



# Audit Report



OIG-15-020

Management Letter for the Audit of the Department of the Treasury's Fiscal Years 2014 and 2013 Financial Statements

December 12, 2014

Office of  
Inspector General

Department of the Treasury



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

OFFICE OF  
INSPECTOR GENERAL

December 12, 2014

**MEMORANDUM FOR SHARON A. KERSHBAUM  
ACTING ASSISTANT SECRETARY FOR MANAGEMENT**

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

**SUBJECT:** Management Letter for the Audit of the Department of the Treasury's Fiscal Years 2014 and 2013 Financial Statements

I am pleased to transmit the attached management letter in connection with the audit of the Department of the Treasury's (Department) consolidated financial statements for fiscal years 2014 and 2013. Under a contract monitored by the Office of Inspector General, KPMG LLP (KPMG), an independent certified public accounting firm, performed an audit of the Department's consolidated financial statements as of September 30, 2014 and 2013, and for the years then ended. The contract required that the audit be performed in accordance with generally accepted government auditing standards and Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*.

As part of its audit, KPMG issued, and is responsible for, the accompanying management letter that discusses certain matters involving internal control over financial reporting that were identified during the audit, but were not required to be included in the auditors' 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 and OMB Bulletin No. 14-02.

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

Attachment

cc: Dorrice C. Roth, Deputy Chief Financial Officer



KPMG LLP  
Suite 12000  
1801 K Street, NW  
Washington, DC 20006

December 10, 2014

Inspector General  
U.S. Department of the Treasury:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of the Treasury (Department), as of and for the year ended September 30, 2014, in accordance with auditing standards generally accepted in the United States of America, the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, we considered the Department's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

We did not audit the financial statements of the Internal Revenue Service and the Office of Financial Stability, component entities of the Department. Those statements were audited by other auditors.

During our audit we noted certain matters involving internal control and other operational matters that are presented below for your consideration. In addition, we and the other auditors noted additional matters that were reported separately to component management. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

#### **1. Improvements Needed in Change Management Oversight**

Departmental Offices (DO) was not able to provide a listing of system changes generated directly from two financial systems. In addition, DO did not fully segregate change management responsibilities over such financial systems, consistent with the National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53). DO stated that the financial systems do not have the ability to produce a system generated listing of changes made and DO does not utilize an external application to control the financial system changes. Separation of change management responsibilities helps prevent unauthorized changes to the financial systems.

#### **Recommendations**

We recommend that the Deputy Chief Financial Officer (DCFO) ensures that DO:

- a. Implements a process to log changes to the financial systems and procedures to resolve any unknown changes to the financial systems.



- b. Implements controls to prevent unapproved financial system changes. If preventative controls cannot be efficiently and effectively implemented, require an individual independent of the change implementation process to compare financial system changes to the approved changes to ensure unauthorized changes are not implemented.

### **Management Response**

The Department concurs with the comment and recommendations. In addition, the Department indicated that it believes several controls are already in place to help mitigate the risk of unauthorized changes identified in the comment above. The Department believes that the following controls have thus far prevented this risk from materializing.

- a. *Change Approval Controls*—Controls related to the approval of changes were designed by the financial system project manager within the DCFO's program office. These controls are currently performed by the project manager as well as the program offices whose business functions are supported by the financial systems.
- b. *System Change Management Controls*—These controls were designed within the Office of the Chief Information Officer (OCIO) and are performed by either OCIO staff or contractors as part of the change management process. Because these controls segregate duties (and related system access) within the process of developing and deploying the financial system changes, the risk of unauthorized changes is limited to one role in the change management process: the database administrator (DBA). This role is currently filled by one individual, a contractor. The Department believes that the system change management controls currently in place mitigate this risk.
- c. *Program Office Controls*—The Department believes that the program office's regular use of the financial systems will detect unauthorized changes after such changes are made. The Department indicated that the DCFO's program office rigorously reviews the system-generated financial statements before those financial statements are issued, whether they are draft statements issued internally or final statements issued to OMB and the public. The Department believes that unauthorized changes by a DBA would likely cause some of the DCFO program office's reconciliations to fail. The DCFO's program office would in turn raise the problem with financial system developers and the project team lead, and the unauthorized changes would be discovered and corrected.

The Department indicated that in order to strengthen existing internal controls over the financial system change management process, the project team will modify its current nightly audit process to generate a separate audit log file exclusively for tracking changes to the financial system objects. The current nightly audit process generates a file containing audit log data related to changes to both application data and financial system objects. The audit log files for a given week are currently reviewed by the DBA on a weekly basis. To improve the current process, the Department will generate audit data on changes to the financial system objects in a separate nightly audit log file. The Department will require the project team lead (OCIO contractor), in addition to the DBA,



to review these nightly object audit log files on a weekly basis for the purpose of detecting unauthorized changes within the financial system. The object audit log files will be saved for a retention period similar to that of the current nightly audit log file or longer. In total, the object audit log files will provide a change history for each financial system object.

This modified process will include procedures for bringing unauthorized changes to the attention of the project manager and correcting those changes. In addition to the Department's current capability to detect unauthorized changes during the releases to the financial system, the new process will better position the project team to detect unauthorized changes in between change releases to the financial system as well. The target completion date is December 15, 2014. As owner of the financial system, the DCFO's program office has worked with OCIO to design the improvements described above. The OCIO will implement these improvements and will continue to be responsible for performing the audit process.

In addition, the project team will research the acquisition and maintenance costs of third-party software products which might provide a more comprehensive solution. The Department's decision to purchase and implement such third-party software will be based on the Department's assessment of value and budget/resource availability.

## **2. Vulnerability Scan Evidence Not Readily Available**

DO was unable to provide supporting documentation evidencing the completion for one of the three monthly financial systems' vulnerability scans, as required by NIST SP 800-53. Specifically, DO indicated that the month of November 2013 had been completed; however, they were unable to locate evidence of such and the individual that performed the scan is no longer under contract to help locate such evidence. In addition, DO was unable to provide evidence that the vulnerability scans were reviewed for the three selected months of November 2013, January 2014, and April 2014.

### **Recommendations**

We recommend that the DCFO ensures that DO:

- a. Maintains documentation evidencing vulnerability scans in a location accessible to authorized individuals to avoid losses of documentation when individuals are on leave or separated.
- b. Reminds personnel to review the vulnerability scans and retain documentation demonstrating completion of the reviews.

### **Management Response**

The Department concurs with the comment and recommendations. The Department stated that DO's Cyber Security has enhanced its vulnerability scanning process by creating a centralized



Information Security Portal location on SharePoint that is accessible to authorized individuals to avoid losses of documentation when individuals are on leave or separated.

In addition, the DO's Cyber Security Organization will update the processes and procedures to ensure that the vulnerability scan data are reviewed by appropriate personnel, to include both system administrators and the Cyber Security Organization. DO has reassigned this responsibility for reviewing and storing vulnerability scan data to a Federal employee within the DO's Cyber Security Organization. This will ensure that the vulnerability scan data are available when individuals are on leave or are separated. The target completion date is January 31, 2015.

### **3. Inconsistent Review of Manual Journal Entries**

A supervisor within the Cash Accounting Division (CAD) of the Bureau of the Fiscal Service (Fiscal Service) did not review two deposit in transit manual journal entries in accordance with the CAD's Standard Operating Procedures (SOP). Section 7100 'Deposits in Transit Reconciliation Standard Operating Procedure,' of the SOP states that a reviewer should "review the journal vouchers, verify the information weekly and ensure that the entries are correct, sign the TFS Form 6606, and return the package to the staff member assigned to review the journal voucher Log file." Inadequate review and approval of journal entries increases the risk that material misstatements may not be prevented or detected and corrected in a timely matter.

#### **Recommendation**

We recommend that the DCFO ensures that the Fiscal Service reminds supervisors to review and approve all deposit in transit manual journal entries and document completion of such review in accordance with the SOP.

#### **Management Response**

The Department concurs with the comment and recommendation. The Department indicated that CAD Deposits in Transit Reconciliation process will be updated to reflect changes due to CARS becoming the system of record in fiscal year 2015, replacing STAR. The new procedures will be reviewed to ensure efficient and effective controls are embedded in the process. The new process requirements will be communicated to the CAD staff and supervisors, and the controls will be monitored to ensure compliance. The target completion date is on or before June 30, 2015.

### **4. Improvements Needed in the Internal Control Assessment Process**

The Department's guidance for assessing internal controls in accordance with Appendix A of Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, did not indicate that bureaus and offices should identify, document, and test the relevant user entity controls related to service organizations. In addition, the Department's guidance identifies information technology as a core financial process; however, the Department did not require DO to perform testing of information technology controls over two key financial reporting systems used to produce the Department's consolidated financial statements. The Department's



internal assessment and conclusions reached as part of the annual Secretary's Assurance Statement may not be accurate if the Department does not assess and test all key controls supporting such assessment and conclusions.

### **Recommendation**

We recommend that the DCFO ensures that the Department updates its guidance to require bureaus and offices to identify, document, and test the relevant user entity controls when using service organizations and information technology controls for all key financial systems.

### **Management Response**

The Department concurs with the comment and recommendation. The Department indicated that bureaus and offices that rely on other structured management reviews or examinations of third party providers are required to submit documentation on the review and approval of the IT process controls in accordance with the Department's guidance. It is the Department's intent that reporting entities also document and test the applicable user controls related to service organizations. However, this is not prescribed in the Department's guidance. The DCFO's program office will update the Department's FY 2015 guidance to include specific requirements for testing user controls related to service organizations.

The Department's guidance identifies technology controls as a core financial process. Although the identification, documentation, and testing of financial system controls are not specifically required of DO and bureaus by the Department's most recent guidance, the DCFO annual assurance statement process would consider any issues identified in the current testing and monitoring work. However, the DCFO's program office will update the Department's FY 2015 guidance to include specific requirements for testing key financial reporting systems used to produce the Department's consolidated financial statements.

\*\*\*\*\*

Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Department's organization gained during our work to make comments and suggestions that we hope will be useful to you. We would be pleased to discuss these comments and recommendations with you at any time.

The Department's responses to the deficiencies identified in our audit are described above. The Department's responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.



Office of Inspector General  
U.S. Department of the Treasury  
Page 6 of 6

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

**KPMG LLP**