Treasury's guidance for both the Risk Management Program and FIA should clearly explain the relationship between the two programs and to what extent one may be used to supplement the other.

CHAPTER 5

PROGRESS TOWARD STRENGTHENED ACCOUNTING SYSTEMS CONTINUES BUT MAJOR PROBLEMS REMAIN

In 1984, Treasury reported nearly 80 instances in which its accounting systems did not conform with the Comptroller General's accounting principles, standards, and related requirements (hereinafter referred to as the Comptroller General's requirements).[9] Treasury has initiated corrective actions to address these problems, including some major system redesigns. During 1984, Treasury also corrected many of the deficiencies identified in 1983. Also in 1984, Treasury expanded testing of systems in operation, including some regional locations; updated its systems inventory; and implemented a system to monitor the progress in correcting deficiencies.

Although the Department attempted to disclose all major deficiencies, we believe Treasury did not have an adequate basis in 1984 to determine whether its accounting systems conform with the Comptroller General's requirements, primarily because of the limited examination and testing of its systems caused in part by its delayed start. By making a number of improvements to its evaluations, Treasury will be in a better position to determine the status of its systems.

STATUS OF ACCOUNTING SYSTEM CONFORMANCE

Treasury's fiscal year 1984 accounting systems report stated that 6 of its 26 accounting systems fully conformed, and 2 systems did not conform to the Comptroller General's requirements. The six systems Treasury identified included: (1) IRS payroll, (2) IRS revenue accounting, (3) IRS administrative accounting, (4) Treasury Payroll Information, (5) Financial Management Service investment accounting, and (6) Financial Management Service financial accounting and reporting. The two nonconforming systems were the IRS property system and the Savings Bonds Division accounting system. For

---

[9]The GAO <u>Policy and Procedures Manual for Guidance of Federal Agencies</u> contains the principles, standards, and related requirements to be observed by federal agencies. Specifically, title 2 prescribes the overall accounting principles and standards, while titles 4, 5, 6, and 7 specify requirements governing claims, transportation, pay, leave and allowances, and fiscal procedures, respectively. Also, agency accounting systems must include internal controls that comply with the Comptroller General's internal control standards and related requirements, such as <u>Treasury Financial Manual</u> and OMB Circulars.

the remaining 18 systems, Treasury concluded the systems conform in all material aspects, except for the instances of nonconformance listed in the Department's report.

Treasury identified major deficiencies and has taken or planned corrective action

Treasury has initiated both long- and short-term system improvements to address reported deficiencies. Planned short-term actions appear sufficient to resolve the cited instances of nonconformance. We can not yet determine, however, whether the long-term efforts will resolve all known system problems. Examples of the major system problems and planned solutions follow.

--The Public Debt Accounting System, which records and reports financial information on several trillion dollars, was reported as labor and paper intensive, with cumbersome audit trails. The system has (1) out-of-balance subsidiary and control accounts, (2) an incomplete chart of accounts, and (3) outdated computer system technology. As a result, the Bureau plans a number of enhancements and revised operating procedures to correct these deficiencies. It also plans to reconcile summary and subsidiary data to ensure external reports agree. A long-term enhancement, the Public Debt Accounting and Reporting System, is expected to integrate summary and subsidiary ledgers. The system has a projected completion date of October 1988.

--The U.S. Mint's administrative accounting system, which controls about $172 million annually, does not provide timely cost reports or cost information because the process is predominantly manual. As a result, management does not have the information necessary to evaluate the cost of its programs. Mint officials plan to automate cost accounting applications by the end of 1985.

Actions were taken on 1983 nonconformance items

In 1983, Treasury identified more than 200 instances of nonconformance. During 1984, about 60 deficiencies were corrected, over 30 were eliminated because similar deficiencies were combined, about 60 were judged to need no action, and over 50 remained uncorrected and were again reported in fiscal year 1984.

For those that were corrected, the actions taken appeared reasonable. These actions included submitting required reports, adding disclosure statements to existing reports, establishing necessary accounts, and eliminating separation of duties weaknesses. For example, the Bureau of the Public Debt began preparing a Statement of Financial Condition (SF-220), which provides detailed information on assets, liabilities, and equity. Also, the Office of Revenue Sharing realigned an accounting branch with another division to adequately separate duties associated with its payment process, which disburses $4.5 billion annually.

For the more than 60 deficiencies for which the bureaus determined corrections were unnecessary, Treasury officials said that reevaluations showed the perceived deficiencies did not exist or were not material. About 60 percent relate to deficiencies reported by the Bureau of the Public Debt and the Federal Law Enforcement Training Center. We are unable to comment on whether these decisions at Public Debt were justified because Public Debt was unable to give details on its decisions. Treasury, in its 1984 training, instructed all bureaus to substantiate these types of decisions. Also, we did not review the activities of the Federal Law Enforcement Training Center in Georgia because it has budget authority of about $15 million, which is a relatively small portion of Treasury's total activity.

BETTER DISCLOSURE NEEDED IN YEAR-END REPORT

In 1984, Treasury initiated a program in which it plans to review its systems over 3 years. In each year, certain systems, subsystems, or portions of systems will be examined until all are fully evaluated. Treasury adopted this approach primarily due to time and staffing limitations. Treasury's 1984 report generally described the 3-year accounting system review cycle and provided the number of known nonconformance items in each accounting system. However, the report did not disclose what portions of the systems were evaluated (see app. VII). Without this information, it is not possible for readers to determine the status of the total system.

Given the number and complexity of Treasury's systems, its 3-year cycle approach appears reasonable. However, under this approach, an entire system may not be examined in the first year. In our opinion, a system must be substantially examined and tested before concluding it conforms with established requirements, because more deficiencies may be uncovered later in the cycle. Full disclosure of the extent to which systems have been examined would then place reported deficiencies in the proper perspective.

PROGRESS AND PROBLEMS IN EVALUATING ACCOUNTING SYSTEMS

Although the 1984 accounting system examinations were more detailed, a number of improvements are needed to fully assess the accounting systems. Overall, more comprehensive system examinations and tests of the systems in operation, including internal controls, are needed to determine conformance with the Comptroller General's requirements. Treasury could also benefit by (1) having its managers become more involved in determining whether the accounting systems conform when contractors conduct the FIA conformance evaluations, (2) developing a comprehensive program for training designated evaluation staff, and (3) beginning earlier to avoid concentrating its effort at year-end to meet reporting deadlines.

Treasury recognized a sound work approach was needed to ensure all important features of each system were examined. Also, because of its diverse bureau operations, Treasury needed not only complete system inventories but also consistent examinations to achieve reliable results. Accordingly, the Department specifically required the accounting systems in operation to be tested when examined. The Department also required internal controls in the accounting systems to be examined.

Treasury developed adequate inventories with only a few operations omitted

In last year's report, (GAO/GGD-84-66), we noted several important accounting systems were omitted from Treasury's inventory. Treasury included most of these systems in its 1984 inventory. They also identified two additional accounting operations that had not been considered in 1983. Except for the four operations discussed below, we believe Treasury's 1984 inventory includes all known accounting systems.

The Financial Management Service excluded its check payment and reconciliation system. Treasury officials consider this system to be a process which reconciles and audits the over 600 million checks issued annually by disbursing officers. In calendar year 1984, Treasury indicated approximately $600 billion in federal reserve system payments were entered in the check payment and reconciliation system. We believe it is substantially an accounting system because its operations involve recording, classifying, and reporting financial data related to assets and liabilities. Treasury officials believe that an internal control review of the system, as part of its section 2 evaluation program, would meet all requirements of the act. On the basis of available information, however, we cannot determine whether this review went far enough in considering the Comptroller General's requirements. In June 1985, a Treasury official stated that after considerable discussion and analysis, Treasury's FIA section 4 conformance questionnaire did not appear to be applicable to this system. He went on to state that a section 2 review would be more meaningful and appropriate and that another internal control review has been scheduled for fiscal year 1986 which will consider Comptroller General requirements where appropriate.

Additionally, we found that a billing operation related to the Financial Accounting and Reporting System was not identified. This important operation accounts for about $60 million due from financial institutions for overpayment of Treasury checks. Financial Management Service officials agreed to include this operation in their 1985 inventories.

Finally, in our 1983 report, we noted that Treasury did not consider the systems for the Exchange Stabilization Fund and the Saudi Arabian Deposit Account as being subject to the act. Although Treasury continues to maintain that position, Treasury officials stated they will conduct an evaluation of the Fund as a matter of policy. We were advised Treasury is exploring a similar approach for the Saudi account.

More testing of systems in operation needed

Although Treasury began testing and evaluating its systems in operation, its 1984 examination work was not adequate because it did not (1) include enough regional operations, (2) test general and application controls in automated systems, (3) include sufficient transaction types, and (4) examine and test internal controls in all accounting systems under evaluation this year.

To determine whether a financial system conforms to the Comptroller General's requirements, it is necessary to review and test the system in operation. Although agency personnel may have extensive system knowledge, systems may operate differently than they believe. Therefore, testing should be done on critical aspects of the system and may include (1) interviewing persons who operate the system, (2) observing operating procedures, (3) examining system documentation, (4) applying procedures to live transactions and comparing results, (5) direct testing of computer-based systems by use of simulated transactions, and (6) reviewing error reports and evaluating error follow-up procedures.

Tests should be designed to disclose whether valid transactions are processed properly and whether the system rejects invalid transactions. The tests should cover the entire transaction, from initial authorization through processing, posting to the accounts, and reporting. Accordingly, manual as well as automated operations should be included. In developing test plans, consideration should be given to the results of any prior system testing.

This testing criteria has been adopted by OMB and included in Appendix H of its publication Guidelines for Evaluating Financial Management/Accounting Systems (May 20, 1985). In determining the tests that would be appropriate for any system, it is important to keep in mind that, in most cases, more than one of the above techniques are needed to test all important aspects of an accounting system, and that transaction testing is essential.

Further, if accounting operations are carried out in regional locations, these regional operations should be examined for the federal manager to be confident there is a uniform implementation of the system.

More regional accounting locations should be tested and evaluated

Treasury reported 11 accounting systems with regional applications. Nine of these accounting systems having regional operations were scheduled for review in 1984. Treasury evaluated regional applications in six of these systems. Three of the nine accounting systems scheduled were not reviewed. For example, the IRS payroll system, operated in seven regional locations, was not tested at any of these locations because of the limited time available. This system, however, was reported to be in full conformance with the Comptroller General's requirements based on the completion of an evaluation of one of the three payroll subsystems.

For the six accounting systems where regional operations were examined, we believe not enough locations were included to provide an in-depth system review and assurance that the systems meet Comptroller General requirements. For example, a Financial Management Service accounting system was operated in seven regional locations where government disbursements were generated. Primarily on the basis of an examination at only one of the seven locations, Treasury reported that this system conforms except for two instances of nonconformance.[10] Treasury believed it was justified in relying on the accounting system examination at one location (Washington, DC) to identify any nonconformance items, because the same system was considered to be in place at all regional locations.

Our work on the system has disclosed that the types of transactions and transaction processing were not uniform in all locations. For example, while Treasury's Washington, DC, and Philadelphia, PA, disbursing operations both prepare and mail checks and bonds and process electronic payments through Treasury's Financial Communication System, there are dissimilarities in their operations. The Philadelphia Financial Center processes large volumes of recurring payments (social security checks) and takes unique recovery actions associated

[10]Financial Management Service officials, subsequent to their 1984 status report on accounting systems, provided us with copies of the remaining six locations' evaluations. These, however, are still incomplete since the internal control reviews will not be complete until the end of 1985.

with these types of payments. The Washington Financial Center, on the other hand, more frequently uses optical character recognition equipment to process disbursements, and it is the only financial center which makes disbursements in foreign currency and reconciles Treasury's bank accounts in foreign countries.

Treasury needs to examine more accounting system internal controls

The internal controls of 11 Treasury accounting systems were not evaluated when the system was examined for conformance with the Comptroller General's requirements. Although Treasury recognized in its guidelines a need to examine these controls through internal control reviews or other systematic review methods, its accounting system reviews were not designed to address specific internal controls, nor did Treasury require the examination of internal controls at the same time the accounting system was examined.

A concurrent review of an accounting system's internal controls is necessary because internal controls are an integral part of the Comptroller General's requirements. A system's conformance with the Comptroller General's requirements cannot be judged without such an examination. Also, an evaluation of the strengths and weaknesses of internal controls is one factor needed to determine the scope of testing necessary in an accounting system. In addition, it is simply a more efficient way to go about doing it--look at all related facets of the system at the same time.

While a few bureaus planned to review entire systems in 1984, most bureaus submitted plans to review accounting subsystems during the 3-year cycle. These plans did not indicate when the accounting system internal controls would be evaluated. Thus, the examination and testing of conformance with Comptroller General's requirements may not coincide with reviews of internal controls. Also, the bureaus may need to duplicate previous work because initial testing did not consider the internal controls.

Testing of systems in operation needs to be expanded

Treasury employs both manual and automated accounting systems. For automated systems, it is important to examine both application controls (controls pertaining to data origination, entry, processing, and output) and general controls (computer security, access, and system design). If such controls are not in place, there is a risk of processing erroneous data, inaccurate reports, and unauthorized system access.

We found no evidence general controls were reviewed under section 4 in the 16 automated accounting system operations

Treasury examined in 1984. We also found no evidence the accounting system review teams coordinated their examinations with other Treasury internal control review teams to determine whether an examination of the ADP systems' controls had been performed. Treasury, therefore, has incomplete information on whether the automated systems conform.

Another issue relates to the number and types of transactions selected. We found no Treasury examinations that were sufficient in this area. For example:

--The financial reporting subsystem for a Customs accounting system was evaluated in 1984. According to available documentation, the subsystem included at least five financial reports, but the evaluation was limited to testing one daily financial report and a portion of the data input for the daily report at one regional location. Similar monthly reports were not tested. Also, the reporting function was not tested at the bureau's headquarters.

--The Financial Management Service's central accounting system was tested, but transactions containing invalid data were not included. These should be tested to ensure the system does not allow such transactions to be processed and cause inaccurate reports.

<u>Expanded training and guidance for testing system operations is needed</u>

Treasury provided its staff responsible for completing 1984 accounting system examinations limited information on proper testing procedures. Guidance, provided in August 1984, was in two forms: written departmental guidelines and training on implementing the guidelines. While the guidance called for examinations to include testing, the guidance did not adequately describe how to (1) determine which standards to test, (2) develop test plans, (3) conduct tests, and (4) systematically review internal controls. Treasury sponsored a 2-1/2 hour formal training session which provided a general overview of the departmental guidelines without expanding on the key issues cited above. This is substantiated by our observations that more testing is needed for regional accounting operations, automated system controls, different transaction types, and internal controls.

Treasury's administrative monitoring team for section 4 of the act reviewed selected documentation and tests and discussed questions concerning the evaluation process. The team's visits verified the need for more training and standards for evaluating and testing internal controls. During April 1985, Treasury conducted a 2-day training course for its bureau staff which included instructions in documenting their evaluations, testing, and reviews of internal controls and regional locations. We believe this training should assist bureau staff to make more complete examinations of Treasury's accounting systems.

Earlier start on accounting system evaluations will be helpful

In our view, more progress would have been made this year if Treasury had begun its examinations earlier. Because Treasury did not issue its guidelines until August 9, 1984, and bureau evaluation reports were due November 1, Treasury staff had only a short period to complete the accounting system reviews. The relatively short time contributed to some of the problems previously mentioned: some staff restricted the scope of the evaluations and limited the amount of system testing, did not do internal control evaluations, or did not evaluate regional accounting operations.

Some internal audit organizations also could not fully assess accounting system reviews, because their evaluation report was needed by the Inspector General for input into the Secretary's section 4 report before the review was completed. For example, one independent contractor completed an accounting system evaluation on October 22, 1984. The internal audit organization, whose fieldwork was complete before the contractor's work, was unable to fully evaluate the assessment. The independent contractor for another accounting system did not begin work until October 15, 1984--the date the internal audit organization's report draft was due.

The Inspector General, in a December 1984 report, concluded that actions were needed to avoid limiting the time available for future accounting system reviews. We concur, and we believe Treasury should start its review process as early as practicable in the fiscal year covered. In effect, the evaluation program should be a concurrent and continuous process. Treasury initiated 1985 work in January with a memorandum to heads of bureaus requesting they appoint a high level official to be responsible for the 1985 review. An additional memo was sent on February 21, 1985, requesting bureau coordinators to begin the annual review of their accounting systems. The FIA Administrative System Coordinator advised that, by June 30, all bureaus had submitted accounting system inventories and evaluation plans for fiscal year 1985 and were in the process of implementing these plans.

Treasury staff should participate in system evaluations

Treasury used contractors to assist in or perform conformance evaluations of 12 accounting systems in 1983 and 11 accounting systems in 1984. Ultimately, to best benefit from the act, Treasury needs to rely more on its own staff, thus building expertise and providing continuity from one year to the next. We recognize that at times it may be appropriate to use contractor assistance. However, if agency staff participate in the reviews, they have the opportunity to gain the experience and understanding necessary to permit them to perform the reviews in subsequent years.

While Treasury recognized that competing work of the bureaus may tax their resources and contractor assistance could be needed, it also recognized the need to reduce reliance on contractors. Therefore, the Department is requiring the bureaus to justify the need for contractor assistance. We believe this action may lead to increased managerial involvement in the evaluations. Such involvement could improve review continuity by building on previous years' experience and, therefore, better meet the intent of the act by focusing the federal managers' attention on the accounting systems.

CONCLUSIONS

Treasury has progressed in evaluating and strengthening its accounting systems in 1984. The agency did identify and report major system deficiencies and took action to correct others. Treasury has a number of major long-term system improvement efforts underway and seems committed to strengthening its systems.

Although progress was made, we believe Treasury does not yet have a sufficient basis to determine whether the accounting systems conform with the Comptroller General's requirements and that all instances of nonconformance have been identified. We believe several areas need strengthening before the act's objectives of improved accounting systems can be achieved.

Treasury needs to test its systems in operation with valid and invalid transactions and include internal controls, regional accounting operations, and automated system controls and emphasize the need for financial managers to be more closely involved in implementing the act. These problems need to be addressed for those systems already reviewed, as well as any new or redesigned systems to be reviewed in the future. Further, Treasury's year-end statement could be improved if more information were given on the scope of the systems' evaluations.

RECOMMENDATIONS

We recommend the Secretary of the Treasury not report systems to be in conformance with the Comptroller General's requirements until they have been adequately evaluated in operation. We further recommend that the Secretary

--expand system testing to include (1) both valid and invalid transactions, (2) general controls over automated systems, and (3) concurrent reviews of internal controls;

--provide for increased staff involvement in accounting system reviews to the extent resources permit;

--expand the 3-year cycle examinations and testing to include regional/field accounting operations and all accounting systems; and

--disclose in the year-end report the extent to which the systems have been evaluated.

AGENCY COMMENTS AND OUR EVALUATION

Treasury did not comment on our recommendations, but did offer a variety of general comments. Treasury commented that our report did not mention that the Inspector General audited the FIA reviews. Treasury further commented that the conclusions reached as a result of these reviews contributed to its reasonable assurance opinion on its accounting systems. The Inspector General concluded that the processes used by the Department were generally satisfactory and made recommendations to improve the FIA process. The Inspector General's work and opinion on Treasury's 1984 evaluations were primarily concerned with the Department's processes used to evaluate its accounting systems. In addition, as discussed on page 53, we believe the timing of Treasury's evaluations, coupled with the deadlines for the Inspector General reports, limited the time available to complete the reviews of the FIA evaluations.

In another comment, Treasury disagreed with our position that their report should better disclose the extent to which they reviewed their systems. As discussed on page 47, we believe full disclosure is needed regarding the extent a system is evaluated to place reported deficiencies in the proper perspective. Without this information it is difficult for the reader to determine the status of the total system.

Treasury also believed they had a reasonable basis for determining whether their systems conform with the Comptroller General's requirements and that limited reviews of systems not fully evaluated in 1984, coupled with the Inspector General's review, contributed to the Department's reasonable assurance opinion. While the Inspector General's statement on Treasury's processes was positive, it also recommended areas in which Treasury can improve. In fact, some of these parallel our own observations. For example, the Inspector General makes recommendations concerning training, the need for more involvement in the FIA evaluations by bureau personnel, and the need for better documentation (see our observations on pp. 47, 48, 52, and 53).

As we state on page 49, determining whether a system conforms to the Comptroller General's requirements necessitates reviewing and testing the system in operation. Although

Treasury has conducted considerable work on its systems, we found that the systems inventory was not complete, insufficient regional locations were evaluated, general controls over automated operations were not reviewed, and the numbers and types of transactions tested were not sufficient (see pp. 48-52). As a result, we continue to believe that additional efforts are needed for Treasury to determine its systems are in conformance.

Treasury also disagreed with our comment that their guidelines did not require concurrent reviews of accounting systems and their associated internal controls. We believe Treasury guidelines were not clear with regard to this requirement. The Treasury guidelines directed the Internal Control Officer to consult with the Financial Management/Accounting Systems' coordinator to ensure internal control reviews coincide, where practicable, with accounting system reviews. The guidelines were not interpreted by the bureaus as requiring the specific performance of such reviews. This lack of specification contributed to 11 accounting systems being evaluated in 1984 without a concurrent evaluation of internal controls.

Treasury also disagreed with our position that we found no systems where sufficient numbers or types of transactions were tested and added this was not an accurate assessment of the total work being done by its bureaus. As stated on page 5, we examined in detail 12 accounting system evaluations in 4 bureaus and also obtained information on all bureaus evaluations--including reviewing documentation and testing. We found 17 of 24 accounting systems evaluated by Treasury in 1984 had insufficient numbers or types of transactions tested. This represents 71 percent of the systems evaluated in 1984. As we acknowledged on pages 45, 48, and 54, Treasury continues to make progress in its accounting system evaluations. We believe, however, based on our reviews of bureau evaluations, that additional testing is needed to determine conformance with the Comptroller General's requirements.

Finally, Treasury commented that the timeliness of our report was not satisfactory for them to take corrective actions during the fiscal year 1985 review of accounting systems. During and at the conclusion of our work in March 1985, we discussed the issues in this report with Department and bureau FIA coordinators. We also attended their April 1985 training session and provided observations obtained through our reviews of their 1984 evaluations. Additionally, as noted throughout the report, Treasury took or agreed to take actions to address many of our concerns (see pp. 48, 49, 52, 53, 54). We believe, therefore, that sufficient time was available for Treasury to use the results of our work to improve its 1985 accounting system reviews.

SCOPE OF GAO REVIEW

Table I.1

Analysis of Treasury's Vulnerability Assessments

Bureau	Total assessable units	Assessments made in 1984	GAO review: Number analyzed	GAO review: Field work
IRS	728	302	278	2
Customs Service	417	417	395	22
Financial Management Service	100	-	-	1
Alcohol, Tobacco and Firearms	101	101	-	-
Public Debt	128	3	-	-
Mint	469	460	61	-
Engraving and Printing	47	47	-	-
Office of the Comptroller of the Currency	101	101	84	-
Office of the Secretary	26	-	-	-
Office of Revenue Sharing	9	-	-	-
Savings Bonds Division	10	10	-	-
Secret Service	16	16	-	-
Total	2,152	1,457	818	25

Table I.2

Assessments Reviewed by GAO Field Staff

Assessable units	Customs Service regions: Northeast	South central	South-west	Pacific
Seized, forfeited, and abandoned property	X		X	X
Revenue collections	X		X	X
Overtime management		X	X	X
Treasury Payroll/Personnel Information System	X	X	X	X
Classification, appraisal, admissibility			X	X
Land passenger examination	X		X	X
Air passenger examination	X	X	X	X

Table II.1

Variables for Each Step in
A Vulnerability Assessment

General control environment	Inherent risk analysis	Preliminary evaluation of safeguards [a]
1. Management attitude	1. Purpose and characteristics	1. Reasonable assurance
2. Organizational structure	2. Budget level	2. Supportive attitude
3. Personnel	3. Impact outside agency	3. Competent personnel
4. Delegation and communication of authority and responsibility	4. Age and life expectancy	4. Internal control objectives
5. Policies and procedures	5. Degree of centralization	5. Internal control techniques
6. Budgeting and reporting practices	6. Special concerns	6. Documentation
7. Organizational checks and balances	7. Prior reviews	7. Recording transactions
8. ADP consideration	8. Management responsiveness	8. Executing transactions
		9. Separation of duties
		10. Supervision
		11. Access to resources

[a]The guidelines on evaluating safeguards do not specifically detail the variables that should be considered. OMB's guidance, however, indicates that the completion of the three steps permits the managers to assess the adherence of a function's internal control system to at least some of GAO's internal control standards. The guidance also contains a suggested form detailing the 11 listed GAO standards to document the assessment. Treasury used these standards as variables in making the preliminary evaluation of safeguards.

Table III.1

Analysis of Inconsistency in Combining Ratings of Three Steps Into Overall Assessment Ratings[a]

Assessment step ratings			Overall vulnerability rating				Inconsistent	
Control environment	Inherent risk	Safeguards	Low	Moderate	High	Total	Number	Percent
Low	Low	Low	350	6	1	357	7	2
Low	Low	Moderate	4	1	0	5	1	20
Low	Low	High	12	1	0	13	1	8
Low	Moderate	Low	129	47	1	177	48	27
Moderate	Low	Low	17	3	0	20	3	15
Low	High	Low	45	23	1	69	24	35
Low	Moderate	Moderate	1	16	0	17	1	6
Moderate	Moderate	Low	4	39	0	43	4	9
Moderate	Moderate	Moderate	4	38	0	42	4	10
Low	High	Moderate	0	5	2	7	2	29
Moderate	High	Low	0	4	2	6	2	33
Moderate	High	Moderate	0	12	3	15	3	20
High	Moderate	Moderate	0	2	1	3	1	33
High	High	Moderate	0	1	3	4	1	25
Moderate	Low	Moderate	0	8	0	8	0	0
Low	High	High	3	0	0	3	0	0
High	Moderate	Low	0	0	1	1	0	0
Moderate	Moderate	High	0	0	1	1	0	0
Moderate	High	High	0	0	2	2	0	0
High	Moderate	High	0	0	3	3	0	0
High	High	High	0	0	7	7	0	0
One or more ratings missing			6	6	2	15[b]	15	100
Total			575	212	30	818[b]	117	14

[a]The analysis involves assessments made by four bureaus: U.S. Mint, Customs Service, OCC, and IRS.

[b]Totals do not crossfoot because no overall rating was assigned to one of the assessments examined.

ADEQUACY OF VULNERABILITY ASSESSMENT COVERAGE

Table IV.1

Vulnerability Assessments Which Did And Did Not Include All Major Operations

	Region			
Assessable unit	Northeast	South Central	Southwest	Pacific
Seized, forfeited, and abandoned property	No	a	No	No
Revenue collections	No	Yes	No	Yes
Overtime management	a	a	Yes	No
Treasury Payroll/ Personnel Information System	Yes	Yes	No	No
Classification, appraisal, admissibility	a	a	Yes	No
Land passenger examination	Yes	b	Yes	No
Air passenger examination	Yes	Yes	Yes	No

[a] Vulnerability assessments were not reviewed.

[b] South Central region does not have any land border processing responsibility.

Table V.1

Customs Service's
Documentation of an Internal Control System

Program Office: Office of Cargo Enforcement and Facilitation

Prepared by: ____________

Assessable Unit: Cargo Control

Manager of Assessable Unit: ____________

Event Cycle	Risk if Controls are Lacking	Control Objective	Control Technique
1. Bonding review process.	Government may lose revenue if imported cargo is not properly reported and controlled.	Ensure against loss of revenue to the Government.	Surety bonds must be posted for all imported cargo which is transported or maintained in storage.
2. Determination of shipments to be examined.	Shipments of goods may illegally enter the country or may be inappropriately entered into the U.S. Commerce without proper Customs review or correct duty paid.	Ensure that only shipments which need examination are examined and that shipments of particular risk or concern are identified and examined.	Establish automated information system (ACCEPT) for determining which shipments should be examined, based on criteria which include information on suspicious shipments, first-time importation, importers with prior violations, quota merchandise, etc.
3. Acceptance and review of cargo manifest and other related documents.	Merchandise or contraband may enter U.S. Commerce without knowledge of Customs or other concerned agencies.	Ensure that Customs knows and controls what cargo enters the U.S.	Review manifest for correctness. Review bills of lading to identify suspicious shipments or those which might be especially subject to pilferage as well as to ensure bills of lading agree with manifest.

INFORMATION ON TREASURY'S RISK MANAGEMENT PROGRAM

Table VI.1

Implementation of the Risk Management Program in Treasury Bureaus in 1984

Treasury bureau	Approved risk mgt. Plan	Risk management inventory		Completed risk analysis		Appointed security officer
		System	Facilities	System	Facilities	
Office of the Secretary-Office of Revenue Sharing	No					Yes
Comptroller of the Currency	Yes	10	1	b		No
U.S. Savings Bonds Division	a					
Internal Revenue Service	Yes	8	12		1	c
Secret Service	Yes	11	1	b		Yes
Customs Service	No					Yes
Financial Management Service	Yes	21	1			Yes
Public Debt	No					Yes
Engraving and Printing	Yes	4	1		1	Yes
Mint	Yes	8	1	b		Yes
Alcohol, Tobacco and Firearms	Yes	4	0			Yes

[a]Savings Bonds Division does not operate any information systems or facilities, but relies on other Treasury bureaus for ADP services.

[b]The Office of Comptroller of the Currency, Secret Service, and the U.S. Mint each completed a risk analysis in late 1984. However, the three risk analyses were not finalized and approved.

[c]IRS has established a security officer position at each information system facility; however, only 1 of the 12 facilities has filled the position.

SCOPE OF BUREAUS' PLANNED EVALUATIONS

Table VII.1

Department of the Treasury's Planned Examination of Accounting Systems for Fiscal Year 1984

Bureau	System	Percent of system scheduled for examination[a]
Office of the Secretary	Administrative Accounting	100
	Working Capital Fund	100
	Treasury Payroll Information	100
Office of Revenue Sharing	Administrative Accounting	100
Alcohol, Tobacco and Firearms	Administrative Accounting	25
Comptroller of the Currency	Administrative Accounting	33
Customs Service	Administrative Accounting	33
	Revenue Accounting	33
Engraving and Printing	Administrative Accounting	29
Federal Law Enforcement Training Center	Administrative Accounting	33

[a]These percentages represent the bureaus' planned evaluation of their systems. We believe that actual evaluations, however, did not meet their plan because all locations were not evaluated, testing was incomplete, internal controls were not always evaluated, and all components were not identified.

SCOPE OF BUREAUS' PLANNED EVALUATIONS

Table VII.1 (Cont)

Department of the Treasury's Planned Examination of Accounting Systems for Fiscal Year 1984

Bureau	System	Percent of system scheduled for examination[a]
Financial Management Service	Administrative Accounting	100
	Disbursing Accounting	100
	Investment Accounting	100
	Central Accounting for Cash	100
	Foreign Currency Accounting	100
	Financial Accounting and Reporting	100
Internal Revenue Service	Administrative Accounting	40
	Revenue Accounting	33
	Payroll	100
	Property Accounting (CAMS)	0
Mint	Administrative Accounting	33
	Bullion and Monetary Accounting	50
Public Debt	Administrative Accounting	b
	Public Debt Accounting	7
Savings Bonds Division	Administrative Accounting	29
Secret Service	Administrative Accounting	100

[a]These percentages represent the bureaus' planned evaluation of their systems. We believe that actual evaluations, however, did not meet their plan because all locations were not evaluated, testing was incomplete, internal controls were not always evaluated, and all components were not identified.

[b]This system was not evaluated because it was being replaced early in calendar year 1985.

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

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

DEPARTMENT OF THE TREASURY
WASHINGTON

ASSISTANT SECRETARY

September 20, 1985

Dear Mr. Anderson:

This is in response to your letter of August 5, 1985, requesting our comments on the General Accounting Office's (GAO) Draft Report, "Treasury's Second Year Implementation of the Federal Manager's Financial Integrity Act: Unreliable Evaluations Detract From Progress." We appreciate having the opportunity to respond to the Draft Report's analyses and recommendations.

At Tab 1, we have provided our detailed comments on the contents of the Report. Overall, the technical analyses conducted by your staff of the Department's internal control processes were of high quality and reinforced some of the conclusions we had already reached concerning the process within the Department. The information and insights provided in the Report will be of great value to us in planning future internal control initiatives.

The Report also contains a number of recommendations for improving the Department's internal control processes. We concur with several of them but have reservations about implementing others. We are particularly concerned with conclusions reached in the Report on the substance and "reasonableness" of Treasury's Second Annual Assurance Letters to the President and the Congress. Additionally, we noted the Report fails to recognize other issues we believe are critical in the implementation of the Federal Managers' Financial Integrity Act (FMFIA) in the Department.

It is stated throughout the Report that Treasury did not have an adequate basis upon which to conclude that its systems of internal control provide reasonable assurance that the objectives of the FMFIA were achieved. This finding was based, in part, on an audit of vulnerability assessments in several Treasury bureaus. Vulnerability assessments are not the sole basis for Treasury's assurance statements and reports to the President and the Congress.

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

Each year, Treasury's bureaus and offices are requested to review the results of vulnerability assessments, internal control reviews, audit reports, reviews of internal control under Section 4 of the FMFIA, management reviews, contractor studies and other source material in preparing reports and assurance letters. These reviews, studies, reports, and analyses involve all levels of management and operational staff, including the Inspector General.

Treasury's annual review process adheres to the instructions promulgated by the Office of Management and Budget (OMB). OMB has not established, nor do they believe it realistic to establish, minimum evaluation criteria for agencies to achieve before reasonable assurance statements can be written. OMB has stated that the sum and substance of all information available to management is to be considered in making a reasonable assurance determination for use in the year-end internal control statements.

On somewhat of a related issue, the Report does not recognize that Treasury bureaus and offices already perform a number of evaluative activities which assist managers to assess the vulnerability of and uncover weaknesses in systems of internal control. Our respective staffs have discussed this issue extensively and mention should be made of this in the Report.

We believe strongly that the internal control system should be useful and not include the collection of unnecessary statistical data. It should be a management tool that enhances control without unreasonable restrictions on our operations and available resources. We feel that focusing too much attention on the "process" and not enough on results defeats the objectives of eliminating waste, fraud, and mismanagement.

Sincerely,

John F. W. Rogers
Assistant Secretary of the
Treasury (Management)

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

DEPARTMENT OF THE TREASURY
RESPONSE TO THE GENERAL ACCOUNTING OFFICE
DRAFT FISCAL YEAR 1984 REPORT

GENERAL COMMENTS

It is stated in the Report that "Treasury does not yet have a sufficient basis to determine whether its internal control and accounting systems comply with the act...".

- Treasury's annual evaluation of its systems of internal control complies with Office of Management and Budget's (OMB) guidelines and policies. OMB has stated that the sum and substance of all information available to management is to be considered in making the reasonable assurance determination in year-end internal control statements.

- Within Treasury, vulnerability assessments are not the sole source of material weaknesses in systems of internal control. All sources are analyzed to determine material weaknesses. Only after this comprehensive study do bureau heads and Assistant Secretaries certify the reports to the Secretary.

CHAPTER 2

- A recommendation is included that Treasury "improve departmental monitoring, including requiring departmental Financial Integrity Act (FIA) staff to periodically visit the bureaus to review phases of the process and to provide feedback to the bureaus on their FIA efforts."

  We concur with this recommendation and have already taken action to implement it. Our quality assurance program has been expanded in Fiscal Year (FY) 1985. The Department's internal control staff is meeting with bureau internal control personnel on a quarterly basis. A simplified set of internal control guidelines has been developed, and seminars are being held on pertinent internal control topics. Additional staff is being assigned to the process at both the Department and bureau levels.

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

- Regarding the Treasury Internal Control System (TICS), all of the information in this automated monitoring system has been updated. Printouts of the information in the system are being provided to the bureaus for their use. The Department uses the data to monitor bureau activities and to prepare reports for policy officials.

  Currently, possible enhancements to the TICS and the Audit Recommendation Monitoring System are being studied. The focus is on integrating both systems or, at a minimum, simplifying them. An additional objective involves the transfer of both systems from a mainframe computer to more convenient personal computers.

CHAPTER 3

- It was recommended Treasury "monitor Customs Service's implementation of its alternative vulnerability assessment process and test the approach on a sample basis at several bureaus to determine whether it improves the reliability of the assessments and should be adopted Departmentwide."

  We concur with this recommendation, except for that portion which would have us test the system in other bureaus. Customs is not expected to complete its preliminary data collection until the second quarter of FY 1986. Following the data collection and verification, Customs intends to obtain an independent quality review of the documentation. Additionally, a rating and ranking system is still undergoing development.

  We will continue to monitor Customs' progress with the new process, but we would refrain from testing the technique elsewhere until its feasibility is proven in Customs. In our opinion, it would be imprudent to disrupt the processes in other bureaus until the Customs' approach is completed and verified.

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

- The GAO recommends that Treasury "require bureaus conducting vulnerability assessments in FY 1986 to detail how they plan to assure that their assessments are reliable and to evaluate the adequacy of such plans relative to the problems discussed in this report."

  We concur with this recommendation provided a reasonable standard for reliability can be established. Treasury's directives and instructional memoranda have covered the area of reliability and quality control at great length. Treasury's internal control personnel and speakers stress quality control at meetings and training sessions.

  Caution, however, must be exerted to ensure the vulnerability assessment process does not become needlessly more complicated and paper-intensive through the imposition of yet another condition. To do so would result in the process losing its utility as a screening device.

COMMENTS FROM BUREAUS AND OFFICES ON ISSUES COVERED IN CHAPTERS 2 AND 3

SECRET SERVICE:

- The GAO urges the involvement of field offices in the vulnerability assessment process. The Service contends that the high degree of centralization of <u>all</u> functions mandates performance of vulnerability assessments by Headquarters personnel to insure their validity and reliability.

  While Secret Service operations are dispersed throughout the country, high level protective, investigative and administrative personnel are centralized in Headquarters and other facilities located in Washington, DC. All policies and procedures are developed within Headquarters for dissemination to field offices. Field office activities are controlled and routinely monitored by Headquarters. There is little possibility of undetected deviation from established policies and operational strategies by field components.

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

- o The GAO also recommends the Service conduct vulnerability assessments on units "omitted" from the process -- the Safety Program, the Office of Inspection, and the Management and Organization Division. The Service considered these programs and related activities when developing their inventory of assessable units. However, the programs were excluded because it was determined that they fell within the policy-making exclusions permitted by the Office of Management and Budget Guidelines.

ENGRAVING AND PRINTING:

See Comment 1.

- o The fourth paragraph on page 11 implies that the Bureau of Engraving and Printing had not made any progress in improving accounting system documentation over production planning and inventory control. During 1983, the Bureau reported weaknesses concerning documentation of its operating accounting system and reconciliation of a fixed asset physical inventory to the general ledger records. Both of these weaknesses have been addressed subsequently. Accordingly, this reference to the Bureau should be deleted from the GAO's final report.

CHAPTER 4

These comments address primarily Chapter 4 of the Draft Report, "Improvements Needed to Evaluate ADP (automated data processing) and Correct ADP Security Programs."

Now on pp. 7,38 and 42.

- o We appreciate the complimentary points made by GAO on our OMB Circular A-71 (Security of Federal Automated Information Systems) risk assessment program (Treasury Directive (TD) 81-41) on pages 10, 47, and 52. The program was not fully implemented in 1984, its first year of operation. We explained to the GAO staff, and they acknowledged, that the first year's efforts would be uneven at best. It takes two to three years for a program like this to mature. In 1983, Treasury reported under the Federal Managers' Financial Integrity Act (FMFIA) that data processing, in

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

general, was vulnerable. In 1984, we reported that our A-71 program was instituted to address that weakness. We did not mean to imply, as this Draft asserts on page 43, that the vulnerability had been corrected.

Now on p. 36.

See Comment 2.

o The statement on page 47 that the FMFIA "requires that all ADP systems be evaluated" is in error. The FMFIA does not use the terms "all" or "ADP systems."

Now on p. 40.

Now on p. 42.

o The GAO's criticism of the lack of documented internal controls in TD 81-41 is true. Our efforts to correct this problem are acknowledged on page 49. The GAO's criticism of the level of coordination between the various FMFIA <u>may</u> be true, but it is not specified how much coordination is enough. We believe the GAO should describe the important role of Treasury's Inspector General in the A-71 program. This role is described in TD 81-41 and represents one of the most effective controls that we have over the program.

o We concur with the two recommendations on page 52. First, "Define the ADP facilities, systems and controls which are to be evaluated through the risk management program and/or the FIA evaluation process." Secondly, "Continue to report all previously identified material weaknesses in the Department's annual report until they are fully corrected."

Now on p. 39.

o The fourth paragraph on page 47 discusses the potential for duplication of effort because of a Bureau of Engraving and Printing contract that provided for three ADP related vulnerability assessments and a risk analysis of ADP facilities. While the end products of the contract may appear to be similar, the vulnerability assessments and the risk analysis were both deemed necessary to provide adequate coverage for Bureau ADP activities from both an OMB Circular A-123 (Internal Control Systems) and Circular A-71 perspective. Further, a vulnerability assessment and a risk analysis are required to be performed using different methodologies and guidelines. The GAO Report appears to take exception to the Bureau approach of performing both reviews and implies that work performed was of duplicative nature. The facts do

ADVANCE COMMENTS FROM THE DEPARTMENT OF THE TREASURY

not support this conclusion. We believe the GAO position regarding concurrent evaluations should be clarified to provide additional guidance regarding the appropriate level of A-123 and A-71 interface.

CHAPTER 5

General Comment - Timeliness of the Report is unsatisfactory as it permits no time for Treasury to take corrective actions during the FY 85 review of accounting systems.

General Comment - The GAO Report neglects to mention that Treasury's Inspector General audited the reviews being done of Treasury's accounting systems. The Inspector General concluded that the reviews were generally in accordance with the Federal Managers' Financial Integrity Act, OMB Circular A-123 and OMB Guidelines.

Now on p. 47.

See Comment 3.

- On page 56, reference is apparently being made to administrative accounting functions within the Bureau of the Public Debt. At the closing conference with GAO personnel, the Bureau reported 26 instances of non-conformance in FY 83 and only 7 major instances of non-conformance in FY 84. The Bureau explained that the 7 major instances of non-conformance were a consolidation of the 26 reported in FY 83. This information was given to the GAO in detail.

Now on p. 47.

- On page 57 the Report states, "However the report did not disclose what portions of the system were evaluated." If this is a deficiency, then the GAO Report is equally deficient in its numerous references to unspecified systems or sub-systems.

  Furthermore, the Report states that "In our opinion, a system must be substantially examined and tested before concluding it conforms with established requirements because more deficiencies may be uncovered later." The GAO gives no reference to our limited reviews of all sections not reviewed in detail, and the Inspector General's review and opinion on the systems reviews. These contributed to the Treasury's arrival at a "Reasonable Assurance" opinion.

ADVANCE COMMENTS FROM THE
DEPARTMENT OF THE TREASURY

Now on p. 51.

o On page 62 the GAO states, "nor did Treasury require the examination of internal controls at the same time the accounting system was examined." This is incorrect; on page 7 of the FY 1984 Guidelines, Treasury states: "In scheduling these reviews, the Internal Control Officer should consult with the Financial Management/Accounting Systems' coordinator to ensure that the internal control reviews coincide, where practicable, with the reviews made to determine conformance with accounting principles and standards other than internal control." GAO staff members attended training sessions held by the Department at which the bureaus were told that the reviews of internal control would have to be done in the same time period as the detailed accounting systems reviews.

Now on p. 52.

o The fourth paragraph on page 63 concludes that examinations of accounting systems were not sufficient in terms of the number and types of transactions tested. This is not an accurate assessment of the total amount of work being done by Treasury bureaus. We do not know where the GAO got sufficient testing information on all 28 Treasury accounting systems to make such a comprehensive statement.

See Comment 4.

For example, the Office of Revenue Sharing was not consulted about the 1984 Arthur Young and Company review. Moreover, the Bureau of Engraving and Printing (BEP) has been subject to comprehensive, independent financial audits on an annual basis, which include in-depth examinations of internal controls within the Bureau's accounting system. These independent audits have been necessitated by the fact that the Bureau operates a very complex commercial-type financial system, rather than an administrative accounting system used by agencies with appropriated funds.

See Comment 5.

During 1984 the BEP also performed further transaction testing and internal control reviews of two major accounting subsystems. Accordingly, it is BEP's view that their efforts in this area provided a more than sufficient basis to ensure conformance with Comptroller General principles, standards, and related requirements.

The following are GAO's comments on the Department of the Treasury's letter dated September 20, 1985.

GAO COMMENTS

1. Because the Department completed corrective action after preparation of this draft, we deleted this information in the final report.

2. We modified our report on page 38 to reflect Treasury's comment.

3. We learned, after discussing this comment with Treasury officials, that the Department misunderstood our discussion on page 46 concerning decisions to take no action to correct about 60 nonconformance items. The 26 instances of nonconformance referred to by Treasury in its comments were reported. Our discussion relates to 60 instances which were not reported because decisions were made by Public Debt not to take corrective action.

4. In our report we list 26 accounting systems shown in Treasury's accounting system inventory. In its comments Treasury refers to 28 systems. A Treasury official clarified that the difference was due to their inclusion of the Saudi Arabian Deposit Account and the Exchange Stabilization Fund. Treasury still disputes the applicability of the act to these two systems; however, it is pursuing some type of evaluation of them (see p. 49).

5. As indicated on page 5, the Office of Revenue Sharing and the Bureau of Engraving and Printing were not bureaus where we did detailed reviews of system evaluations. Our limited review of the methodology used at the Office of Revenue Sharing, however, did not indicate that invalid transactions were used for testing transactions.

(015025)

For sale by:

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

Telephone (202) 783-3238

Members of Congress; heads of Federal, State, and local government agencies; members of the press; and libraries can obtain GAO documents from:

U.S. General Accounting Office
Document Handling and Information Services Facility
P.O. Box 6015
Gaithersburg, Md. 20760

Telephone (202) 275-6241