# Audit Report

OIG-10-035

Management Letter for Fiscal Year 2009 Audit of the Department of the Treasury's Financial Statements

February 4, 2010

## Office of Inspector General

DEPARTMENT OF THE TREASURY

Information within the **FISCAL YEAR 2009 COMMENTS** has been **REDACTED** under **FOIA Exemption 2, 5 U.S.C. §552(b)(2)**:

**FISCAL YEAR 2009 COMMENTS**:

**09-07: Encryption** (see pages 9 and 10)

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

February 4, 2010

**MEMORANDUM FOR DANIEL TANGHERLINI**
**ASSISTANT SECRETARY FOR MANAGEMENT**
**AND CHIEF FINANCIAL OFFICER**

**FROM:** Michael Fitzgerald
Director, Financial Audits

**SUBJECT:** Management Letter for Fiscal Year 2009 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 2009 financial statements. Under a contract monitored by the Office of Inspector General, KPMG LLP (KPMG), an independent certified public accounting firm, performed an audit of the financial statements of the Department as of September 30, 2009 and for the year then ended. The contract required that the audit be performed in accordance with generally accepted government auditing standards; applicable provisions of Office of Management and Budget Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements,* as amended; and the *GAO/PCIE Financial Audit Manual*.

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

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

Should you have any questions, please contact me at (202) 927-5789, or a member of your staff may contact Ade Bankole, Manager, Financial Audits at (202) 927-5329.

Attachment

KPMG

# U.S. DEPARTMENT OF THE TREASURY
# FISCAL YEAR 2009

Management Letter

December 15, 2009

**U.S. DEPARTMENT OF THE TREASURY**

Fiscal Year 2009
Management Letter Report

**Table of Contents**

**KPMG LLP**
2001 M Street, NW
Washington, DC 20036

December 15, 2009

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

We have audited the consolidated financial statements of the U.S. Department of the Treasury (Treasury Department) as of and for the year ended September 30, 2009, and have issued our report thereon dated December 15, 2009. Our report indicated that we did not audit the amounts included in the consolidated financial statements related to the Internal Revenue Service (IRS) or the Office of Financial Stability (OFS), both component entities of the Treasury Department. The financial statements of the IRS and the OFS were audited by another auditor whose reports were provided to us.

In planning and performing our audit of the consolidated financial statements of the Treasury Department in accordance with auditing standards generally accepted in the United States of America, we considered the Treasury Department's internal control over financial reporting (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 Treasury Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Treasury Department's internal control.

During our fiscal year (FY) 2009 audit of the Treasury Department's consolidated financial statements, we, and the other auditor, noted certain matters involving internal control and other operational matters that we considered significant deficiencies under standards established by the American Institute of Certified Public Accountants (AICPA). A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Treasury Department's financial statements will not be prevented or detected and corrected on a timely basis.

Our consideration of internal control was for the limited purpose described above and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. In our Independent Auditors' Report dated December 15, 2009, we reported the following significant deficiencies in the following areas involving internal control over financial reporting:

- Financial Management Practices at the Departmental Level (Repeat Condition)
- Financial Systems and Reporting at the IRS (Repeat Condition)
- Financial Accounting and Reporting at the OFS
- Information System Controls at the Financial Management Service (FMS).

We consider the significant deficiencies related to Financial Systems and Reporting at the IRS and Financial Management Practices at the Departmental Level, noted above, to be material weaknesses. Detailed findings and recommendations to address the above significant deficiencies are not repeated within this document.

Although not considered significant deficiencies, 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 Treasury Department's management, are intended to improve internal control or result in other operating efficiencies. The matters presented in this letter do not include internal control or operational matters that have been presented to the management of the Treasury Department's offices or operating bureaus that were audited separately by other auditors.

Exhibit 1 provides the status of the five comments included in our management letter arising from our FY 2008 audit. We have not considered the Treasury Department's internal control since the date of our report.

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

The Treasury 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 Treasury Department, the Treasury Department's Office of Inspector General, the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and Congress and is not intended to be, and should not be, used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

## FISCAL YEAR 2009 COMMENTS

### 09-01: Financial Reporting Standards for Treasury's Component Entities (Repeat Comment)

The Treasury 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 Treasury 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 continue to do so. These component entities include the Bureau of Engraving and Printing, the Office of Thrift Supervision, the Exchange Stabilization Fund, the Federal Financing Bank, and the Community Development Financial Institutions Fund.

The use of a combination of generally accepted accounting principles (GAAP) by the Treasury Department and its component entities complicates the preparation of the Treasury Department's consolidated financial statements since additional information required for Federal GAAP reporting must be developed, mapped, and submitted to the Treasury Department's data warehouse by component entities, and reviewed for compliance with Federal GAAP and overall reasonableness by the Treasury Department's 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. Consequently, the concept of "presents fairly" for those entities does not adequately convey 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 the Statement of Budgetary Resources (SBR), although this statement is an integral part of the Treasury Department's consolidated financial statements, and must be prepared regardless of whether or not the component receives appropriations from the U.S. Government. Moreover, information reported in the Treasury Department's SBR must be reconciled to enacted amounts in the President's budget and disclosed in the notes to the Treasury Department's consolidated financial statements. Considerable additional preparation is 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 nonreimbursed 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 Treasury Department's component entities.

This matter has been reported since FY 2004 and has not been resolved. The continued use of private sector GAAP by certain Treasury Department component entities decreases the usefulness of information reported by these entities for users of Federal financial statements and complicates the preparation of the Treasury Department's consolidated financial statements.

***09-01 Recommendation***

We recommend that the Treasury Department's Chief Financial Officer (CFO), with input from the Director, Office of Accounting and Internal Control (AIC), work with those Treasury Department bureaus following FASB reporting standards to achieve conformance so that all reporting entities within the Treasury Department prepare their financial statements in accordance with Federal GAAP in order to strengthen and standardize financial accounting and reporting throughout the Treasury Department. If a bureau is statutorily required to report on a different basis of accounting, then a separate set of financial statements should be prepared by these entities to meet such requirements.

***Management Response***

We will continue to work with those Treasury components that prepare their stand-alone financial statements on a commercial GAAP basis in order to work towards their migration to Federal GAAP reporting in their stand-alone statements, especially as components have the need to replace their legacy financial systems. At the same time, we will continue to monitor FASAB's ongoing work on this topic. At the present time, FASAB standards allow component entities who have historically reported on a commercial GAAP basis to continue reporting in the same manner. However, we recognize that this situation causes several financial reporting issues at the Departmental level.

**09-02: Opening Balances**

Certain opening balance differences were identified during our review of the documentation provided in support of opening balances. AIC did not adequately prepare supporting documentation and review the FY 2009 opening balances.

OMB Circular No. A-123, *Management's Responsibility for Internal Control*, (OMB Circular No. A-123) states that monitoring the effectiveness of internal control should occur in the normal course of business. In addition, periodic reviews, reconciliations, or comparisons of data should be included as part of the regular assigned duties of personnel. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. If an effective continuous monitoring program is in place, it can level the resources needed to maintain effective internal controls throughout the year.

In implementing the GAO *Standards for Internal Control in the Federal Government*, management is responsible for developing the detailed policies, procedures, and practices to fit in a Department's operations and to ensure that they are built into an integral part of its operations.

Internal controls should be clearly documented in management directives, administrative policies, or operating manuals and should be properly managed and maintained.

***09-02 Recommendation***

We recommend that the CFO, with input from the Director of AIC, review existing preparation and review procedures over the opening balances analyis that is conducted annually, assess the improvements needed, and develop procedures to address the needed improvements.

***Management Response***

We concur with the recommendation and will perform a review of our policies and procedures over opening balances, including supervisory review, and make improvements for identified weaknesses.

**09-03: Intragovernmental Transactions and Activities**

AIC did not fully develop and validate a comprehensive process to include effective internal controls over the intragovernmental reporting process to ensure compliance with the *Treasury Federal Intragovernmental Transactions Accounting Policies Guide's* (TFITAPG) reporting requirements in FY 2009.

We identified material variances in several line items in the Trading Partner balances between what was submitted by AIC for third quarter FY 2009 into the FMS Intragovernmental Reporting and Analysis System (IRAS) and the related intragovernmental partner and account balances in Treasury Department's general ledger. Specifically, we determined that not all intragovernmental balances were submitted by AIC into IRAS as required by TFITAPG. These errors could have been avoided had there been appropriate supervisory reviews of the data before submission.

The Treasury Department's FMS provides detailed guidance on accounting and reconciling intragovernmental balances in the TFITAPG. TFITAPG Section 4706.30b states, "In support of the quarterly reconciliation process, verifying agencies must submit full proprietary adjusted trial balances or submit, at a minimum, a trial balance that contains all their accounts with an 'F' attribute and the following other US Standard General Ledger (USSGL) accounts: 1010 (Fund Balance With Treasury), 3101 (Unexpended Appropriations – Appropriations Received), and 3106 (Unexpended Appropriations – Adjustments) to FMS no later than July 23, 2009, for third quarter fiscal 2009, and October 18, 2009, for fourth quarter fiscal 2009."

OMB Circular No. A-123 states that monitoring the effectiveness of internal control should occur in the normal course of business. In addition, periodic reviews and reconciliations, or comparisons of data, should be included as part of the regular assigned duties of personnel. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. If an effective continuous monitoring program is in place, it can level the resources needed to maintain effective internal controls throughout the year.

In implementing the GAO *Standards for Internal Control in the Federal Government*, management is responsible for developing the detailed policies, procedures, and practices to fit in a Department's operations and to ensure that they are built into an integral part of its operations.

Internal controls should be clearly documented in management directives, administrative policies, or operating manuals and should be properly managed and maintained.

***09-03 Recommendations***

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

1. Develop policies and procedures to account and appropriately report the Treasury Department's intragovernmental transactions as required by FMS in compliance with TFITAPG.
2. Mandate supervisory reviews of intragovernmental accounting transactions and related underlying data to assess accuracy and reasonabless prior to reporting to FMS.

***Management Response***

We agree with the recommendation. We will incorporate the review of intragovernmental transactions and balances into our overall review/updating of policies and procedures to ensure that intragovernmental balances and transactions are properly identified and reviewed for accuracy and completeness prior to reporting to FMS.

**09-04: Reconciliation of the SBR to the SF-133, Report on Budget Execution and Budgetary Resources**

The FY 2009 third quarter reconciliation of the SF 133, *Report on Budget Execution and Budgetary Resources (SF 133)*, to the unaudited third quarter SBR reconciliation for comparable line items was not completed until September 2009.

The Treasury Department does not have policies in existence to require the timely completion of these budgetary reconciliations, which could cause material differences requiring correction between the SF 133 and the SBR. As a result, amounts reported on the SBR may be misstated. In addition, the Treasury Department is not in compliance with reconciliation and reporting requirements prescribed by OMB Circular No. A-136, *Financial Reporting Requirements* (OMB Circular No. A-136).

OMB Circular No. A-136, Section II.4.6.1, states, "Information on the SBR should be reconcilable to the budget execution information reported on the SF 133 *Report on Budget Execution and Budgetary Resources* and with information reported in the Budget of the United States Government to ensure the integrity of the numbers presented…Consistency between budgetary information presented in the financial statements and the Budget of the United States Government is critical to ensure the integrity of the numbers presented. The FACTS II helps to ensure the consistency of data. The FACTS II data submitted by agencies are USSGL-based trial balances, which are used to populate the SF 133 and the actual column of the Program and Financing Schedule of the Budget."

OMB Circular No. A-136, Sections II.4.6.5, 6, and 8 state, "The resources reported on this statement shall agree with, and be reconciled to, the total budgetary resources reported for the aggregate of all budget accounts on the SF 133... The status of budgetary resources reported on this statement shall agree with, and be reconciled to, the total status reported for the aggregate of all budget accounts on the SF 133...The outlays shall also agree with, and be reconciled to, the

aggregate of outlays reported on the SF 133 for the aggregate of all budget accounts, including nonbudgetary financing accounts and the disbursements and collections reported to the Treasury Department on a monthly basis (SF 224, *Statement of Transactions*; SF 1219, *Statement of Accountability;* and SF 1220 *Statement of Transaction*s) per Circular No. A-11."

OMB Circular No. A-136, Section IV.3, indicates that "Agencies are required to submit an analysis of material differences between the current quarter's unaudited SBR and the current quarter's department-wide SF 133, *Report on Budget Execution and Budgetary Resources*. Agencies should reconcile the two reports; however, agencies are only required to provide to OMB an explanation for the material differences between the SBR and SF 133 for comparable line items related to budgetary resources, obligations, and outlays."

***09-04 Recommendation***

We recommend that the CFO, with input from the Director of AIC, strengthen current policies and procedures related to its quarterly SF 133 to SBR reconciliations to require timely quarterly reconciliations to be prepared and documented, including completion of supervisory review, so that explanations for any material differences between the SBR and SF 133 for comparable line items are provided to OMB timely.

***Management Response***

We agree with the recommendation. The current Standard Operating Procedures (SOP) for Reconciliation of Budget Execution Data will be reviewed and updated as necessary to incorporate any additional documentation requirements, to clarify timelines, and to include provision for a robust review by Treasury officials to support the SF-133/SBR Reconciliation. Quarterly reconciliations of the FACTS II data and SBR are completed and are identified both in the Office of Performance Budgeting (OPB) execution timeline and in the SOP, as are periodic reconciliations of the SF-133 data and the SBR. OPB Management has filled the Budget Execution Team Lead position, which will provide for regular supervisory review of reconciliations and other budget execution reports and increased emphasis on timeliness and accuracy. In addition, an automated tool to populate the data from the SBR and SF-133 into the reconciliation worksheet was developed to assist in the reconciliation. This tool should improve the timeliness of the reconciliation.

**09-05: Audit Logs**

Currently, a database administrator (DBA) of the system is performing the review of the audit logs for the Oracle database that supports the Treasury Department's Information Executive Repository (TIER), which creates an issue with segregation of duties, and in addition, there is no evidence of review of the Oracle audit logs. The Treasury Department also has not documented who should review the audit logs to ensure there is not a conflict of interest or require evidence to support the review of the audit logs.

The lack of monitoring by a designated individual who is independent of the operation of TIER makes it difficult for the DBA and System Owner to protect TIER against security and infrastructure vulnerabilities and hold individual users accountable for system activities. When audit logs are not reviewed independently, and are not supported with evidence of a review by the

designated individual, suspicious activities may go undetected, leading to the compromise of TIER data. In addition, unauthorized disclosure or changes to TIER may go undetected, compromising the confidentiality and integrity of the data.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security*, Section 9.4.2.1, *Review of System Logs*, states that "a periodic review of system-generated logs can detect security problems, including attempts to exceed access authority." Section 18.3.2, *Review of Audit Logs*, states, "Application owners, data owners, system administrators, data processing function managers, and computer security managers should determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities. This determination should have a direct correlation to the frequency of periodic reviews of audit trail data."

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* **(**NIST SP 800-53), Control AU-6, *Audit Monitoring, Analysis, and Reporting*, states, "The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions."

NIST SP 800-53, Control AU-11, *Audit Record Retention*, states, "The organization retains audit records [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements."

***09-05 Recommendations***

We recommend that the Chief Information Officer (CIO), with input from the Office of the Deputy Chief Financial Officer (DCFO):

1. Assign an individual other than the DBA to perform a review of the audit logs, or implement mitigating controls if the DBA has to perform the review such as System Owner or Management reviews.
2. Maintain evidence of the audit log reviews for the Oracle database.

***Management Response***

We agree with the recommendations to enhance audit log reviews. The Department believes that reviewing the audit logs is an integral part of the DBA's role. Therefore, the DBA will continue to monitor the logs to identify any unusual or suspicious activities. In addition, a second party will review the audit logs on a periodic basis to provide an independent review. DCFO and CIO Offices will develop a corrective action plan that will implement segregation of duties in the review of audit logs and provide evidence that logs have been appropriately reviewed.

**09-06: Baseline Configurations**

The Treasury Department does not currently have the baseline configurations documented for the production servers that support TIER and CFO Vision in the system security plan. The Treasury

Department's management was not aware that they needed to document their standard baseline configuration for the production servers of TIER and CFO Vision.

Without properly implemented baseline configurations, systems may not be updated properly with needed patches and upgrades. Insecure system configurations may expose security weaknesses, provide enticement information to a malicious user, provide access to remote users, and allow users to replace, retrieve, or modify sensitive data.

The Treasury Department's Information Technology Security Program, Treasury Directive Publication 85-01, Section 3.5, *Security Configuration and Vulnerability Management Policy,* states, "Bureaus shall develop and implement Configuration, Vulnerability, and Patch Management plans for all of their IT systems and networks."

NIST SP 800-53, Control CM-2, states, "The organization develops, documents, and maintains a current baseline configuration of the information system."

NIST SP 800-53, Control CM-6, states, "The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system."

***09-06: Recommendations***

We recommend that the CIO, with input from the DCFO:

(1) Formally document the baseline configuration for the production servers of TIER and CFO Vision.
(2) Assess compliance with the baseline configuration on an annual basis, at a minimum.

***Management Response***

We agree with the recommendation. The CIO's Office has developed a baseline configuration for the FARS server environment and will update the System Security Plan during the upcoming 2010 document update. On at least an annual basis, Treasury will conduct a system test to assess the baseline configuration and document any variances to the baseline.

**09-07: Encryption**

User sessions [redacted] are not encrypted using Secure Sockets Layer (SSL). The Treasury Department's management did not completely enforce the security requirements that require the use of SSL when accessing [redacted], and the Treasury Department did not have an effective monitoring process established to ensure compliance with their minimum security controls. Without the use of SSL, users' logon credentials could be compromised. If a user's logon credentials were compromised, unauthorized access [redacted] could occur.

FARS System Security Plan, Control SC-13, *Use of Cryptography*, states that the SSL should be used for the [redacted] applications.

NIST SP 800-46, *Security for Telecommuting and Broadband Communications*, Section 5.7, states, "Encryption is important for both data transmission and data storage. Encryption is critical for transmission whenever sensitive data is being transmitted over an insecure network such as the Internet. Encryption is important for storage whenever the data is subject to compromise."

***09-07 Recommendation***

We recommend that the CIO, with input from the Office of the DCFO, implement the use of SSL for the [redacted] applications.

***Management Response***

We agree with the recommendation. The Department will implement Transport Layer Security (TSL) to provide data encryption for the [redacted] applications. It is anticipated that this implementation will be completed during the second quarter of fiscal year 2010.

**EXHIBIT 1**

**U.S. DEPARTMENT OF THE TREASURY**

Fiscal Year 2009
Management Letter Report
Status of Prior Year Management Letter Comments

| **Prior Year Comments** | | **Current Year Status** |
|---|---|---|
| 08-01 | President's Budget Reconciliation (Repeat Comment) | This comment has not been corrected and is included in the FY 2009 Audit Report on the Treasury Department's financial statements as a significant deficiency that formed part of the material weakness titled "*Financial Management Practices at the Departmental Level (Repeat Condition)*." |
| 08-02 | Financial Reporting Standards for Treasury's Component Entities (Repeat Comment) | This comment has not been corrected and is repeated in the current year as comment 09-01. |
| 08-03 | Mortgage-backed Securities (MBS) Purchase Reconciliations | This comment has been corrected. |
| 08-04 | Disaster Recovery Procedures (Repeat Comment) | This comment has been corrected. |
| 08-05 | Database-level User Access | This comment has been corrected. |