Audit Report

OIG-06-021

Management Letter For Fiscal Year 2005 Audit of the Department of the Treasury's Financial Statements

January 3, 2006

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

JAN 3 2006

MEMORANDUM FOR SANDRA L. PACK
ASSISTANT SECRETARY FOR MANAGEMENT AND CHIEF FINANCIAL OFFICER

FROM: William H. Pugh, *William H. Pugh*
Deputy Assistant Inspector General
for Financial Management and Information Technology Audits

SUBJECT: Management Letter for Fiscal Year 2005 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) 2005 financial statements. We contracted with the independent certified public accounting firm KPMG LLP to audit the Department's financial statements for FY 2005. The contract required that the audit be performed in accordance with generally accepted government auditing standards; Office of Management and Budget Bulletin No. 01-02, *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 operations 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 2005

Management Letter Report

November 11, 2005

DEPARTMENT OF THE TREASURY
FISCAL YEAR 2005

Management Letter Report

Table of Contents

KPMG LLP
2001 M Street, NW
Washington, DC 20036

Inspector General
U.S. Department of the Treasury:

We have audited the consolidated financial statements of the U.S. Department of the Treasury (Department) as of and for the year ended September 30, 2005, and we have issued our report thereon dated November 11, 2005. 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, or the gold and silver reserves of the U.S. Government. In planning and performing our audit of the consolidated financial statements, we considered the Department's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing an opinion on the consolidated financial statements, and not to provide assurance on internal control over financial reporting.

During our FY 2005 audit of the Department's consolidated financial statements, we and the other auditors noted certain matters involving internal control over financial reporting and its operations that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants. 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. Our consideration of internal control over financial reporting would not necessarily disclose all matters in internal control that might be reportable conditions. In our *Independent Auditors' Report* dated November 11, 2005, we reported the following matters involving internal control over financial reporting and its operation that we and the other auditors considered to be reportable conditions:

- Financial Management and Reporting at the IRS Needs Improvement (Repeat Condition)
- Electronic Data Processing (EDP) Controls and Information Security Programs Over Financial Systems Should Be Strengthened (Repeat Condition).

The reportable condition related to the financial management and reporting 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 reports of the other auditors, on the Department's consolidated financial statements and, therefore, may not bring to light all weaknesses in policies or procedures that exist. However, we take this opportunity to share our knowledge of the Department, gained during our work, to make comments and suggestions that we hope can be useful to you.

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 seven of the prior year financial statement audit findings and determined the status of each corrective action. Of the seven findings:

- Five were corrected; and
- Two were not corrected.

Exhibit 1 provides the status of the seven recommendations included in our management letter arising from the FY 2004 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.

This report is intended solely for the information and use of the U.S. Department of the Treasury and its Office of Inspector General and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 11, 2005

DEPARTMENT OF THE TREASURY
FISCAL YEAR 2005

Management Letter Report

November 11, 2005

I. FISCAL YEAR 2005 RECOMMENDATIONS

05-01: Succession Planning Must be Implemented Immediately.

During the course of our audit, we noted that several key personnel having significant institutional knowledge of the Department's accounting and reporting processes within various Departmental Offices are 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. 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 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, (including the Federal debt), Federal Government credit policies, and lending and privatization. AIC's experienced senior staff are critical to carrying out its financial management mission. These individuals, with whom we customarily deal with during the audit, have significant institutional knowledge and will soon be eligible for retirement.

The Office of Performance Budgeting (OPB) is responsible for the Department's budget execution, and 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 the duties under the supervision of either AIC or OPB senior staff, nor are we aware of any plans by the Department to provide additional staff to perform the duties 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 do not have standard operating procedures that would help new staff understand how to perform their duties should the need arise.

In conclusion, we have significant concerns that the amount of resources (training, tools, 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.

(Continued)

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 its 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 additional staff, nor have they been able to train other Treasury staff to assume their responsibilities, due in part to budget constraints. Treasury officials stated that they have requested and received approval for additional positions but were unable to fill them due to a hiring freeze.

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.

Recommendations

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

1. Immediately begin the strategic human capital planning necessary to ensure that the offices will have the knowledge, skills, and abilities it needs to meet its mission.
2. As part of its planning effort, 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.

Management Response

The Department will continue its efforts in filling current vacancies and bringing staffing to a reasonable level to accomplish its critical missions. However, budget constraints for fiscal years 2006 and 2007 may significantly limit the resources available for additional staffing in a number of critical functions. The Department will consider alternatives to prepare and implement succession planning such as: identifying and documenting standard operating procedures for critical functions; providing opportunities in cross-training current staff in a number of critical functions; and considering details from the bureaus for rotational assignments.

---

[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.

(Continued)

***05-02: Financial Reporting Standards for Department Component Entities Should be Consistent.* (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 American Institute of Certified Public Accountants 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. In addition, the separately issued financial statements of the component entities using FASB accounting principles do not adequately portray the importance of the budgetary process as it relates to federal entities. That is the concept of "presents fairly" for those entities is incomplete as it relates to the significant budgetary disclosures required by Federal GAAP.

Private sector GAAP does not contemplate budgetary reporting and, therefore, components using this basis of accounting do not prepare statements of budgetary resources or statements of 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 Statement of Budgetary Resources (SBR) must be reconciled to enacted amounts in the President's Budget and disclosed in the notes to the Department's consolidated financial statements. Considerable additional preparation and audit steps are required to develop and report this data at the Department level for components using private sector GAAP.

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.

Finally, private sector GAAP does not require management's discussion and analysis (MD&A) of the information presented in the annual report. The MD&A is one of the most valuable aspects of an annual financial report, since it provides management's assessments of key trends, fluctuations, and unusual items. It should also link financial and performance information to provide meaningful analysis of the cost-benefit relationships of program accomplishments. Several of the Department's component entities using private sector GAAP do not present MD&A in their annual reports.

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.

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:

1. All 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, and

2. Entities that are statutorily required to report on a basis of accounting other than Federal GAAP provide supplemental information in their annual reports to include a section on MD&A in order to meet the reporting requirements of Federal GAAP.

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 2005 and FY 2004 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.

The Department again in FY 2005 approached those bureaus/reporting entities that are required by statute to produce their stand-alone financial statements to do so on a Federal sector GAAP basis. The U.S. Mint has agreed to prepare its FY 2006 financial statements on a Federal sector GAAP basis, and is currently revising its FY 2005 statements to reflect Federal GAAP. Treasury will work with the FASAB and the OIG in addressing this issue, and will continue working with the affected bureaus in FY 2006 to achieve greater conformance.

(Continued)

05-03: The Exchange Stabilization Fund's (ESF) Budgetary Accounting Methodology Should be Clarified. (Repeat Comment)

The Exchange Stabilization 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 the Treasury Information Executive Repository (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 Statement of Budgetary Resources (SBR) nor does it have any transactions that meet Office of Management and Budget (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.

Another SGL account that is reported inaccurately is Fund Balance with Treasury (FBWT) (SGL account 1010). ESF does not use this account nor is it included in its stand-alone financial statements. However, in order to pass the Department's Financial Management Service's (FMS) FACTS II edit checks, ESF must reclassify amounts from its asset accounts to SGL 1010. In FY 2005 and 2004, ESF reported approximately $16.4 billion in FBWT into FACTS. The amounts misclassified in FACTS II then are misclassified in the government-wide financial statements.

ESF's reporting to 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.

In response to our prior year recommendation 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 which was submitted to OMB and FMS. However, no waivers were granted for fiscal year 2005 and AIC is still in the process of communicating with OMB and FMS on this matter.

OMB Circular No. A-11, Part IV, requires non-appropriated 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*[1] states:

---

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

> "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, but has not 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. While the Department requested FMS to resolve the requirement to report FBWT to meet FACTS II edits as early as 2002, FMS has been unable to provide an automated solution to date. No approved model of budgetary transactions exists for ESF that would ensure consistent budgetary and proprietary data is readily available that can be traced directly to the SGL accounts.

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 methodolgy used in the translation of the ESF propietary accounts to budgetary accounts.

Recommendations

We recommend the CFO:

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.
4. Continue to work with FMS to resolve the requirement to report FBWT in order to pass FACTS II edits, recognizing that ESF does not have FBWT balances.

Management Response

The Department submitted a draft letter in September 2005 requesting a waiver from the Office of Management and Budget from including the budgetary reporting for the Exchange Stabilization Fund in the Department's consolidated financial statements, and the Financial Management Service and OMB budgetary reporting systems. In addition, a draft request was sent to Treasury's Financial Management Service in September 2005 on waiving the reporting of Fund Balance with Treasury (FBWT) for ESF investments.

The Department has tried to engage OMB and FMS on more than one occasion over the past ten years to help resolve the ESF budgetary reporting issue. However, more pressing events and workload issues prevented OMB

(Continued)

and the Department from fully addressing and resolving this issue. Treasury also worked with the Department's Office of Inspector General in attempting to develop transaction posting models that allow for the production of ESF's budgetary reporting.

The initial response received in October 2005 from FMS indicated that OMB and FMS will not grant a reporting waiver for ESF's FBWT. FMS provided a recommendation for reporting the FBWT for FY 2005, and suggested working with the Department on the unresolved issues in FY 2006. The Department will work with OMB and FMS to obtain specific guidance on providing more meaningful budgetary and FBWT reporting for ESF.

(Continued)

05-04: Annual Reconciliation Procedures to the President's Budget Should be Improved.

The Department's Office of Performance Budgeting (OPB) prepares the annual reconciliation of actual Budgetary Resources, Outlays, and Offsetting Receipts in the President's Budget (PB) to comparable information contained in the Department's Statement of Budgetary Resources for disclosure in the Department's consolidated financial statements as required by Statement of Federal Financial Accounting Standards (SFFAS) No. 7, *Accounting for Revenue and Other Financing Sources*. The PB reconciliation prepared for inclusion in the current year with respect to fiscal year 2004 revealed the following:

- The initial documentation provided to support the reconciliation did not fully support the reconciling amounts reported in the PB reconciliation.
- There were inconsistencies with respect to the classification of budgetary resources within the PB reconciliation when compared to the prior year PB reconciling classifications.

In response to questions raised during the audit, OPB provided additional documentation, revised the PB reconciliation, and ultimately reduced its initial fiscal year 2004 unreconciled differences from $318 million, $206 million, and $96 million, in absolute values, for amounts reported in the Budgetary Resources, Outlays, and Offsetting Receipts categories, respectively, to $124 million as shown in the table below for fiscal year 2004.

The final unreconciled differences reported in the PB reconciliation for this year in comparison with the previous year's unreconciled differences (in millions) are:

($ in Millions)

Fiscal Year	Budgetary Resources	% of Budgetary Resources	Outlays	% of Outlays	Offsetting Receipts	% of Offsetting Receipts
2004	$ 54	0.01	$ 69	0.02	$ 1	0.05
2003	109	0.03	109	0.03	151	11.90

The total of the unreconciled differences for FY 2004 were $124 million in comparison with a total of $369 million for FY 2003, a major reduction in unreconciled differences. Many improvements were made in the current year with respect to the PB reconciliation details as well as the supporting documentation provided to support the PB reconciliation. However, further improvements can be made to the process of preparing the reconciliation and expediting its review.

If key Department officials are unavailable to perform the reconciliation, the preparation of the reconciliation cannot be easily picked up by new staff without detailed written guidance. Given the complexity of the reconciliation for the Department, a detailed procedural manual providing step-by-step guidance for performing the reconciliation, as well as the documentation needed to be on hand for the annual audit, could help improve the efficiency, consistency in methodology, and completeness of the reconciliation. During the audit, OPB began the process of preparing an operating manual for the reconciliation; however, these policies and procedures have

(Continued)

not yet been approved that describe the process OPB uses for the reconciliation, nor is there a complete list of Department funds identified for PB reconciliation purposes with a classification of those funds by budget category, together with an explanation of why such funds should be reported in a particular budget category.

SFFAS No. 7, and the OMB Circular A-136, *Financial Reporting Requirements,* provide guidance for preparing the note on Reconciliation of the SBR to the PB. SFFAS No. 7, Part II, *Reconciliation Statement—Budgetary and Financial Accounting*, Section 79, states:

> "Disclosures are required if the information shown differs from that which is included in the "actual" column of the President's Budget. For example, this disclosure would be needed in cases where the reporting entity in the financial statements is different than the reporting entity in the Budget."

Section 1.7 of OMB Circular No. A-136, states:

> "Agencies should discuss any material changes to budgetary information subsequent to the publication of the audited Statement of Budgetary Resources (SBR) with their auditors to determine if restatement or note disclosure is necessary. At a minimum, any material differences between comparable information contained in the SBR and the actual information presented in the Budget of the United States Government must be disclosed in the footnotes to the SBR."

Section 9.33 of OMB Circular A-136, further states that the related note should:

> "Identify and explain material differences between amounts reported in the SBR and the actual amounts reported in the Budget of the United States Government as required by SFFAS No. 7…. Differences, in and of themselves, may or may not indicate a reporting error. Legitimate reasons for differences could exist. For example, expired unobligated balances are reported in the SBR and SF 133 but not in the Budget of the United States Government. This disclosure should be provided when comparable line items differ between the President's Budget and the SBR."

In addition, GAO's *Standards for Internal Control in the Federal Government*[1] 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 relies on the knowledge and skills of key experienced staff to prepare the reconciliation each year. However, because the reconciliation is performed only once a year, the lack of written procedures contributed to initial misclassification of budgetary resources for reconciliation purposes. This led to additional efforts to obtain documentation and increased time spent on the reconciliation that an operating manual containing detailed policies and procedures might help to correct.

---

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

(Continued)

Recommendations

We recommend that the CFO in coordination with the Director of OPB, and the Director of AIC prepare detailed policies and operating procedures for the reconciliation of the Combined SBR to the President's Budget. As part of its procedures, OPB and AIC should classify amounts reported in the SBR and President's Budget by reconciling budgetary source to fund symbol along with a definition of each reconciling item and an explanation of what funds should be included in the line item. Policies and procedures developed should also include procedures for review and approval by authorized officials.

Management's Response

The Office of Performance Budgeting (OPB) prepared operating procedures for the Statement of Budgetary Resources/President's Budget reconciliation process in 2005. This procedure was shared with the consolidated financial statement auditors for their review. OPB has agreed with the auditors' recommendation to add a list of fund symbols with explanations on why they are reconciling items.

(Continued)

05-05: A Formal Process is Needed to Monitor the Use of Sensitive System Software Utilities.

There is no formal process in place to monitor the use of sensitive system software utilities, such as those with the capability to add, remove, or alter user accounts and privileges within the operating system.

The Federal Information Security Management Act (FISMA), issued as part of the E-Government Act of 2002, requires Federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. FISMA further requires Federal agencies to follow information security guidance issued by the National Institute of Standards and Technology (NIST).

Office of Management and Budget (OMB) Circular A-123, *Management Accountability and Control* (OMB Circular A-123), requires that access to resources and records should be limited to authorized individuals; and accountability for the custody and use of resources should be assigned and maintained.

OMB further states in OMB Circular A-130 Appendix III (Security of Federal Automated Information Resources) (OMB Circular A-130), that access controls should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, and loss. Such controls include logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Ineffective access controls increase the risk of unauthorized changes to the data that may affect the data's reliability and increases the risk of destruction or inappropriate disclosure of the data.

The Department currently does not have an effective means to monitor the use of sensitive system software utilities. However, we have been informed that the Department is currently in the procurement phase for software utility that will allow for the logging and monitoring of sensitive system utility use.

Without a defined process, or a means to effectively and consistently monitor the use of system utilities, management cannot reliably review the activities of users to look for inappropriate or unusual activity. Accordingly, this activity may go unnoticed and may not be investigated.

Recommendations

We recommend that the Deputy Assistant Secretary Chief Information Officer (CIO) develop formal policies and procedures, and enforce such policies for the monitoring of sensitive system software utilities.

Management Response

Treasury Departmental Offices management, in partnership with the SEAT management contractor, has identified software which will be able to monitor sensitive system software utilities. Note that this capability does not exist in the MicroSoft Windows operating system itself. Treasury has directed the support contractor to purchase and implement this software to assist in the implementation and enforcement of monitoring sensitive system software utilities. DO plans to implement Quest's Intrust Log Management tool. It will send real time alerts when unusual activity is reported in system and network security, application, and system logs. The system will also allow the Security group to review periodically all logs on a central console, where they can review the activities of users to look for inappropriate or unusual activity.

(Continued)

05-06: Access Controls over the Treasury Information Executive Repository (TIER) System Should be Strengthened.

Configuration management controls over TIER, do not prevent lead developers from gaining access to the production environment. The two lead developers have access to the three TREAS-TIER servers, development, test, and production. Furthermore, they serve as the chief implementers of TIER changes. The lead developers create, test, and also load TIER changes onto the production server. Additionally, the lead developers perform system administrator duties.

A segregation of duties violation exists for system changes made outside of the scheduled TIER quarterly releases. We noted that system change requests (SCR) indicate that one individual performs several roles such as Owner, Submitter, Requester, Developer, Tester, and Reviewer of the SCR.

The SCR process deviates from aspects of the Department's Treasury Software Change Management (SCM) Plan. Specifically, the lead developers perform the Team Lead's roles and responsibilities over the SCR process. This segregation of duties violation bypasses the Team Lead's necessary oversight as prescribed in the SCM.

CRs are not completed for all change requests made outside of the scheduled TIER Quarterly Releases. Furthermore, a documented approval does not exist for emergency enhancements, bug fixes, and data fixes.

Also, test documentation is not available for changes implemented outside of the scheduled TIER quarterly releases; specifically data fixes, bug fixes, and emergency enhancements. During our review, we noted that test results were not always maintained.

The SCM describes the process for creating and managing change requests for Application Systems Support Contract (ASSC) documents, templates, and processes. The Plan guides that requests are submitted verbally or through written documentation by the client to the Project Manager or Team Lead who then evaluates the requests and enters it into Tracker. Other roles pertaining to the SCR process are summarized within the SCM Plan. Furthermore, the SCM Plan states that "Software control ensures that changes to computer programs are developed and tested using valid copies of programs and test databases, and that such changes do not adversely affect system users. Software control procedures are particularly important for documenting and tracking maintenance changes during the operation phase of the life cycle."

The Department's *ASSC SDLC Workflow and Processes Handbook* states that "Emergency requests are approved by the Team Leaders; corrections are made, tested, and implemented; and finally the change request is completed and forwarded to the Team Leader for review." Furthermore, "The project Change Control Board consisting of the Team Lead/Project Manager, Treasury Liaison and the Customer must approve every change or operational problem request. Once approved, the request will be added to the Team Master Project schedule and tracked accordingly."

The Department's *TIER FY05 Project Plan* states, "The Database Administrators (DBA) will then execute the appropriate scripts loading the release onto the production server and advise the development team when completed." OMB Circular A-130 states, "Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process."

(Continued)

OMB Circular A-130 further requires that proper life cycle development requires the complete documentation of a system. "Each stage of the information life cycle carries with it records of management responsibilities. Agencies need to record their plans, carefully document the content and procedures of information collection, ensure proper documentation as a feature of every information system, keep records of dissemination programs, and, finally, ensure that records of permanent value are preserved."

OMB Circular A-127, *Financial Management Systems*, states that "all documentation associated with systems and software should be continually updated to provide sufficient detail to obtain a comprehensive knowledge of understanding of their operation." Further, adequate documentation of program changes facilitates future testing of other modifications and allows a reconstruction, if necessary, to research a problem based on the actual tests and results.

NIST's *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST SP 800-14, Section 3.12), recommends that organizations base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

The Department's personnel indicated that lead developers also perform the system administrator roles due to limited resources. In addition, due to limited resources and time constraints, the prescribed method for System Change Requests is not always followed. Further, the Department does not maintain documentation of approval for all changes made outside of Quarterly Releases. Due to time constraints, approval is often received following the implementation of a change. The Department's personnel explained that due to time constraints and limited resources, testing documentation is not consistently documented and maintained.

Excessive system privileges, such as privileges related to sensitive system components like the production server, increase the risk that the data is subject to unauthorized access, loss, or misuse. Furthermore, providing this privilege to developers could allow them to circumvent the configuration management process and implement code that has not been tested or approved by the appropriate parties.

Effectiveness of testing could be skewed and biased if performed by the developer of the code change. Additionally, flawed system software changes may be implemented into the production environment.

Lack of oversight of software configuration management as described in the SCM Plan increases the risk that erroneous or fraudulent changes to software could be processed and implemented, which could impact the integrity of computer resources.

A lack of documentation for each system change capturing detailed systems testing prepared by the programmer and reviewed by a programming supervisor may allow unauthorized and potentially inaccurate computer program changes to be implemented into the production environment.

Inadequate documentation of testing and results may inhibit future testing of other modifications and prevents reconstruction, if necessary, to research a problem based upon the actual tests and results. Additionally, without documentation of testing, evidence that testing in fact took place is not available for verification.

(Continued)

Recommendations

We recommend that the CIO take steps to:

1. Ensure that the access privileges to migrate changes into the production environment are removed from the development staff.
2. Segregate the duties of the lead developer of software changes thereby preventing developers of a software change from testing their own work.
3. Ensure that the Department's management follows the Treasury SCM methodology and a higher degree of management oversight occurs for the development and implementation of all changes over TREAS TIER.
4. Update the Treasury SCM Plan and ASSC SDLC Workflow and Processes Handbook to reflect the current practices for opening an SCR.
5. Maintain test plans and test results for all changes implemented outside of the scheduled TIER quarterly releases.

Management Response

Many of the changes that occur outside of the scheduled releases are called "data fixes" because currently, that is the only choice left to enter an SCR in Tracker. In reality, these are changes to the reference infrastructure data, not the user's data. The most common reference changes are built into the application, such as additions or changes to SGLs or Fund Symbols. These are straightforward, and by definition do not change the application code. No test plan is needed because the reviewer only has to view the appropriate reference table to see the change has been made. For these cases, the recommendation to maintain test plans and results for such "data" fixes is not considered necessary. The tester/reviewer or actual user requesting the change could easily verify that the change was done correctly. In most cases, these changes are needed on a very short timeline. If the KPMG recommendations were implemented as written, requested changes—often time-critical especially at the end of the fiscal year—would be delayed to the extent that our service to users would not be timely.

05-07: Configuration Management Processes Over CFO Vision Needs Improvement.

During our FY 2005 review of the configuration management process over CFO Vision, we noted the following control weaknesses:

a. Formal processes are not followed when making changes to CFO Vision reporting templates.

b. CFO Vision does not have a version manager tool for template changes made to the application.

Treasury Information Technology Security Program Publication: *IT Security Program Handbook for Sensitive Systems,* states that "Organizational Elements shall prepare configuration management plans for all IT systems and networks. Organizational Elements shall establish, implement, and enforce change management and configuration management controls on all IT systems and networks."

The NIST Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle*, states that configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

NIST SP 800-18, *Guide for Developing Information Technology Security Plans*, states "There are many models for the IT system life-cycle but most contain five basic phases: Initiation, development/acquisition, implementation, operation, and disposal."

CFO Vision is primarily used as a reporting tool for TIER. The changes made within CFO Vision are not performed on the actual source code but instead to the templates of the report. Any change performed only modifies the look or organization of a report. A formal configuration management process is not documented because minor changes are performed on CFO Vision; therefore, the Department believes that a formal configuration management process or SDLC is not needed.

CFO Vision administrators do not keep previous versions of the application stored locally due to a lack of space and because changes are only made to the templates and not to the source code. They believe that the minor template changes performed on CFO Vision do not need to be readily available and tracked.

Without a proper System Development Life Cycle (SDLC) or configuration management process regarding the flow of changes from development to production, unauthorized and potentially inaccurate program changes may be implemented into the production environment.

As a result, since there is no version manager tool in place for CFO Vision, once a change is made to the application, the previous version of the application no longer exists locally. If there is a problem once changes have been made in production, there is no way to immediately revert back to the previous version of the templates without having to restore from tape backups.

(Continued)

Recommendations

We recommend that the CIO:

1. Develop and implement a detailed SDLC or configuration management procedures for performing changes over CFO Vision. These procedures should include a formal change request form, proper authorization of the change prior to the initiation of the work, formal approval of the change prior to the initiation of the work, and retention of all change request forms.

2. Implement a version manager mechanism in order to maintain previous versions of CFO Vision reports.

Management Response

Recommendation #1: Treasury is implementing a new version of CFO Vision, a COTS product, during fiscal year 2006. This version will be web-based and available to all Treasury bureaus through the Treasury Intranet. As part of the implementation of this new version, the Department will update the configuration management process to formalize the process to include change requests, a review and approval process, and retention of supporting documentation.

Recommendation #2: As part of this new release, the systems development team will implement a version manager mechanism to maintain versions of CFO Vision reports.

We anticipate implementing these changes after the new version is installed, stabilized, and rolled out to the bureaus.

 (Continued)

05-08: CFO Vision Access Controls Should be Strengthened.

No policies or procedures are currently in place to periodically review CFO Vision user access lists to determine if access is still needed, including employees that have been terminated, or the same level of access is still required by the user. Additionally, a formal process has not been documented to ensure the timely notification to application administrators when personnel transfers or terminations occur.

The Department's Information Technology Security Program TD P 85-01 Volume I, Policy Part 1, *Sensitive Systems,* states: "Program officials shall ensure users of the systems supporting their programs have a validated requirement (need to know) and an appropriate security clearance to access their systems."

NIST Special Publication 800-12, *An Introduction to Computer Security,* states, "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."

OMB Circular 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").

In the *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST SP 800-14, Section 3.12), NIST recommends that organizations base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

Due to limited resources, management has not established formal policies and procedures for the periodic review of CFO Vision user access lists. Additionally, the Department is still in the process of developing procedures related to CFO Vision, including the processes related to user account management.

By not performing a periodic review of user accounts to ensure that all access levels are appropriate for a given user's job description and to verify that all user accounts belong to current employees, the Department increases the risk that employees may have unnecessary access privileges to the system. This access increases the risk of intentional or inadvertent alteration of the integrity of the application.

Furthermore, should a separated employee's CFO Vision user account not be timely removed, the separated employee, with malicious intent, or another person with knowledge of this active user account, could use this account to alter the integrity of the application data.

 (Continued)

Recommendations

We recommend that the CIO take steps to establish formal policies and procedures regarding user administration surrounding the CFO Vision application. We also recommend that the CIO:

1. Develop and implement policies and procedures requiring periodic review of CFO Vision access lists to determine whether logical user access is current, consistent with job responsibilities, and in accordance with the principle of least privilege.

2. Develop and implement policies and procedures to promptly notify the application administrators of the termination or transfer of personnel with CFO Vision access.

Management Response

Recommendation #1: Treasury is implementing a new version of CFO Vision, a COTS product, during fiscal year 2006. This version will be a web-based system and available to all Treasury bureaus through the Treasury Intranet. With the implementation of this version, Treasury will follow the procedures implemented for other applications maintained by the Office of the DCFO under the umbrella Financial Analysis and Reporting System (FARS). This includes a structured process for granting new user access and an annual recertification of all system users. These existing procedures require new users to take the Department's systems security training and review the system Rules of Behavior.

Recommendation #2: As part of the implementation of the new release, the systems team will evaluate the feasibility of linking the CFO Vision user file with the LDAP, which maintains the inventory of authorized users to the Treasury network. As employees leave the Department, they are removed from the LDAP and will not be able to access the Treasury network. This will eliminate the potential for former users accessing CFO Vision.

Canceling user authorization of employees who no longer require access to the system is much more difficult to control. This relies on the user's manager to notify the DCFO's Office to remove the access rights. We will catch these changes as part of the annual user recertification that will be implemented for the new version of CFO Vision.

We anticipate implementing some of these changes after the new version is installed, stabilized, and rolled out to the bureaus. New user access will be granted in accordance with existing FARS new user procedures.

05-09: Financial Analysis and Reporting System (FARS) Access Controls Should be Strengthened.

Financial Analysis and Reporting System (FARS) access request forms could not be provided for three out of five CFO Vision users selected for testing. The Department's management is not enforcing the completion of new user access request forms for authorizing CFO Vision access.

OMB Circular A-123 states that access to resources and records should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.

OMB Circular A-123 further states that access controls should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, and loss. Such controls include logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Ineffective access controls increase the risk of unauthorized changes to the data that may affect the data's reliability and increases the risk of destruction or inappropriate disclosure of the data.

Granting system access without evidence of supervisory authorization increases the risk of unauthorized individuals gaining access to the Department's data.

Recommendations

We recommend that the CIO reinforce, through training or an updated policy statement, a requirement for Department personnel to consistently utilize the FARS access request form to document management authorization for access to the CFO Vision application.

Management Response

Treasury concurs with this recommendation. CFO Vision is currently available only to users on the DO LAN, the only users are in the Office of the DCFO, Office of Performance Budgeting, Office of Financial Management, the financial statement auditors, and the FARS systems development team. While it was the practice to have CFO Vision users complete a new user access form, this practice was not consistently followed. With the scheduled upgrade of CFO Vision to a web-based application, it will become available to Treasury bureaus as well. As a result, the existing FARS new user access process will be adhered to by all new CFO Vision users. All new users will be required to complete a new user access request form that is signed by their organization's Responsible Official, complete the Department's systems security awareness training, and complete the FARS Rules of Behavior.

CFO Vision currently has two systems administrators with responsibility for administering the system. One has had this responsibility since the startup of the system in 1999 and the other has been an administrator since 2003. As is the case for other CFO Vision users, new user access forms were not required until procedures were revised within the past year. In addition, since there are only two administrators, who worked closely with the DCFO's Office of Financial Systems Integration, no annual recertification was performed. As part of the implementation of the new version of CFO Vision in 2006, we will implement the access procedures currently followed for all other FARS applications, as described above.

(Continued)

05-10: Backup Tapes for the Treasury Information Executive Repository (TIER) System and CFO Vision Production Servers Should Be Protected.

The backup tapes for the Treasury Information Executive Repository and CFO Vision production servers are stored in the cage with the server within the Treasury data center. Additionally, the backup tapes are not stored in a protective case prior to being transported to the off-site location.

FISMA requires agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. FISMA further requires Federal agencies to follow information security guidance issued by the NIST.

Also, in the *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Section 3.5.1), the NIST SP 800-14 states that backups should be stored securely and that measures should provide physical and environmental protection.

Further, OMB Circular A-130 states that agencies shall maintain disaster recovery and continuity of operations plans for information technology installations. To ensure continuity of operations during an extended outage of the computer system, backups of computer system data must be performed and stored off-site.

Management has not made it a priority to see that backup tapes are stored in protective cases. In the event that the tapes located in the data center were damaged within the data center or during transport to the off-site storage facility, Treasury would be forced to rely on older tapes and have to expend additional resources reconstructing the information lost on the daily and weekly tapes.

Recommendations

We recommend that the CIO develop and implement policies to require storage of these backup tapes in fireproof boxes so that they will be protected in the event of a disaster.

Management Response

Treasury has identified alternative back-up service approaches and their relative funding requirements. However, funding for a formal off-site storage service is currently unfunded. The Department will review its options for implementing this recommendation.

(Continued)

05-11: Formal Continuity of Operations Plan and Disaster Recovery Procedures for TIER and CFO Vision Should be Established.

There is no formal continuity of operations plan (COOP) and disaster recovery procedure (DRP) in place for TIER and CFO Vision. NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* (Chapter 11), states:

"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 off site 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 A-130 states that a contingency plan must 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 disaster/recovery plan.

OMB Circular A-130 further guides that "Agencies shall 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 plan maintained by the installation at which the application is processed."

Management informed us that due to funding constraints, both the COOP and DRP have been unfunded for TIER and CFO Vision. Without corporate business continuity and disaster recovery plans, if a natural disaster caused the system to fail, the Department's ability to restore operations and continue its business operations may be significantly delayed.

Recommendations

We recommend that the CIO develop, implement, and test a continuity of operations plan and a disaster recovery plan for the TIER and CFO Vision applications. Additionally, this plan should be tested annually upon implementation.

Management Response

To achieve economy of scale, the CIO's Office intends to review disaster recovery and COOP planning for the suite of applications managed at the Qwest CyberCenter. Though the Department agrees with the recommendation, we must prepare a justification to obtain the required funding through the CIO's investment management program.

Exhibit I

DEPARTMENT OF THE TREASURY

FISCAL YEAR 2005

Management Letter Report

Status of Prior Year Management Letter Comments

	Prior Year Recommendations	Current Year Status
I	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 number 05-02.
II	Analysis of Financial Reports at the Department Level Should be Improved	This comment has been resolved and closed.
III	Fund Balance with Treasury Reconciliations Should be Prepared on a Consistent Basis	This comment has been resolved and closed.
IV	The Exchange Stabilization Fund Budgetary Accounting Methodology Should be Clarified	This comment has not been corrected and is repeated in the current year as comment number 05-03.
V	Segregation of Duties Related to TIER Should be Strengthened	This comment has been resolved and closed.
VI	CFO Vision Access Controls Should be Strengthened	This comment has been resolved and closed.
VII	TIER Access Controls Should be Strengthened	This comment has been resolved and closed.