Audit Report

OIG-07-029

Management Letter for the Fiscal Year 2006 Audit of the Department of the Treasury's Financial Statements

February 9, 2007

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

February 9, 2007

MEMORANDUM FOR RICHARD HOLCOMB
ACTING CHIEF FINANCIAL OFFICER

WES FOSTER
ACTING ASSISTANT SECRETARY FOR MANAGEMENT

FROM: Joel A. Grover
Deputy Assistant Inspector General
for Financial Management and Information
Technology Audits

SUBJECT: Management Letter for the Fiscal Year 2006 Audit of the Department of the Treasury's Financial Statements

I am pleased to transmit the attached management letter in connection with the audit of the Department of the Treasury's (Department) fiscal year (FY) 2006 financial statements. Under a contract monitored by the Office of Inspector General, KPMG LLP, an independent certified public accounting firm, performed the audit of the Department's FY 2006 financial statements. The contract required that the audit be performed in accordance with generally accepted government auditing standards, Office of Management and Budget Bulletin No. 06-03, *Audit Requirements for Federal Financial Statements*, and the *GAO/PCIE Financial Audit Manual*.

As part of its audit, KPMG LLP issued and is responsible for the accompanying management letter that discusses certain matters involving internal control over financial reporting and its operation that were identified during the audit which were not required to be included in the audit report.

In connection with the contract, we reviewed KPMG LLP's letter and related documentation and inquired of its representatives. Our review disclosed no instances where KPMG LLP did not comply, in all material respects, with generally accepted government auditing standards.

Should you have any questions, please contact me at (202) 927-5400, or a member of your staff may contact Mike Fitzgerald, Director, Financial Audits at (202) 927-5789.

Attachment

cc: Harold Damelin
Inspector General

Marla A. Freedman
Assistant Inspector General For Audit

DEPARTMENT OF THE TREASURY
FISCAL YEAR 2006

Management Letter Report

November 13, 2006

DEPARTMENT OF THE TREASURY

Fiscal Year 2006
Management Letter Report

Table of Contents

KPMG LLP
2001 M Street, NW
Washington, DC 20036

Inspector General
U.S. Department of the Treasury
Washington D.C.

November 13, 2006

We have audited the consolidated financial statements of the U.S. Department of the Treasury (Department) for the year ended September 30, 2006, and we have issued our report thereon dated November 13, 2006. Our report indicated that we did not audit the amounts included in the consolidated financial statements related to the Internal Revenue Service (IRS), a component entity of the Department. The financial statements of the IRS were audited by another auditor whose report has been provided to us.

In planning and performing our audit of the consolidated financial statements of the Department, we considered the Department's internal control as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

During our fiscal year (FY) 2006 audit of the Department's consolidated financial statements, we and the other auditor noted certain matters involving internal control and other operational matters that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants (AICPA). Reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Department's ability to record, process, summarize, and report financial data consistent with the assertions of management in the consolidated financial statements. Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud, in amounts that would be material in relation to the consolidated financial statements being audited, may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal control, misstatements, due to error or fraud, may nevertheless occur and not be detected.

Our consideration of internal control would not necessarily disclose all matters in internal control that might be reportable conditions. In our *Independent Auditors' Report* dated November 13, 2006, we reported the following matters involving internal control and its operation that we and the other auditor considered to be reportable conditions:

- Financial Management Practices at the IRS (Repeat Condition);
- Electronic Data Processing (EDP) Controls and Information Security Programs Over Financial Systems (Repeat Condition); and
- Controls Over Transactions and Balances Related to the International Assistance Programs.

The reportable condition related to the financial management practices at the IRS noted above is considered to be a material weakness. Detailed findings and recommendations to address the above reportable conditions are not repeated within this document.

Our audit procedures were designed primarily to enable us to form an opinion, based on our audit and the report of the other auditor, on the Department's consolidated financial statements and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Department's organization gained during our work to make comments and suggestions that we hope are useful.

Although not considered reportable conditions, we noted certain matters involving internal control and other operational matters that are presented in the attachment for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of the Department management, are intended to improve the Department's internal control or result in other operating efficiencies. The matters presented in this letter do not include any internal control or operational matters that may have been presented to the management of the Department's operating bureaus that were separately audited by other auditors.

We reviewed all eleven of the prior year management letter comments and determined the status of corrective actions for each. Of the eleven findings:

- Five were corrected;
- One was partially corrected; and
- Five were not corrected.

Exhibit 1 provides the status of the eleven recommendations included in our management letter arising from the FY 05 audit. We have not considered the Department's internal control since the date of our report.

We appreciate the courteous and professional assistance that Department personnel extended to us during our audit. We would be pleased to discuss these comments and recommendations with you at any time.

The Department's written response to our comments and recommendations has not been subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of the management of the Department, Department's Office of Inspector General (OIG), Office of Management and Budget, Government Accountability Office, and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 13, 2006

FISCAL YEAR 2006 RECOMMENDATIONS

06-01: Succession Planning (Repeat Comment)

In our fiscal year (FY) 2005 audit, we reported that several key personnel having significant institutional knowledge of the Department's accounting and reporting processes within various Departmental offices were at or near retirement eligibility status. Furthermore, we noted no policies or procedures related to succession planning, or staff being trained to succeed these individuals. In FY 06, we noted that some improvements had been made, but significant succession planning activities still remained to be conducted to prevent serious loss of operational and institutional knowledge in the event of unexpected absences or retirement by key officials. Details related to some of the Departmental offices we observed as needing immediate succession planning actions follow.

The Office of Accounting and Internal Control (AIC) is responsible for Treasury-wide financial accounting and reporting matters, such as preparation of the consolidated financial statements and notes for the Department, and provides financial policy guidance to the bureaus and offices of the Department. AIC deals directly in broad matters of domestic and international finance, financial markets, Federal, State, and local finance (including the Federal debt), Federal Government credit policies, and lending and privatization. AIC has experienced senior staff critical to carrying out its financial management mission. These individuals, whom we customarily deal with during the consolidated audit, have significant institutional knowledge and will soon be eligible for retirement.

During FY 06, we noted that within AIC, two experienced new staff joined during FY 06 (one in the accounting branch, and one in the internal control branch), two contractors had been used to assist with various year-end consolidated financial statement activities, and various standard operating procedures had been documented for guidance purposes. Although these activities reflect management's commitment to take corrective action, these activities will not significantly improve AIC's capability to continue with mission-critical activities if a key AIC staff member is unexpectedly unavailable to perform his/her duties. For example, during the FY 06 interim audit work conducted during July and August 2006, significant delays were experienced in receiving requested audit documentation and/or explanations to audit-related questions due to the unexpected absence of one key AIC staff member, and leave taken by another key AIC staff member causing significant interim audit completion delays since these individuals were critical in terms of support for the audit.

The Office of Performance Budgeting (OPB) is responsible for the Department's budget execution and for financial management of the Department's International Assistance program, among other duties. OPB is a small office with employees with budget formulation and execution responsibilities. Two key officials with significant institutional knowledge and skills, whom we customarily deal with to resolve Treasury budgetary-related matters, are also eligible for immediate retirement. We are not aware of and did not observe any staff being trained to perform their duties under the supervision of OPB senior staff.

Further, we are not aware of any plans by the Department to provide additional staff to perform the key duties within AIC and OPB as part of succession planning. Succession planning is a government-wide issue that the Government Accountability Office (GAO) has identified as requiring attention by top government officials. In addition to the lack of trained staff to take over such positions, AIC and OPB still do not have a complete set of standard operating procedures that would help new staff understand how to perform their duties should the need arise.

The Office of Personnel Management (OPM) issues regulations related to personnel management for the Federal government. GAO has issued several reports citing the need for succession planning by the government in order to address workforce challenges. In an April 21, 2005, testimony[1] before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, GAO stated:

> A key piece of an agency's strategic human capital plan should also acknowledge the demographic trends that the agency faces with its workforce, especially pending retirements, and include succession strategies and training and development programs to ensure that it will have the knowledge, skills, and abilities it needs to meet its mission…
>
> Training and developing new and current staff to fill new roles and work in different ways will transform how agencies do business and engage employees in further innovation and improvements.

AIC and OPB have not been able to hire the staff necessary, nor have they been able to train other Treasury staff to assume their responsibilities, due in part to budget constraints. This is the second year that succession planning has been identified as a recommendation. In the event of the retirement or sudden prolonged absence of one or more of these individuals, Treasury would face a serious loss of operational and institutional knowledge absent any adequate, formalized succession plan, resulting in serious financial management deficiencies.

In conclusion, we continue to have significant concerns that the amount of resources (training, tools, and staff) available to implement successful succession planning is lacking. Department support for succession planning and actions to prepare for the future are needed now, given the long lead times needed to ensure the knowledge and skills of key staff are transferred effectively. We acknowledge that at a time of budget constraints and deadlines that Departmental offices must meet, it is difficult to request additional staff or to train other staff to assume additional responsibilities. However, the day-to-day constraints should not be allowed to deter the Department from the advance planning and preparation needed to ensure that its offices will be able to perform their responsibilities effectively in the absence of key senior staff members. Any further delays in

[1] U.S. Government Accountability Office, *Human Capital: Agencies Need Leadership and the Supporting Infrastructure to Take Advantage of New Flexibilities*, GAO-05-616T, April 21, 2005.

this process will impact the Department's future ability to manage financial accounting and reporting activities.

06-01 Recommendations

We recommend that the Acting Assistant Secretary for Management (ASM), Acting Chief Financial Officer (CFO), and Deputy Assistant Secretary for Human Resources and Chief Human Capital Officer, with input from the Directors of AIC and OPB, as well as other offices, as appropriate:

1. Consider what actions can be taken now, without additional staff, to ensure that if a key staff member is unexpectedly unavailable to perform his/her duties, that the offices' mission will be met with minimal disruption, and document these as necessary.

2. Clearly define the roles and responsibilities, organizational structure of AIC and OPB, and critical success factors that are necessary to manage the financial reporting activities needed to support the Department-wide financial management practices.

3. Perform a human capital needs assessment, with particular focus on AIC and OPB management skills needed to perform the daily operations of AIC and OPB. The assessment should be conducted either internally or by an independent specialist, and should identify the additional managerial skill sets, e.g., financial accounting background, knowledge, and expertise, required to strengthen the financial accounting and reporting infrastructure, and, once strengthened, to effectively manage the processes necessary to be conducted throughout the year.

4. Once the human capital needs are assessed (per recommendation 3 above), hire staff, or consider transferring suitable staff from other offices within Treasury to meet these immediate needs.

Management Response

The Deputy CFO will work with the Office of Human Resources to address a long term solution. The budget constraints for fiscal years 2007 and 2008, and probably future years, will significantly limit the resources available for additional staffing in a number of critical functions. To address the immediate needs of training and developing current staff, the Department is placing top priority on documenting standard operating procedures and preparing an information handbook for critical functions. We will define specific roles and responsibilities and assign a backup for each critical function. In addition, we will implement cross-training among current staff for these critical functions. We will also explore using detailees from other offices to provide some back-up expertise.

Additionally, during FY 2006 we performed an assessment of existing staff core competencies and tailored each staff's Individual Development Plans to address any areas needing improvement. We developed comprehensive listings of core competencies for each job series within DCFO, utilizing core competency materials from the Department of Defense, the Joint Financial Management Improvement Program, the Office of Personnel Management, and our own internal knowledge of required competencies. Each employee rated his or her knowledge of each competency, and their supervisors independently performed the same rating. Employees and supervisors then met to identify and discuss any differences in ratings and determine competencies that the employee needs to enhance. Employees and their supervisors then developed Individual Development Plans tailored to specifically address the targeted core competencies, increase special competencies, and provide for overall professional development. Training to address targeted core competencies will receive first priority in the DCFO's training budget.

06-02: Financial Reporting Standards for Treasury's Component Entities (Repeat Comment)

The Department's consolidated financial statements are prepared in conformity with accounting principles prescribed by the Federal Accounting Standards Advisory Board (FASAB), the accounting standards-setting body for the Federal Government, as recognized by the AICPA in October 1999. However, certain Department component entities prepare their financial statements in accordance with accounting standards prescribed by the Financial Accounting Standards Board (FASB), the private sector standards-setting body, since the FASAB has allowed entities that issued financial statements prior to October 1999 using FASB accounting to do so. These entities include the Bureau of Engraving and Printing (BEP), the Office of Thrift Supervision (OTS), the Exchange Stabilization Fund (ESF), the Federal Financing Bank (FFB), and the Community Development Financial Institutions Fund (CDFI).

The use of a combination of generally accepted accounting principles (GAAP) by the Department and its component entities complicates the preparation of the Department's consolidated financial statements since additional information required for Federal GAAP reporting must be developed, mapped and submitted to the Department's data warehouse by component entities, and reviewed for compliance with Federal GAAP and overall reasonableness by Department accounting management.

Private sector GAAP does not contemplate budgetary reporting and therefore components using this basis of accounting do not prepare Statements of Budgetary Resources (SBR) or Financing, although these statements are an integral part of the Department's consolidated financial statements, and must be prepared regardless of whether the component receives appropriations from the U.S. Government or not. Moreover, information reported in the Department's SBR must be reconciled to enacted amounts in the President's Budget and disclosed in the notes to the Department's consolidated financial statements.

Additionally, private sector GAAP does not provide sufficient information regarding the costs of programs and activities. The Statement of Net Cost required by Federal GAAP requires that costs and offsetting earned revenues be presented by responsibility segments, with net costs identified for each of the segments, in order to provide more meaningful information to evaluate the operating results of major activities.

Further, inconsistencies exist in how certain costs are reported by entities using private sector GAAP. For example, Federal GAAP requires that non-reimbursed costs paid by the Office of Personnel Management for retirement plans be recognized by the receiving entity as an imputed cost in order to report the full cost of operations. Since private sector GAAP does not provide guidance for the reporting of such imputed costs, these costs are being reported inconsistently, or not at all, by the Department's component entities.

This matter has been reported since FY 04, and has not been resolved to date. Some progress has been made in that two components have converted from commercial to Federal GAAP reporting, and the Department has requested the Financial Accounting Standards Advisory Board (FASAB) to address this situation. The continued use of private sector GAAP by certain Department component entities decreases the usefulness of information reported by these entities for users of Federal financial statements. In order to strengthen and standardize financial accounting and reporting throughout the Department, all component entities should be required to prepare their financial statements in accordance with Federal GAAP, unless statutorily required to report on a different basis of accounting.

06-02 Recommendations

We recommend that the Department research and determine whether component reporting entities reporting on a basis other than Federal GAAP are required to do so by statute. We further recommend that the Department continue to work with the affected Treasury bureaus to achieve conformance in FY 07, so that all such reporting entities within the Department prepare their financial statements in accordance with Federal GAAP, unless statutorily required to report in accordance with a different basis of accounting.

Management Response

The Department requires that all bureaus/reporting entities comply with the United States Standard General Ledger (USSGL), which is used for Federal sector GAAP. The USSGL balances transmitted by the bureaus to the Department's centralized database are appropriately mapped to reflect transactions on a Federal GAAP basis in the Department's consolidated financial statements. No errors resulting from conversion from private sector GAAP to Federal GAAP were noted in the Department's FY 2006 and FY 2005 consolidated financial statements.

In April 2004, the OIG requested that FASAB consider requiring Federal GAAP for the general purpose financial statements of Federal entities, unless there is a statutory or regulatory requirement to report on a different basis. FASAB has included this issue as one of the four potential projects identified in the *Invitation to Comment – Technical Agenda Options* document dated July 22, 2005. Treasury and the OIG provided comments to FASAB, and ranked the Appropriate Source for GAAP project as the second highest priority project next to the Federal Entity project.

In discussing this matter with component entities, one of the problems that surfaced was their belief that the audiences for their financial statements are used to commercial-type financial statements and would not understand statements prepared following FASAB/OMB standards. The question of the usefulness of the component level statements needs to be addressed and resolved.

Treasury will work with the FASAB and the Office of Inspector General in addressing this issue, and will continue to work with the affected bureaus in FY 2007 to achieve greater conformance.

06-03: The Exchange Stabilization Fund's Budgetary Accounting Methodology (Repeat Comment)

The Exchange Stabilization Fund (ESF or Fund) maintains a transaction-based accounting system for the federal proprietary Standard General Ledger (SGL) accounts, but does not have a transaction-based budgetary accounting system. Some of the ESF budgetary data reported in TIER, the Department's repository accounting system is misclassified or inaccurate, but has been left in TIER to force a fit with budgetary accounting definitions. For example, undelivered orders, SGL account 4801, has been reported in ESF's Trial Balance in TIER as $14.1 billion since 2000. However, the ESF does not report any undelivered orders in its SBR nor does it have any transactions that meet the Office of Management and Budget's (OMB) definition of undelivered orders. As a result, ESF's SBR is prepared manually outside of TIER, and outside of CFO Vision, the Department's financial reporting system that converts TIER data into its financial statements.

ESF's reporting to the OMB for purposes of the President's Budget is also inconsistent with ESF's audited financial reporting data and requires reconciliation each year. The President's Budget includes actual obligations and outlays inconsistent with the audited ESF SBR for the reporting year. For example, outlays reported in the President's Budget do not contain valuation gains and losses on foreign currency, whereas the Department prepared SBR for ESF includes such amounts in outlays. As a result, the Department's budgetary financial data for ESF submitted to FACTS II for government-wide reporting purposes is inconsistent with its SBR, Statement of Financing, TIER, and with the information provided to OMB for the President's Budget. In addition, the lack of written, approved operating procedures for ESF has resulted in inconsistencies from year to year in the methodology used in the translation of the ESF proprietary accounts to budgetary accounts.

OMB Circular No. A-11, Part IV requires nonappropriated funds, such as the ESF (as well as appropriated funds) to be included in an agency's combined SBR. It also requires the SBR to be based on budget terminology, definitions, and guidance. In addition, OMB Circular No. A-127, Section 7a, requires Federal financial management systems to "… ensure consistent information is collected for similar transactions throughout the agency, …and ensure consistent information is readily available and provided to internal managers at all levels within the organization." Section 7c states further, "Reports produced by the systems that provide financial information, whether used internally or externally, shall provide financial data that can be traced directly to the SGL accounts." In addition, GAO's *Standards for Internal Control in the Federal Government*[2] states:

> Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form."

The Department has complied with OMB and other requirements by adopting unique budgetary applications for ESF data, and in FY 06 requested OMB to review and agree with the Department's budgetary reporting adaptations that require major reconciliations with the President's Budget, with TIER, and with FMS FACTS II requirements for the Fund. OMB and FMS provided a solution in FY 06 to resolve the requirement to report FBWT to meet FACTS II edits but has not yet reviewed and agreed to the Department's budgetary reporting adaptations. No approved model of budgetary transactions exists for ESF that would ensure that consistent budgetary and proprietary data is readily available that can be traced directly to the SGL accounts.

In response to prior year recommendations to request a waiver from OMB from the requirement to provide Statements of Budgetary Resources and Financing for ESF, AIC prepared a draft waiver request in 2005 which was submitted to OMB and the Financial Management Service (FMS). No waivers have been granted as yet, and the AIC is still in the process of communicating with OMB and FMS on this matter.

06-03 Recommendations

We recommend that the Acting CFO, with input from the Director of AIC, as appropriate:

1. Prepare written operating procedures with accompanying rationale as to why the proprietary accounts chosen approximate budgetary definitions.

2. Request approval from OMB for the definitions the Department uses to translate ESF proprietary accounts to budgetary line items to prepare Statements of Budgetary Resources and Financing, recognizing that standard federal budgetary definitions do not apply to the ESF's investment portfolio fund.

3. Explore with OMB alternative ways of providing meaningful, accurate, and consistent data on ESF in the President's Budget and how the information should be reported in the government-wide financial statements.

---

[2] U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1, November, 1999.

Management Response

The Department agrees with the auditor's recommendations and will continue to work with OMB to obtain specific guidance on providing more meaningful budgetary and FBWT reporting for ESF. The Department will also prepare written operating procedures fully explaining the rationale supporting those procedures, and update the procedures as necessary based on any reporting improvements agreed to by OMB and the Department.

06-04: Financial Reporting Practices at the Department Level

Financial reporting processes and procedures at the Departmental level need improvement to enable the timely preparation and issuance of the Department's consolidated financial statements and the annual *Performance and Accountability Report* (PAR), and to ensure proper financial management.

AIC is responsible for establishing and maintaining financial policies that guide consolidated financial reporting throughout the Department, implementing internal controls to ensure the overall integrity of financial data, and preparing periodic consolidated financial statements. The Department's Office of Strategic Planning and Performance Management (SPPM) within the Office of Management and Budget, and the Office of Accounting and Internal Control (AIC) within the Office of the Deputy Chief Financial Officer, are jointly responsible for the preparation of the PAR. Under the current financial reporting structure, AIC prepares consolidated financial statements, including footnote and supplementary data, from trial balances and other financial data submitted by the components to AIC through the TIER system. AIC is dependent on the Treasury components for complete, accurate, and timely submission of monthly financial data. SPPM manages the completion of the performance sections of the PAR in conjunction with input from Treasury components. SPPM and AIC work jointly together to produce the complete PAR. Certain quality control procedures are conducted by both AIC and SPPM to ensure that component financial, performance, and other data is accurate and complete for inclusion in the consolidated financial statements/PAR; however, several quality control deficiencies and other issues were noted during the FY 06 audit as follows:

- The Department prepared its first interim consolidated financial statements (to include footnote and supplementary data) in FY 06 based on financial data for the nine months ended June 30. These interim consolidated financial statements were prepared to allow for an early start on interim audit reviews due to significant changes in accounting and reporting requirements occurring in FY 06. However, preliminary reviews of these interim consolidated financial statements revealed errors, inconsistencies, inadequate or incomplete footnote disclosures, and lacked supporting documentation for certain footnote disclosures and required supplementary data. Preparation of interim consolidated financial statements reflected a good start by AIC management to begin an early review of the consolidated financial statements, but reflected inadequate quality control procedures. As a result, unnecessary audit time was spent on reviewing the interim consolidated financial statements as well as on the audit of various June 30 account balances. Consequently, some routine audit test work procedures typically performed on interim consolidated financial statements were delayed until year-end, and extensive time was spent at year end by both AIC officials and the audit team to ensure that the consolidated financial statements conformed to new FY 06 accounting and reporting requirements.

- The following are examples of the significant non-routine accounting and reporting matters that had not been completed or addressed timely by AIC:
  - The Department did not finalize its preparation of the detailed footnote disclosure required under Statement of Federal Financial Accounting Standard (SFFAS) No. 27, *Identifying and Reporting Earmarked Funds,* for FY 06 reporting until late October;

  - After meeting with all responsible parties to discuss the effects on the financial statements and footnotes, the Department accepted accounting and reporting changes resulting in a reclassification of certain cash and cash equivalents account balances to investments that had been approved by OMB as part of the ongoing effort to address unique ESF reporting issues. However, a subsequent review by the audit team of the approved accounting and reporting changes, and upon agreement with responsible parties, led to the conclusion that the reclassification should in fact not have been made, mainly because the reclassification did not meet the criteria for change from cash and cash equivalents to that of an investment; and

  - Various accounting and reporting requirements stipulated by OMB Circular A-136, Financial Reporting Requirements, applicable to FY 06 had not been addressed and included until the final draft of the year-end consolidated financial statements. For example, changes to footnote disclosure requirements related to the Department's Reconciliation to the President's Budget to include a reconciliation of Obligations Incurred had not been addressed until it was identified as a requirement during the audit.

- Adequate reviews were not performed on documentation provided to support audit requests. For example, the initial documentation provided to support the Department's Reconciliation to the President's Budget (PB) did not fully support the reconciling amounts reported in the PB reconciliation even though the documentation had been reviewed by AIC officials prior to submission to auditors. Although differences identified were fully explained and supported, the initial supporting documentation provided was not comprehensive enough to eliminate the level of discussions needed to understand the Department's unique budget transactions and how they contribute to the PB reconciliation.

- Year end variance analysis explanations provided in some instances were vague and were not properly reviewed and/or followed up. Consequently, significant time was spent by the audit team in discussions with component audit teams as well as component management to clearly establish the rationale for the variances identified as necessary. Although the Department requires components to provide variance explanations on a quarterly basis, the explanations provided at year end are not adequately reviewed or explanations followed up in a timely manner.

- Procedures followed by responsible AIC officials in the accounting and reporting of various unique transactions, such as the reporting of the U.S. Mint's Seigniorage in the Department's consolidated financial statements, were not fully documented.

- The year-end consolidated financial statements as well as certain PAR sections reflected a lack of adequate review by responsible officials within AIC and SPPM prior to submission to the auditors. Further, comments provided by the auditor and OIG on the initial consolidated financial statements and draft PAR were not reviewed by a responsible official within AIC or SPPM prior to submission of the revised consolidated financial statements and drafts of the FY 06 PAR for audit review, causing the same errors to be identified repeatedly. In addition, later versions of the FY 06 PAR continued to contain various errors that had previously been corrected due to version control problems.

The consolidated financial statements issues identified above occurred mainly due to the fact that existing AIC senior staff had excessive work-loads. Therefore, insufficient time was available to be devoted to supervisory reviews and other financial management activities. This situation resulted in substantial reliance being placed on the annual audit process to identify errors and omissions in the consolidated financial statements and PAR.

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires that agencies establish internal controls according to standards prescribed by the Comptroller General and specified in the GAO's *Standards for Internal Control in the Federal Government (Standards).* The GAO defines "internal control" as an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The GAO *Standards* identify the control environment as one of the five key elements of control, which emphasizes the importance of control conscientiousness in management's operating philosophy and commitment to internal control. These standards cover controls such as human capital practices, supervisory reviews, and segregation of duties, policies, procedures, and monitoring.

06-04 Recommendations

We recommend that the Acting CFO and Acting ASM, with input from the Directors of AIC, SPPM and OPB, as appropriate:

1. Recruit experienced accounting staff necessary to assist in the performance of day-to-day activities of AIC (see finding 06-01, *Succession Planning,* for additional recommendations).

2. Establish new or improve existing policies and procedures to ensure that:

   i. Interim consolidated financial statements are prepared to include all disclosures, including the adoption of new accounting standards and restatements (if any) of prior year consolidated financial statements, and are addressed early each fiscal year, no later than the third quarter, to give management and the auditors adequate time to review changes before year-end;

ii. Documentation exists to support all new and/or unique accounting and reporting requirements as well as non-routine or complex accounting and reporting matters. This documentation should include a review of the documentation by responsible officials within AIC. For example, any new financial statement footnote disclosures to be developed should include a policy memo, financial statement footnote disclosure format as well as evidence of review by responsible officials within AIC of both the policy as well as the format to be followed.

iii. Adequate reviews are conducted by senior AIC officials on all audit-requested documentation to ensure that the documents and information being provided are accurate and complete.

iv. Quality control reviews are performed on interim and consolidated financial statements as well as the respective sections of the PAR by responsible officials prior to submission to auditors to ensure that all errors and inconsistencies are corrected prior to submission to the auditors.

Management Response

As mentioned in our response to finding 06-01, succession planning, budget constraints for fiscal years 2007 and 2008 will likely prohibit the opportunity for recruiting additional experienced accounting staff. However, the Department will take actions to develop policies and procedures to ensure full disclosure in interim financial statements. Internal guidance will be developed to ensure new reporting requirements and audit-requested documentation will receive proper management review prior to being provided to the auditors, and likewise to ensure that all requested documentation is provided in accordance with agreed-upon schedules.

During FY 2007, the Department will update its papers documenting unique accounting and reporting requirements and unusual or complex accounting/reporting matters. We will also expand our formal review procedures to ensure that all components of the PAR are reviewed by responsible officials prior to submission to the auditors.

06-05: OMB Circular A-123, Management's Responsibility for Internal Control

OMB Circular No. A-123 Revised, *Management Accountability and Control* (A-123), issued December 2004, and effective for implementation in FY 06, requires agencies to (1) develop and implement management controls; (2) assess the adequacy of management controls; (3) identify needed improvements; (4) take corresponding corrective actions; and (5) report annually on management controls (commonly known as management's *Federal Manager's Financial Integrity Act (FMFIA)* report). A-123 provides the guidance for agencies to implement the FMFIA and applies to all Federal agencies. Appendix A, *Internal Control over Financial Reporting*

Implementation Guide from A-123 requires management's evaluation of the internal controls over financial reporting (ICOFR), and separate assurance statements on the operating effectiveness of the ICOFR by 24 CFO Act agencies. Agencies are to use the *Standards for Internal Control in the Federal Government* (the Green Book) to evaluate the three objectives of internal control which are to ensure (1) the effectiveness and efficiency of operations; (2) reliability of financial reporting; (3) compliance with applicable laws and regulations.

During FY 06, the Department significantly enhanced its FMFIA assessment policies and procedures to be conducted by its components. The AIC, in response to A-123 Appendix A, prepared the Department's Methodology and Implementation Plan, which provided a clear, organized implementation strategy with well-defined documentation processes and requirements for Treasury components. Components used this guidance to assess the adequacy of controls over selected financial reporting processes identified as key by the Department.
While we noted that the Department had undertaken the steps needed to meet the minimum threshold for general compliance with A-123 requirements, further improvements are needed in various areas as identified during our limited review of the A-123 work undertaken by the Department and its components.

Implementation Procedures

- Components are responsible for conducting the A-123 related work and to report on management controls once AIC has approved the transaction testing plans for the respective component. There is limited involvement by AIC staff once testing plans are approved, other than the review conducted on the interim and final FMFIA and A-123 assurance statements provided by the respective components in support of the overall Departmental level assurance. Consequently, there is no centralized review of any of the work done by components to assess whether the testing plans and other A-123 Methodology and Implementation Plan requirements have been followed.

  A centralized review will help in identifying issues early and assist the AIC in evaluating whether A-123 assessments are based on verifiable results.

- Several instances were noted whereby A-123 required steps for the components/offices which we selected for limited review were not conducted as required, or were omitted in their entirety due to various reasons, or the required steps were conducted, but were not appropriately documented by the respective components/offices:

  - Three of six components/offices did not develop test plans and related results in accordance with the guidelines provided by the Department's Methodology and Implementation Plan. For example, details of the scope of the test, expected results, and results of testing were not documented in accordance with the required format. Therefore, it was unclear without significant explanation from component entity staff, what the components' processes and results were.

- One of six components/offices did not have its test plans approved in accordance with the guidelines provided by the Department's Methodology and Implementation Plan.

- Four of six components/offices did not conduct tests over the controls to compile, consolidate, assemble, and distribute their financial statements and other financial reports. The Department's Methodology and Implementation Plan requires components to specifically address (1) elimination procedures and controls in place to ensure that financial statement preparation is controlled and footnotes and other supplemental information is complete and accurate, and (2) TIER transmissions to the Department are complete and accurate. Although components have controls in place to compile, consolidate, assemble, and distribute their financial statements and other financial reports, the testing of these controls had not been formally documented as required by the Department's Methodology and Implementation Plan.

- Two of six components/offices provided no evidence of review of the status of corrective actions developed in response to audits that directly affect financial reporting, except for a statement that they conducted the review. According to the Department's Methodology and Implementation Plan, each component is to review the status of corrective actions developed in response to audits that directly affect financial reporting. The review should consider whether corrective actions are on schedule, their degree of impact on the controls over financial reporting, and the impact of corrective actions planned or taken, to the total financial reporting control environment. Bureaus and offices are to document the completion of these actions as part of the total assessment methodology.

- Three of six components/offices provided no evidence of review of testing of compliance with governing regulations. According to the Department's Methodology and Implementation Plan, each component entity is to review their compliance with governing regulations, as necessary. Some components made references to prior year external audit results on compliance with laws and regulations, instead of actually identifying and testing the laws and regulations that apply.

- Five of six components/offices did not test Information Technology (IT)-related controls. We were informed by AIC that review and testing of IT controls were not required to be conducted since Treasury management expected to rely on the procedures already in place by components to evaluate general and application systems and related controls to comply with the *Federal Financial Management Improvement Act of 1996,* and the *Federal Information Security Management Act of 2002.*

The above issues revealed a need for improvement by components in the conduct of A-123 testing and related documentation.

Transactions Testing

- For one of six components/offices tested, the component:

  - Performed testing over summary transactions in the general ledger and did not trace transactions to source documents or systems, which are maintained by other entities or related offices.

  - Did not test material components of expense and balance sheet line items, and also did not test certain material balances even though material transaction activity had occurred during the course of the year. This occurred because the transactions and balances to be tested are determined by AIC at the Departmental level based on pre-set materiality thresholds.

- For three of six components/offices of test work documentation reviewed documentation of the source of the population and the sample selection processes followed were insufficient.

Reporting

- A number of the components/offices did not follow the A-123 assurance assessment format provided by the Department, and there was no follow-up by the AIC to require that the format was followed. As a result, key phrases needed to assert assurance were not included in the assurance statement.

- The Department did not consider certain material weaknesses in internal control over financial reporting as weaknesses affecting the overall assurance level at the Departmental level.

  The Secretary's Letter of Assurance for FY 06 reports that it is only the IRS' revenue accounting system weakness that affected Treasury's overall assurance level for internal controls over financial reporting. Other material weaknesses identified such as reducing overclaims in the Earned Income Tax Credit program, and improving system security controls cited in the FY 06 assurance letter also meet the definition of a weakness in internal control over financial reporting and as such, should also have been included as weaknesses affecting the overall assurance level for internal controls over financial reporting.

FMFIA requires Federal agencies to establish internal accounting and administrative controls to: (1) ensure that obligations and costs comply with applicable law; (2) assets are safeguarded against waste, loss, unauthorized use or misappropriation; and (3) revenues and expenditures are properly recorded and accounted for. Further, the Act directs the head of each agency to evaluate such controls annually and to submit to Congress and the President either a statement that the controls are adequate or a report on any weaknesses in such controls with a schedule for corrective measures. The issuance of A-123 provided further guidance to agency management for evaluation of the internal controls over financial reporting in support of its annual FMFIA assurance statement.

The recurrence of the issues discussed above may ultimately result in A-123 evaluations by components that are not supported by verifiable results since appropriate procedures were not documented as required or not conducted.

06-05 Recommendations

We recommend that the Acting CFO, with input from the Director of AIC, as appropriate:

1. Designate a responsible official within AIC to review the A-123 work being conducted by components to ensure that the Department's A-123 guidance is complied with.

2. Consider the use of a checklist to facilitate review of key requirements when reviewing A-123 documentation provided by components, and specifically include reviews of the areas needing improvement as discussed above.

3. Communicate the deficiencies identified during the FY 06 A-123 testing, as discussed above, to all components, and conduct follow-up to ensure that these deficiencies have been addressed, as necessary, during FY 07 A-123 testing.

4. Develop and implement procedures to require testing of the IT systems and related controls supporting the financial reporting processes, as well as applicable laws and regulations.

5. Revise existing procedures to identify and include control testing of all significant transactions, including those that are either generated by other entities or resident in related offices (for example, transactions processed for Treasury bureaus by the Federal Reserve Banks).

6. Develop an interim assurance letter for purposes of early review for concurrence on conclusions by all responsible officials so as to eliminate any future reporting deficiencies.

Management Response

AIC has a responsible official to review the A-123 work conducted by Treasury's components to ensure that the Department's A-123 guidance is complied with. All test plans submitted by the material components for FY 2006 were reviewed using the required outline prescribed in the A-123 Methodology and Implementation Plan. The level of compliance and final results of testing, which was prescribed to be conducted at the transaction level, was communicated to the AIC in the same manner as the results of the annual assurance statement process for FMFIA and FFMIA (e.g., as a draft and as a final assurance statement).

The AIC simply does not have on-board resources sufficient to review all of the work that was performed in the bureau and offices. The A-123 testing performed in FY 2006 spanned 12 bureaus and offices that utilized approximately 45 in-house resources and 12 contract resources to conduct and document the testing, while the AIC has two resources to review all of their collective efforts. Further, these two AIC resources cannot be 100% dedicated to A-123 due to other demands and expectations placed on the AIC. Thus, primary responsibility must be placed upon the testing bureaus and offices to complete the testing and assessment for A-123, Appendix A, in accordance with the guidance issued. However, we will explore using existing accounting branch staff to assist the internal control staff in reviewing bureau work on a test basis.

During the update to the A-123, Appendix A guidance for FY 2007, more explicit reporting and documentation requirements have been placed upon the bureaus and offices, and specific IT-controls have been identified and added to the Treasury Catalogue of Risks and Controls.

We will review our existing procedures with the goal of identifying significant transactions that are generated or resident in other offices so that we can consider additional testing that may be necessary and identify resources required to perform any additional testing in FY 2008.

We currently receive interim assurance information from the bureaus on the financial reporting aspect of Circular A-123 as of June 30, and receive complete draft assurance statements in early September. We will continue to follow this practice and enhance it by summarizing the proposed A-123 Appendix A reporting for review and discussion well before fiscal year end.

06-06: Intragovernmental Transactions and Activities

The Department conducts business with other Federal agencies resulting in intragovernmental receivables, payables, and the reporting of revenues and expenses from intragovernmental transactions. Federal accounting and reporting regulations require Federal agencies to routinely identify and reconcile intragovernmental balances and transactions with trading partners. These procedures help ensure that intragovernmental balances properly eliminate in the government-wide consolidated financial statements. AIC is responsible for the issuance of policy and procedures, coordinating the reconciliation of intragovernmental transactions at the Department level in conjunction with Treasury components. While the Department conducted the work required on intragovernmental transactions and balances differences with partner agencies in compliance with the requirements of the *Treasury Federal Intragovernmental Transactions Accounting Policies Guide*, dated August 18, 2006 (TFITAPG) to the extent possible, we believe that the Department can further improve the resolution of any remaining unresolved differences by meeting with responsible officials from the partner agency rather than through e-mail communications.

The TFITAPG states that OMB Circular No. A-136, requires Federal CFO Act and non-CFO Act entities identified in the Treasury Financial Manual 2006, Vol. I, Part 2-Chapter 4700, *Agency Reporting Requirements for the Financial Report of the United States Government*, perform quarterly reconciliations of intragovernmental activity/balances and resolve differences as necessary.

Treasury Financial Manual Bulletin No. 2007-03, *Intragovernmental Business Rules*, dated November 15, 2006, and effective for FY 07, provides further guidance to Federal agencies for standardizing the processing and recording of intragovernmental activities, and also provides guidance on resolving intragovernmental disputes and major differences.

Reconciling trading partner activity and balances and resolving unknown or contentious differences at least quarterly is necessary to identify the reasons for any material out-of-balance conditions between Federal entities on a timely basis.

06-06 Recommendation

We recommend that the Acting CFO, with input from the Director of AIC, as appropriate, revise existing resolution procedures both at the Departmental and component levels to require meeting directly with responsible officials from the partner agency for any intragovernmental differences that are considered unknown and/or contentious so that such differences are resolved in a timely fashion. If necessary, OMB officials should be requested to be involved as a mediator.

Management Response

AIC is drafting the Department's intragovernmental transaction procedures to emphasize compliance with FMS Business Rules, using Treasury intragovernmental elimination reports for bureau accounting and monitoring, establishing and updating executive agency intragovernmental transaction points of contact, and resolving intragovernmental transaction differences via periodic meetings with partner agencies. If necessary, we will seek OMB mediation of differences we are unable to resolve with other agencies.

06-07: Performance Measures

Agencies report on their annual performance in their PAR utilizing performance measures. OMB Circular No. A-136 requires Federal agencies to discuss their key performance measures in the Management's Discussion and Analysis (MD&A) section of their PAR.

Treasury issues an annual report titled "Full Report of Treasury's FY 06 Performance Measures by Focus and Strategic Goal" (Report) which is attached as an Appendix to the PAR. The Department's SPPM within the OPB is responsible for the preparation of the Department's annual report on performance measures as well as the monitoring of component-submitted performance information. The components submit performance information to Treasury's Performance Reporting System (PRS) that tracks components' progress in achieving their performance objectives. Specifically, the system primarily tracks progress against current year performance targets and prior year's actual performance levels. Reliability of the performance information in PRS is monitored at the component level where internal performance tracking systems are maintained. Each component has an assigned official that is responsible for: (1) ensuring that the information for their assigned component was entered into the PRS; and (2) that the information that is entered into the system can be validated. In addition, SPPM staff (or the component) ensures that the information submitted relating to the performance measures matches/relates to the original budget submission.

While SPPM's process for monitoring performance measures appears appropriate, certain improvements are needed with respect to the processes reviewed, and the documentation maintained as evidence of the reviews conducted. For example, we were unable to determine whether the quarterly monitoring procedures were conducted as described by SPPM staff as there was no documentation retained to evidence the work that was conducted.

GAO's Standards for Internal Control in the Federal Government requires that management clearly document internal control and all transactions and other significant events, and ensure that the documentation is readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

06-07 Recommendations

We recommend that the Acting ASM, with input from the Directors of SPPM and OPB, as appropriate:

1. Develop procedures to match performance measures reported in the PAR to that in the PRS and inquire into the reasons for any discrepancies, document explanations, and retain supporting documentation as necessary.

2. Select a sample of performance measures from each component, and request appropriate documentation supporting the existence and completeness of these performance measures.

3. Require retention of all documentation used in the monitoring of the performance measures to serve as evidence of review, and for reference purposes, should questions arise at a later date.

Management Response

Although not all measures used in the PAR have to be in the Performance Reporting System, such as enforcement revenue, the Department agrees with the recommendations and will develop appropriate actions to address each recommendation.

06-08: Deferred Maintenance

SFFAS No. 6, *Accounting for Property, Plant and Equipment*, describes deferred maintenance as maintenance (needed to return each major class of asset to its acceptable operating condition) that was not performed when it should have been or was scheduled to be, and which is put off or delayed for a future period. SFFAS No. 14, *Amendments to Deferred Maintenance Reporting,* requires that deferred maintenance information be included as required supplementary information in the consolidated financial statements.

The AIC is responsible for accumulating and reporting deferred maintenance information on a Department-wide basis. However, the deferred maintenance information that was provided to us to support the information reported as *Required Supplementary Information* in the Department's FY 06 consolidated financial statements was inadequate due to the lack of a comprehensive policy at the Department level.

Lack of a process to identify deferred maintenance may allow assets to deteriorate at a rate faster than if they were maintained well and not allow adequate funds to be identified in the budget process for the necessary maintenance or replacement of assets, which will ultimately adversely affect Treasury's ability to accomplish the mission for these assets. In addition, this situation may also cause inadequate or incomplete information to be disclosed in the Department's consolidated financial statements.

06-08 Recommendation

We recommend that the Acting CFO, with input from the Director of AIC, as appropriate, develop and implement policies and procedures for the identification and monitoring of deferred maintenance on a Department-wide basis. This policy and its implementation should be coordinated with Treasury components.

Management Response

The Office of Accounting and Internal Control, coordinating with the Office of Asset Management, will work with the bureaus to develop Departmental policies and procedures for the identification and monitoring of deferred maintenance. These policies and procedures will be implemented during FY 2007 to ensure complete documentation for the required deferred maintenance disclosures.

06-09: Backup Tapes for the TIER System and CFO Vision Production Servers (Repeat Comment)

The Treasury Information Executive Repository (TIER) and the CFO Vision applications, including the supporting information technology infrastructures for both systems, were recently moved to the Qwest Cyber Center in Sterling, VA. Within the Cyber Center, the supporting infrastructure for each of these applications is housed in a four-sided gated off area, known as the Security Extranet Gateway (SEG) cage. This area is physically secure and accessible only by authorized individuals.

The Qwest Cyber Center was noted as having adequate controls in place to ensure the timely and consistent archiving of critical data related to the TIER and CFO Vision applications, including daily and weekly full and incremental backups of data. In order to ensure that backup media is physically and environmentally protected, including maintaining backup media at a location that is geographically separated from the primary site, Qwest has recently entered into contract with the Iron Mountain Corporation, an organization that provides information and record management, to provide long-term offsite storage for backup media for all of their managed systems, including the TIER and CFO Vision application.

On a regular basis, Iron Mountain arrives at Qwest to rotate backup media related to TIER and CFO Vision on and off site. However, we noted onsite data back-up tapes for the TIER and CFO Vision financial systems are not stored in an environmentally secure and stable location within the Qwest Cyber Center prior to being rotated offsite to Iron Mountain. If data back-up tapes are not being stored in an environmentally secure and stable environment during all stages of the rotation cycle, there is a risk that the most current data will not be recovered in the event of a disaster.

The National Institute of Standards and Technology (NIST) Special Publication 800-14, *Generally Accepted Principles and Practices for Security Information Technology*, recommends that back-up tapes should be stored security and that measures should be established to physically and environmentally protect the archives data.

06-09 Recommendation

We recommend that the Acting CFO, with input from the Director of the Office of Financial Systems Integration (FSI) instruct the Qwest Cyber Center to store TIER and CFO Vision data back-up tapes in an environmentally secure and stable environment prior to being rotated offsite for long-term storage with Iron Mountain.

Management Response

A fireproof storage box was purchased and installed at the Qwest Cyber Center in Sterling, VA. Effective December 19, 2006, Qwest began storing backup tapes for TIER and CFO Vision in this storage box, while waiting for pickup by the Iron Mountain Corporation. We think we have effectively addressed this recommendation.

06-10: Continuity of Operations Plan and Disaster Recovery Procedures for TIER and CFO Vision (Repeat Comment)

In FY 05, it was noted that a Continuity of Operations Plan (COOP) and a Disaster Recover Plan (DRP) for the TIER and CFO Vision applications had not been implemented. Specifically, the Department was unable to fund the development of a COOP or DRP for the TIER and CFO Vision applications during the fiscal year due to monetary constrains.

In FY 06, the Department established a Contingency Plan for the IT environment at the Department's Headquarters, including the DO LAN. Additionally, the Department implemented the Assistant Secretary for Management (ASM)/COOP, which provided guidance, requirements, and procedures for the continuance of the Department's essential functions in the event of an emergency. While both the TIER and CFO Vision applications have been identified in this document, it does not identify or specify IT specific recovery requirements or procedures for the infrastructure that support each system.

In addition, TIER and the CFO Vision applications, including their supporting information technology infrastructures, were recently moved to the Qwest Cyber Center in Sterling, VA for offsite management. The Qwest Cyber Center has taken several steps to ensure the physical and environmental security, as well as the continuance of operations, for the systems Qwest has been contracted to manage. However, neither Qwest, nor the Department, have implemented a DRP at the Cyber Center for the TIER and CFO Vision applications.

Should a disaster occur without a documented DRP for TIER and CFO Vision, Treasury's Office of the DCFO's ability to restore operations and continue its business operations related to these systems may be significantly delayed.

NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, states that "Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. NIST Special Publication 800-34 also states that "IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort; however, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions."

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook (Chapter 11) guide* states that "Contingency planning directly supports an organization's goal of continued operations. Organizations practice contingency planning because it makes good business sense. To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event. Generally called contingency planning, this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses. Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization.

OMB Circular No. A-130, Security of Federal Automated Information Systems, Appendix III (A-130) requires that a contingency plan be developed, documented, and tested to assure that users of the system can continue to perform essential functions in the event the information technology support for their application is interrupted. The plan should also be consistent with the agency-wide

DRP. *A-130* further requires that agencies establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users continue to perform essential functions in the event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed.

06-10 Recommendation

We recommend that the Acting CFO, with input from the Director of FSI instruct the Qwest Cyber Center, to develop a DRP for the TIER and CFO Vision financial systems in accordance with the guidance outlined in *NIST Special Publication 800-34*.

Management Response

The OCIO strategic plan was to leverage the hosting services requirements of the Treasury Communication Enterprise (TCE) procurement to obtain both primary and backup hosting site services. On December 21, 2006, the TCE procurement was cancelled.

The cancellation will result in Treasury adopting the General Service Administration NETWORX Contracts which includes hosting. Since GSA is currently scheduled to award these contracts in the third quarter of FY 2007, specific Treasury hosting plans will be framed in the fourth quarter of FY 2007. It is envisioned a strategic COOP/DR plan will be drafted in the third quarter with a budget estimate for the hosting services in fourth quarter.

Until the final resolution and implementation of the GSA NETWORX contract at Treasury, the Department will evaluate interim disaster recovery solutions for the FARS applications, including TIER and CFO Vision.

06-11: Segregation of Duties

TIER was implemented as a result of the OMB's request for high-risk agencies to create a repository for standardized data. TIER is an Oracle database management system and a system of record where individual Treasury components submit monthly financial data and serves as a repository for this information. Once data is received from a component, TIER runs a series of tests against it to ensure that the data is valid. It checks for such things as appropriate SGL account and Budget Object Codes, as well as ensuring that no letters are entered in a data field where numbers are required. Once these validations are complete, the data is sent to the repository area within TIER. In 1995, the application was expanded to include all of Treasury components for the purpose of producing the Department's consolidated financial statements. In March 2002, TIER was web-enabled for faster and easier access by the bureaus.

TIER was developed, and is currently being maintained by Aspex, Inc., a contractor. During fieldwork, it was noted that systems administration duties in the TIER system have not been properly segregated between Treasury employees and the Aspex, Inc. contractors. Specifically, four Aspex, Inc. contractors with application developer responsibilities have also been granted TIER production system administration rights. We noted that, in addition to these four individuals, there are currently three (3) full-time Treasury employees with this level of access. The four contractors were assigned this level of access as a back-up in the event that the three primary administrators are not available.

NIST Special Publication 800-53, *Recommended Controls for Federal Information Systems* states that "The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security.

NIST Special Publication 800-12, *Introduction to Computer Security*, states that segregation of duties is the process by which users' roles and responsibilities are divided so that a single individual cannot subvert a critical process. NIST Special Publication 800-12 also states that users should only be granted access to functions necessary to accomplish their assigned responsibilities, thereby helping to maintain the principle of least privilege.

By allowing multiple individuals to create, modify, or delete TIER accounts, there is an increased risk that these individuals could cause accidental or intentional harm that could threaten the integrity of TIER data.

06-11 Recommendations

We recommend that the Acting CFO, with input from the Director of FSI either:

1. Remove the TIER production system administration rights access from the four (4) application developers and/or reassign the duties to individuals without application development roles; or

2. In the event these roles are not reassigned (as recommended in (1) above), implement a monitoring mechanism to ensure these roles are not used in an inappropriate manner.

Management Response

Effective July 15, 2006, TIER developers no longer have TIER production systems administration rights. This responsibility resides with three Treasury employees in the Office of Financial Systems

Integration. To provide contingency back-up, TIER systems administration rights were granted to an InfoPro contractor, who does not have access to the TIER application for development/maintenance purposes.

In addition, the Department will develop a control report to record any administrative changes to TIER for subsequent review by Treasury management.

As a result of the above, we have determined the requested correction actions have already been completed.

06-12: User Account Passwords

Logical access controls implemented within the TIER application were reviewed to determine compliance with Treasury-specific IT policy and Federal government guidance. As a result of our review we noted that Aspex, Inc., the Application Systems Support Contractors used by DCFO to implement and manage the TIER application, was not made aware of access controls requirements in the Treasury Information Technology Security Program TD P 85-01 Volume 1 policies (TD P 85-01) when developing the application. Specifically, we noted two access controls were not properly implemented in the TIER application based on the guidance outlined in TD P 85-01 Volume 1 as follows.

- Currently, TIER user account passwords are set to expire after 180 days. Should a user account password remain unchanged for a long period of time, there is increased risk that the user account could become compromised by an individual with malicious intent. Depending on the level of access assigned to a compromised account, this issue could potentially lead to alterations in the functionality of the application or the data contained within.

- A user session timeout has not been implemented in TIER. Allowing user sessions in TIER to remain active for lengthy periods of time creates the risk of malicious individuals hijacking user sessions and potentially altering the integrity of the data within the system.

During the course of the audit, this issue was brought to the attention of Treasury DCFO management. Corrective actions were undertaken by establishing a 90-day password expiration on all TIER user accounts. Evidence was provided to us to verify the implementation of this new configuration.

TD P 85-01 Volume 1 Policy Part 1, *Sensitive Systems* states that “Bureaus shall ensure that passwords are changed at least every 90 days.”

NIST Special Publication 800-53, *Recommended Controls for Federal Information Systems* states that “For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations."

TD P 85-01 Volume 1 Policy Part 1, *Sensitive Systems* states that "Bureaus shall implement and enforce threshold limits for the amount of time a session is inactive before the session timeout feature is invoked."

NIST Special Publication 800-53 also states that "The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system."

06-12 Recommendation

We recommend that the Acting CFO, with input from the Director of FSI require the addition of a functionality to the TIER application that will automatically invoke a session timeout after an extended period of time as required by *TD P 85-01*.

Management Response

As part of an upcoming system upgrade to TIER, the application will be modified to invoke a timeout after the system is idled for an extended period of time. These requirements will be consistent with Federal and Treasury policies and procedures.

06-13: User Accounts

The *Departmental Offices Local Area Network Operational and Technical Controls* manual is not being completely adhered to when initiating the removal of a user account from the Departmental Offices (DO) Local Area Network (LAN) following an employee termination. Specifically, of the twenty (20) terminated full-time employees and contractors selected for review, the user account belonging to one (1) individual, who was terminated on July 21, 2006, was still active on the DO-LAN as of September 1, 2006. When the employee left Treasury, an entry was initiated in the Employee Entry Exit (EEE) system; however, this entry was not saved and later followed up on when the individual left the premises. As a result, the user account was never disabled or deleted.

During the course of the audit, this issue was brought to the attention of FSI management. Corrective actions were undertaken by disabling this user account on the DO-LAN. Information was provided to us to verify the disabling of this account.

The Departmental Offices' *Local Area Network Operational and Technical Controls Manual* outlines procedures to be followed by the Help desk for the disabling of all user accounts on DO owned system, including the DO LAN. These procedures state that "terminating a user account is an automated process via the Employee, Entrance and Exit (Triple EEE) program. The program automatically generates a ticket to disable any pending invalid user accounts."

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* states that "From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed and so forth."

A-130 requires Federal agencies to incorporate personnel-related security controls to ensure the screening of individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. This is extremely important when employees leave an organization, as they may be in a position to cause severe harm to the organization's systems after they leave if their system access is not promptly terminated. The Circular requires that agencies ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information (least privilege).

By not having an efficient mechanism by which the DO-LAN manager is made aware of terminated employees, the Department's data processing environment could be significantly impacted by a terminated employee that maintains unauthorized access.

Furthermore, should a separated employee's DO-LAN user account not be timely removed, the separated employee or another person with malicious intent and knowledge of this active user account could use this account to alter the integrity of the system.

06-13 Recommendation

We recommend that the Acting CFO, with input from the Director of FSI continue to ensure that procedures established for the timely removal of user accounts belonging to former employees and contractors are followed.

Management Response

Strengthening the management of system user accounts is being resolved by additional near term and long term business process improvements. Tools to assist in this function being developed include:

1. *Electronic Notification:* The Departmental Office (DO) Employee Entry Exit (EEE) system has a feature which provides email notification to key DO system administrators that LAN Access Accounts for just (or in-process) separated Federal or contractor personnel are to be de-activated. Such an email notification will be provided to the DCFO office.

2. *End User Manager Re-certification:* On at least an annual basis, the DCFO system administrator will complete a client account recertification process. The process entails forwarding to client organization managers a list of those client personnel needing system access privileges. The manager shall validate that organizations current personnel still needing access, and annotating those who through role change or reassignment no longer merit access privileges. This procedure would be performed outside the realm of EEE.

3. *Aged Open Personnel Separations:* The EEE system will have an exception notification feature that notifies DO Office administrators or action initiators that an employee separation created in EEE is not recorded as closed in EEE and follow-up action is needed. The notification may be through a report and/or email notification.

EXHIBIT 1

DEPARTMENT OF THE TREASURY

Fiscal Year 2006
Management Letter Report
Status of Prior Year Management Letter Comments

Prior Year Recommendations		**Current Year Status**
05-01	Succession Planning Must be Implemented Immediately	This comment has not been corrected and is repeated in the current year as comment # 06-01.
05-02	Financial Reporting Standards for Department Component Entities Should be Consistent	This comment has not been corrected and is repeated in the current year as comment # 06-02.
05-03	The Exchange Stabilization Fund's Budgetary Accounting Methodology Should be Clarified	This comment has not been corrected and is repeated in the current year as comment # 06-03.
05-04	Annual Reconciliation Procedures to the President's Budget Should be Improved	This comment has been partially corrected and is repeated in the current year as part of comment # 06-04.
05-05	A Formal Process Is Needed to Monitor the Use of Sensitive System Software Utilities	This comment has been resolved and closed.
05-06	Access Controls over the TIER System Should be Strengthened	This comment has been resolved and closed.
05-07	Configuration Management Processes Over CFO Vision Need Improvement	This comment has been resolved and closed.
05-08	CFO Vision Access Controls Should be Strengthened	This comment has been resolved and closed.
05-09	Financial Analysis and Reporting System (FARS) Access Controls Should be Strengthened	This comment has been resolved and closed.
05-10	Back-up Tapes for the TIER System and CFO Vision Production Servers Should be Protected	This comment has not been corrected and is repeated in the current year as comment # 06-09.
05-11	Formal Continuity of Operations Plan and Disaster Recovery Procedures for TIER and CFO Vision Should be Established	This comment has not been corrected and is repeated in the current year as comment # 06-10.