Audit Report

OIG-08-024

Management Letter for the Fiscal Year 2007 Audit of the Department of the Treasury's Financial Statements

December 20, 2007

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

December 20, 2007

MEMORANDUM FOR PETER B. MCCARTHY
ASSISTANT SECRETARY FOR MANAGEMENT
AND CHIEF FINANCIAL OFFICER

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

SUBJECT: Management Letter for the Fiscal Year 2007 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 2007 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, 2007 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*; 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) 927-5768, or a member of your staff may contact Michael Fitzgerald, Director, Financial Audits at (202) 927-5789.

Attachment

DEPARTMENT OF THE TREASURY
FISCAL YEAR 2007

Management Letter Report

November 14, 2007

DEPARTMENT OF THE TREASURY

Fiscal Year 2007
Management Letter Report

Table of Contents

KPMG LLP
2001 M Street, NW
Washington, DC 20036

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

November 14, 2007

We have audited the consolidated financial statements of the U.S. Department of the Treasury (Department) for the year ended September 30, 2007, and we have issued our report thereon dated November 14, 2007. Our report indicated that we did not audit the amounts included in the consolidated financial statements related to the Internal Revenue Service (IRS), a component entity of the Department. The financial statements of the IRS were audited by another auditor whose report has been provided to us.

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

During our fiscal year (FY) 07 audit of the Department's consolidated financial statements, we and the other auditor noted certain matters involving internal control and other operational matters that we considered to be significant deficiencies under standards established by the American Institute of Certified Public Accountants (AICPA). A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the Department's internal control.

Our consideration of internal control would not necessarily disclose all matters in internal control that might be significant deficiencies. In our *Independent Auditors' Report* dated November 14, 2007, we reported the following matters involving internal control and its operation that we and the other auditor considered to be significant deficiencies:

- Financial Management Practices at the IRS (Repeat Condition)
- Information System Controls (Repeat Condition)
- Financial Management Practices at the Departmental Level

We consider the significant deficiency related to Financial Management Practices at the IRS, noted above, to be a material weakness. 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 Department's 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 offices or operating bureaus that were separately audited by other auditors.

Exhibit 1 provides the status of the 13 comments included in our management letter arising from our FY 06 audit. We have not considered the Department's internal control since the date of our report.

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

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

This communication is intended solely for the information and use of the management of the Department, the Department's Office of Inspector General (OIG), 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 2007 COMMENTS

07-01: President's Budget Reconciliation **(Repeat Comment)**

The Department of the Treasury's (Treasury/Department) Office of Performance Budgeting (OPB) prepares the annual reconciliation of Treasury's actual Budgetary Resources, Outlays, Offsetting Receipts, and Obligations Incurred reported in the President's Budget to comparable information contained in Treasury's Statement of Budgetary Resources (PB Reconciliation) for disclosure in Treasury's consolidated financial statements as required by Statement of Federal Financial Accounting Standards (SFFAS) No. 7, *Accounting for Revenue and Other Financing Sources*, and OMB Circular A-136, *Financial Reporting Requirements* (OMB Circular No. A-136). The PB Reconciliation is then provided to the Department's Office of Accounting and Internal Control (AIC) for final review and approval as well as inclusion in the Department's consolidated financial statements. The PB Reconciliation prepared for inclusion in the FY 07 consolidated financial statements revealed the following:

- Adequate management reviews were not performed on documentation provided to support PB Reconciliation audit requests. For example, the initial documentation provided to support the PB Reconciliation did not fully support certain reconciling amounts reported in the PB Reconciliation even though the documentation had been reviewed by both OPB and AIC officials prior to submission to auditors.
- In one instance, a schedule provided to support the PB Reconciliation reflected a mathematical error.
- Inadequate explanations were provided for the inclusion and classification of a reconciling item amounting to $129 million related to the U.S. Mint in the PB Reconciliation. Consequently, significant time was spent by the audit team in discussions with the component audit team as well as component management to clearly establish the rationale for the reconciling amount. This led to the reclassification of this item from that initially reported as a reconciling amount recorded in the section titled "Treasury's Statement of Budgetary Resources but not in the Treasury Chapter of the PB" to "Included in the Treasury Chapter of the PB but not in the Treasury's Statement of Budgetary Resources."

In response to questions raised, OPB officials provided additional documentation, revised the PB Reconciliation on two separate occasions to incorporate auditor requested changes, and assisted us with resolving the issues identified.

Improvements can be made to the process of preparing the reconciliation and expediting its review. Although differences identified were ultimately fully explained and supported, the initial supporting documentation provided was not comprehensive enough to eliminate the detailed discussions needed to understand the Department's unique budget transactions and how they contribute to the PB Reconciliation.

Section II.4.2 of OMB Circular No. A-136, states:

> "Agencies should discuss any material changes to budgetary information subsequent to the publication of the audited 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 notes to the SBR."

Section II.4.10.34 of OMB Circular No. 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. Since the financial statements are now published before the Budget, this reconciliation will be based on the SBR and Budget published in the prior year (e.g., fiscal year 2005 column on the SBR and the fiscal year 2005 actual column of the fiscal year 2007 Budget). The reporting entity should disclose that the President's Budget with actual numbers for the current fiscal year has not yet been published, explain when it is expected to be published, and indicate where it will be available…..Agencies should provide a schedule to display material differences between the SBR and Budget. At a minimum, agencies should display the material differences for comparable line items related to budgetary resources, obligations, distributed offsetting receipts and outlays."

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 adequacy of review issues identified above occurred mainly due to the fact that existing OPB and AIC senior staff work loads exceed what can be reasonably conducted by senior staff. Therefore, insufficient time is available to be spent on supervisory reviews, and other financial management activities. This situation has resulted in increased reliance being placed on the audit of the PB Reconciliation to identify errors and omissions.

Further, Treasury relies on the knowledge and skills of key experienced OPB officials at the Departmental level to prepare the PB Reconciliation each year. However, because the PB Reconciliation is performed at the Department level, the lack of intimate knowledge of component transactions contributed to the initial misclassification of budgetary resources for reconciliation purposes and significant time investment by the audit team to get the clarifications needed. This led to additional efforts to obtain documentation and increased time spent on the PB Reconciliation that, if the PB Reconciliation had been performed by each component, could have been minimized.

07-01 Recommendations

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

1. Ensure that adequate reviews are conducted by OPB and AIC officials on requested documentation to ensure that the documents and information being provided are accurate and complete; and

2. Instruct all Treasury components to reconcile their respective SBR amounts to what is included in the PB, and provide the operating procedures needed for the PB Reconciliation to the components. This will streamline the process, provide better detail and clarification of reconciling items, and reduce the significant time spent by Departmental staff. Once received, OPB and AIC should perform only a consolidation of the data. At the component level, management should classify amounts reported in the SBR and President's Budget by reconciling budgetary sources to fund symbols, along with an explanation for each reconciling item, and also explain what funds are included in the line item.

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

Policies and procedures developed should also include procedures for review and approval by appropriate component officials. Alternatively, the Departmental PB reconciliation should be shared with the bureaus prior to finalizing the PB reconciliation.

Management Response

Recommendation 1: The Department agrees with this recommendation. AIC and OPB will ensure that adequate reviews are conducted by responsible AIC and OPB officials on requested documentation to ensure that the documents and information being provided are accurate and complete.

Recommendation 2: While the Department agrees that the PB Reconciliation process can be improved, we have determined that the reconciliation should continue to be prepared at the Department level. AIC and OPB are looking into utilizing the CFO Vision application to prepare the Departmental reconciliation worksheet, which identifies bureau/component entity differences. By automating the initial reconciliation process as much as possible, OPB and AIC staff will be able to focus more time on explaining the differences and getting the supporting documents from the bureaus. We will consider sharing the Departmental reconciliation with the bureaus prior to finalizing the reconciliation. We will also improve management review of the reconciliation.

07-02: Financial Reporting Standards for Treasury's Component Entities **(Repeat Comment)**

The Department's consolidated financial statements are prepared in conformity with accounting principles prescribed by the Federal Accounting Standards Advisory Board (FASAB), the accounting standards-setting body for the Federal Government, as recognized by the AICPA in October 1999. However, certain Treasury 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 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 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. 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 SBR, although this statement is an integral part of the Department's consolidated financial statements, and must be prepared regardless of whether the component receives appropriations from the U.S. Government or not. Moreover, information reported in the Department's SBR must be reconciled to enacted amounts in the President's Budget and disclosed in the notes to the Department's consolidated financial statements. 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 Department's component entities.

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

07-02 Recommendation

We recommend that the CFO, with input from the Director, AIC work with the affected Treasury bureaus to achieve conformance during FY 08 so that all such reporting entities within the Department prepare their financial statements in accordance with Federal GAAP. 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. If 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

The Federal Accounting Standards Advisory Board (FASAB) has an active project that addresses this recommendation. The Department has provided information to FASAB regarding Treasury components and continues to monitor the progress of the FASAB project. We believe the Department should not take any additional action until FASAB completes the project. FASAB describes the project as follows (http://www.fasab.gov/projectsgaap.html):

"Since October 1999, the American Institute of Certified Public Accountants (AICPA) has recognized the Federal Accounting Standards Advisory Board (FASAB) as the standard-setting body for federal governmental entities; therefore, the pronouncements resulting from the FASAB process represent generally accepted accounting principles (GAAP) for the entire federal government (FASAB GAAP). Nevertheless, some federal entities follow GAAP for nongovernmental entities promulgated by the private sector Financial Accounting Standards Board (FASB GAAP). For example, federal government corporations, the US Postal Service, certain component entities of the Department of Treasury, and some smaller entities in the executive and legislative branches have historically applied FASB GAAP and continue to do so. The primary objective of this project is to consider the appropriate source of GAAP for federal entities."

07-03: Disaster Recovery Procedures **(Repeat Comment)**

A Disaster Recovery Plan (DRP) has not been developed for the Treasury Information Executive Repository (TIER) and the Chief Financial Officer Vision (CFO Vision) financial systems.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems*, states "Information Technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so

essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster." NIST SP 800-34 also states that 'IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire).'

Many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort; however, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions. NIST SP 800-12, *An Introduction to Computer Security,* states that "Contingency planning directly supports an organization's goal of continued operations. Organizations practice contingency planning because it makes good business sense. To avert potential contingencies and disasters or minimize the damage they cause, organizations can take steps early to control the event." Generally called contingency planning, this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses. Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization.

According to the Office of the Deputy Chief Financial Officer's (DCFO) office, funding was not made available in the FY 07 Treasury budget to develop a DRP; however, funding was submitted for the FY 08 budget. Development of the plan has begun, and the DCFO office has targeted June 30, 2008 to have the plan completed and tested.

Should a disaster occur without a documented DRP for TIER and CFO Vision, the DCFO office's ability to restore and/or continue operations related to these systems may be significantly delayed.

07-03 Recommendations

We recommend the DCFO's office continue in its efforts to:

1. Develop a DRP for the TIER and CFO Vision financial systems;

2. Test the DRP annually in accordance with the guidance outlined in NIST SP 800-34; and

3. Update the DRP following any changes made to the systems to ensure that the current version is available for recovery.

Management Response

Recommendations 1-3: The Department agrees with these recommendations and will continue efforts to: develop a Disaster Recovery Plan (DRP) for the TIER and CFO Vision financial systems, test the DRP annually, and update the DRP following any changes made to the systems to ensure the current version is available for recovery. A Hosting Study for enterprise applications is nearing completion and will provide input into a decision on the location of the disaster recovery site for enterprise applications, which will include DCFO FARS.

07-04: Documentation of Application-Level Changes

The DCFO office is not sufficiently documenting evidence of the completion of TIER application-level change management steps using the Software Change Request (SCR) process, as outlined in Section 3.2, "Operation and Maintenance" section, of the Treasury Application Systems Support Contract (ASSC) Systems Development Life Cycle (SDLC) Workflow and Processes Handbook v.2.1.5. In summary, the SDLC Workflow and Process Handbook require appropriate documentation of all program changes through the SCR process.

In addition, the NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that "Controls should be placed on system software commensurate with the risk. The controls should include authorization of system changes." This involves the protection of software and backup copies and can be done with a combination of logical and physical access controls.

TIER application programmers indicated that user testing approval and production migration authorization was obtained verbally and documentation was not consistently maintained. A lack of internal controls over the program change function could result in unauthorized and potentially inaccurate computer program changes being implemented into the production environment.

07-04 Recommendation

We noted that upon notification of this condition, the DCFO's office implemented a policy to obtain written approval for acceptance of all changes following user acceptance testing. However, we recommend that the DCFO's office provide additional oversight to ensure that all steps required by the SDLC Workflow and Process Handbook are consistently followed for all changes to the TIER application.

Management Response

As noted by the auditors, the DCFO's office implemented procedures to require formal, written acceptance of software testing results. The DCFO's office will provide additional oversight to ensure all steps required by the SDLC Workflow and Process Handbook are consistently followed for all changes to the TIER application. In addition, the CIO plans to modify the SDLC guidance to recognize different workflow approaches for a large planned release group of SCRs versus a single SCR for a minor data fix, bug fix, report change, etc.

07-05: User Account Passwords **(Repeat Comment)**

The user account and password configurations established in TIER do not meet the requirements outlined in the Financial Analysis and Reporting System (FARS) System Security Plan (SSP) or Treasury Directive Publication 85-01, Volume 1, *Treasury Information Technology Security Program*. Specifically, TIER has not been configured to (1) terminate active user sessions following 30 minutes of inactivity, (2) require the use of a password with alpha, numeric, and special characters, and (3) restrict password reuse.

The FARS SSP requires that "passwords are changed every 90 days; contain a minimum of 8 characters composed of alphanumeric, upper/lower case, and special characters; all passwords should be unique; passwords must not contain dictionary words pertaining to personnel data (e.g. user's name, date of birth, address, telephone number, social security number); and passwords are not to be reused."

Treasury Directive Publication 85-01, Volume I, *Treasury Information Technology Security Program*, indicates in Appendix A, Minimum Standard Parameters, items 21 and 22, that both users and privileged users should have idle sessions timed out following 30 minutes of inactivity for systems with a Federal Information Processing Standard 199 categorization of Moderate.

The DCFO office indicated that the TIER application was configured to verify that passwords contain at least one character that is not a letter; however, the application was not configured to verify that a special character or number was included in the password. The DCFO office further indicated that the current version of TIER has not been configured to end sessions following 30 minutes of inactivity. However, this issue will be resolved in version 7.1 due for release during FY 08.

Without proper configuration of passwords, the potential exists for an unauthorized user to gain access to the system. This could result in exposure, modification, and deletion of data.

07-05 Recommendations

We recommend that the DCFO's office:

1. Establish a session timeout for TIER following 30 minutes of inactivity;

2. Configure the TIER application to require passwords with complex characters (i.e., alphanumeric and special characters); and

3. Configure the TIER application to prohibit the reuse of passwords.

Management Response

Recommendation 1-2: The Department agrees with the recommendations to strengthen user account passwords, and has already completed the following actions to address recommendations 1 - 2 for TIER 7.1: established a session timeout for TIER, and configured TIER to require complex passwords.

Recommendation 3: The Department agrees with this recommendation and will coordinate with network contractors to change password configuration to prohibit the reuse of passwords.

07-06: System Security Plan

The FARS was assigned a Federal Information Processing Standard (FIPS) 199 rating of Moderate. However, the FARS SSP does not document all of the minimum security requirements for the moderate baseline, as outlined in the NIST Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems,* and as required by NIST SP 800-18, Revision 1, *Guide to Developing Security Plans for Federal Information Systems*. Specifically, 7 of the 124 baseline security controls required by NIST 800-53 to be addressed in the SSP of a system with a FIPS 199 rating of Moderate were not addressed in the FARS SSP. The 7 baseline security controls missing from the FARS SSP follows:

- AU – 11 – Audit Record Retention
- CM – 8 – Information System Component Inventory
- PE – 18 – Location of Information System Components
- PL – 6 – Security-Related Activity Planning
- SC – 20 – Secure Name/Address Resolution Service (Authoritative Source)
- SC – 22 – Architecture and Provisioning for Name/Address Resolution Service

- SC – 23 – Session Authenticity

NIST SP 800-18 requires the agency to implement a NIST SP 800-53 minimum security control baseline commensurate with the level of risk assessed for the information system. Each control in the baseline selected (i.e. low, moderate, or high) must be addressed as planned, in-place, or not applicable. For each control that is implemented or addressed (i.e. planning or not applicable) in the minimum security control baseline selected, NIST SP 800-18 states that the agency must include the following information in the SSP for each of the NIST SP 800-53 controls included in the baseline, (1) the security control title, (2) how the security control is being implemented or planned to be implemented, (3) any scoping guidance that has been applied and what type of consideration, and (4) indicate if the security control is a common control and who is responsible for its implementation.

These seven controls were inadvertently omitted from the FARS SSP during the recertification process. Without a detailed SSP that identifies all minimum baseline controls, the full extent of threats, risks, and vulnerabilities may not be known.

07-06 Recommendation

We recommend that the DCFO's office update the FARS SSP to include the seven baseline controls and document the status of each control, as required by NIST SP 800-18.

Management Response

The Department agrees with this recommendation and has already updated the FARS SSP to include all minimum baseline controls for a system with a FIPS 199 rating of moderate and identified the status of each control, as required by NIST SP 800-18.

07-07: Password Configurations

Password configurations within the CFO Vision application do not conform to the requirements set forth in the FARS SSP. Specifically, CFO Vision has not been configured to require passwords to be changed every 90 days and not be reused.

The FARS SSP requires that "passwords are changed every 90 days; contain a minimum of 8 characters composed of alphanumeric, upper/lower case, and special characters; all passwords should be unique; passwords must not contain dictionary words pertaining to personnel data (e.g., user's name, date of birth, address, telephone number, social security number); and passwords are not to be reused."

The authentication mechanism for the CFO Vision application is tied to the server providing authentication services for the Departmental Offices Human Resource Connect (HR Connect) application. Currently, this configuration change is being reviewed and is expected to be modified to conform to the requirements documented in the FARS SSP during FY 08.

Without the proper configuration of passwords, the potential exists for an unauthorized user to gain access to the system.

07-07 Recommendations

We recommend that the DCFO's office:

1. Configure the CFO Vision application to require users to change passwords every 90 days; and

2. Configure the CFO Vision application to prohibit the reuse of passwords.

Management Response

Recommendation 1: The Department agrees with this recommendation and has already implemented the requirement for CFO Vision users to change their passwords every 90 days.

Recommendation 2: The Department agrees with this recommendation and will coordinate with network contractors to change password configuration to prohibit the reuse of passwords.

07-08: Plan of Action and Milestones Reporting

Prior year IT audit findings and recommendations were not included in the Treasury Departmental Offices Plan of Action and Milestones (POA&M).

OMB M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, states that POA&Ms must "…include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations."

The DCFO's office indicated that they were unaware of the requirement to include all audit findings and recommendations in the POA&M.

By not properly identifying all known weaknesses from all sources in the POA&M and tracking the status of each, the DCFO's office may not be adequately addressing the security weaknesses identified for the FARS.

07-08 Recommendation

We recommend that the DCFO's office follow OMB guidance and include all reported IT weaknesses from all sources in the POA&M and track the status of each weakness through to resolution.

Management's Response

The Department agrees with this recommendation and will start to enter all reported IT weaknesses from all sources in the POA&M and track their status through resolution.

07-09: User Access Policies and Procedures

The policies and procedures outlined in Treasury Directive Publication 85-01, Volume 1, *Treasury Information Technology Security Program,* for granting user access to information systems are not being consistently followed. Specifically, out of the nine new Treasury Information Executive Repository (TIER) users and the three new Chief Financial Officer Vision (CFO Vision) users selected, Financial Analysis and Reporting System (FARS) Access Request Forms were not available for two new TIER users and one new CFO Vision user.

Treasury Directive Publication 85-01 - Volume I, states that managers and supervisors should, "…review and authorize privileges for personnel and review user security agreements on at least an annual basis to

verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., systems authorized for access and type)."

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook, Chapter 10.2 User Administration*, states that "User account management involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions." In addition, it states that "User account management typically begins with a request from the user's supervisor to the system manager for a system account. If a user is to have access to a particular application, this request may be sent through the application manager to the system manager. This will ensure that the systems office receives formal approval from the "application manager" for the employee to be given access. The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile. (Often when more than one employee is doing the same job, a "profile" of permitted authorizations is created.)"

Regarding the TIER user accounts without a FARS Access Request Form, a Treasury ASSC contractor with system development responsibilities created two user accounts within TIER to test functionality in the new TIER release. However, a form was never initiated to document the creation of these accounts.

Regarding the CFO Vision user account without a FARS Access Request Form, the DCFO's office indicated that the user was recertified during the fiscal year, and therefore, the access was approved by management. However, a form was never completed and maintained on file for the creation and initial authorization of this account.

By not properly documenting and authorizing the request for user access to an information system, there is the risk that unauthorized individuals could be inappropriately granted access to a system.

07-09 Recommendation

We recommend that the DCFO's office ensure that all users granted access to TIER or CFO Vision attain the necessary approvals and have a final FARS Access Request Form maintained on file in accordance with Treasury Directive Publication 85-01.

Management's Response

For a number of years, the Department has conducted an annual FARS user recertification to verify that only properly authorized users continue to have access to FARS applications. The instances of noncompliance with Treasury Directive 85-01 cited in the audit report were unique instances where new users were granted access to FARS only for test purposes. We acknowledge, however, that there are some weaknesses in our controls. The DCFO's office will review and update, as appropriate, existing procedures for granting FARS access to ensure that all users granted access to TIER or CFO Vision attain the necessary approvals and that the DCFO maintains a final FARS Access Request Form on file for each user in accordance with TD 85-01.

07-10: Segregation of Duties **(Repeat Comment)**

As noted in the prior year, the segregation of various duties are not being properly enforced within the TIER production environment. We noted that Treasury's TIER development contractors had been granted excessive access to the application. Specifically, during FY 2007, efforts were taken to remove the TIER TIER_USER_MANAGER role from three TIER development contractors; however, one retained access. In addition, several other issues related to segregation of duties within the TIER application were identified. Specifically:

- Two development contractors have been granted access to the TIER_ADMIN, TIER_ZAP, and TIER_FUND roles. Of these two contractors, one is also the development contractor noted above with TIER_USER_MANAGER role.

- Two other development contractors have been granted access to the TIER_ADMIN role.

NIST Special Publication 800-53, Revision 1, *Recommended Controls for Federal Information Systems*, states that, "…the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions."

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

07-10 Recommendation

This issue was brought to the attention of the DCFO's office during the course of fieldwork. Corrective actions were undertaken by removing the inappropriate access levels noted above. Therefore, no further corrective action is necessary.

Management's Response

The Department, as noted above, has already completed the removal of access levels from individuals with development access so they cannot create, modify, or delete TIER data or accounts.

07-11: Individual User Accountability

Individual user accountability is not being enforced on the Oracle database management system that supports TIER. Specifically, two database administrators share the Oracle accounts TREASDBA, sys, system, and sysman.

NIST Special Publication (SP) 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that, "Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability…Access control usually requires that the system be able to identify and differentiate among users…User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users."

Due to system limitations in the Oracle database management system, the system accounts "sys", "system", and "sysman" must be shared between two (2) individuals. These are default Oracle accounts and are used for system maintenance functions. However, the passwords for these three (3) accounts, as well as several others, are stored in Version Manager and are accessible by five (5) individuals. The database administration account "TREASDBA" is not specific to Oracle, and duplication of this account

is not bound by system limitations. The DCFO's office has created this one account to be shared between the two database administrators.

The use of shared user accounts removes individual accountability from the information system, thus making it difficult to hold a specific user accountable for actions performed. This situation is exacerbated when the shared account has system administration roles.

07-11 Recommendation

We recommend that the DCFO's office either create separate accounts for each database administrator to allow for individual accountability or implement alternative individual user accountability mechanisms.

Management's Response

The Department agrees with this recommendation and has already created separate accounts for the database administrators and disabled and deleted their shared Oracle account. In addition, as part of the Department's continuity of operations business requirements, the Office of the Chief Information Officer will develop a process to allow adequate backup of database administrators in their absence and still provide individual user accountability mechanisms.

EXHIBIT 1

DEPARTMENT OF THE TREASURY

Fiscal Year 2007
Management Letter Report
Status of Prior Year Management Letter Comments

Prior Year Comments		Current Year Status
06-01	Succession Planning	This comment has not been corrected and is reported in the FY 07 Audit Report on the Department's financial statements as a control deficiency that formed part of the significant deficiency titled "*Financial Management Practices at the Departmental Level*."
06-02	Financial Reporting Standards for Department Component Entities	This comment has not been corrected and is repeated in the current year as comment # 07-02.
06-03	The Exchange Stabilization Fund's Budgetary Accounting Methodology	This comment has been closed in view of management's communications with OMB in FY 07.
06-04	Financial Reporting Practices at the Department Level	This comment has not been corrected and is included in the fiscal year 2007 Audit Report on the Department's financial statements as a control deficiency that formed part of the significant deficiency titled "*Financial Management Practices at the Departmental Level*."
06-05	OMB Circular A-123, Management's Responsibility for Internal Control	This comment has not been corrected and is included in the fiscal year 2007 Audit Report on the Department's financial statements as a control deficiency that formed part of the significant deficiency titled "*Financial Management Practices at the Departmental Level*."
06-06	Intragovernmental Transactions and Activities	This comment has been corrected.
06-07	Performance Measures	This comment has been corrected.
06-08	Deferred Maintenance	This comment has been corrected.
06-09	Backup Tapes for the TIER System and CFO Vision Production Servers	This comment has been corrected.
06-10	Continuity of Operations Plan and Disaster Recovery Procedures for TIER and CFO Vision	This comment has not been corrected and is repeated in the current year as comment # 07-03.
06-11	Segregation of Duties	This comment has not been corrected and is repeated in the current year as comment # 07-10.
06-12	User Account Passwords	This comment has not been corrected and is repeated

Prior Year Comments		Current Year Status
		in the current year as comment # 07-05.
06-13	User Accounts	This comment has been corrected.