Audit Report

OIG-12-028

Management Letter for the Audit of the Office of the Comptroller of the Currency's Fiscal Years 2011 and 2010 Financial Statements

December 16, 2011

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

December 16, 2011

MEMORANDUM FOR JOHN WALSH
ACTING COMPTROLLER OF THE CURRENCY

FROM: Michael Fitzgerald
Director, Financial Audits

SUBJECT: Management Letter for the Audit of the Office of the Comptroller of the Currency's Fiscal Years 2011 and 2010 Financial Statements

I am pleased to transmit the attached management letter in connection with the audit of the Office of the Comptroller of the Currency's (OCC) Fiscal Years 2011 and 2010 financial statements. Under a contract monitored by the Office of Inspector General, GKA, P.C. (GKA), an independent certified public accounting firm, performed an audit of the financial statements of OCC as of September 30, 2011 and 2010 and for the years 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, GKA issued and is responsible for the accompanying management letter that discusses certain matters involving internal control over financial reporting and its operation that were identified during the audit, but were not required to be included in the auditor's reports.

In connection with the contract, we reviewed GKA's letter and related documentation and inquired of its representatives. Our review disclosed no instances where GKA 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

gka, p.c.
Certified Public Accountants
& Consultants

1015 18th Street, NW
Suite 200
Washington, DC 20036
Tel: 202-857-1777
Fax: 202-857-1778
www.gkacpa.com

OFFICE OF THE COMPTROLLER OF THE CURRENCY
MANAGEMENT LETTER
FISCAL YEAR 2011

October 31, 2011

Member of the American Institute of Certified Public Accountants

gka, p.c.
Certified Public Accountants
& Consultants

www.gkacpa.com

Inspector General, Department of the Treasury, and
the Comptroller of the Currency:

We have audited the balance sheet as of September 30, 2011 and the related statements of net cost, changes in net position, and budgetary resources for the year then ended, hereinafter referred to as “financial statements”, of the Office of the Comptroller of the Currency (OCC) and have issued an unqualified opinion thereon dated October 31, 2011. In planning and performing our audit of the financial statements of the OCC, we considered its internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide assurance on internal control. We have not considered the internal control since the date of our report.

During our audit we noted certain matters involving OCC’s information technology general controls that are presented in this letter for your consideration. The comments and recommendations, all of which have been discussed with the appropriate members of OCC management, are intended to improve OCC’s information technology general controls or result in other operating efficiencies.

OCC management’s responses to our comments and recommendations have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we do not express an opinion or provide any form of assurance on the appropriateness of the responses or the effectiveness of any corrective action described therein.

We appreciate the cooperation and courtesies extended to us during the audit. We will be pleased to meet with you or your staff, at your convenience, to discuss our report or furnish any additional information you may require.

GKA, P.C.

October 31, 2011

Improvements Needed in Information Technology General Controls over OCC's Financial Systems (Repeat Condition).

In our fiscal year (FY) 2010 audit, we identified weaknesses in the areas of entity-wide security management and contingency planning controls, and configuration management. We reported these weaknesses to management in a management letter. In FY 2011, these two issues identified in the prior years remain partially unresolved. In addition, three new findings related to access controls, contingency planning and configuration management were identified.

The weaknesses noted in OCC's IT general controls are noted and discussed below.

(A) <u>Security Management and Contingency Planning</u>

OCC's process for updating its Certification and Accreditation (C&A) documentation needs improvement. (Repeat Condition).

As noted during our prior year audit, OCC's process for updating its Certification and Accreditation (C&A) documentation needs improvement. Specifically, we noted the following:

- The $MART Systems Security Plan (SSP) version 5.0 is not updated to meet NIST 800-18 Revision 1 requirements. Specifically, we noted the following:
  - The $MART SSP does not describe how each security control is being implemented or planned to be implemented;
  - The $MART SSP does not identify the scoping guidance that has been applied to the security controls
  - The $MART SSP does not identify any of the agency-defined parameters in the security controls
  - The $MART SSP does not describe how the common controls are implemented or who is responsible for their implementation.
  - The $SMART SSP does not accurately document the $MART operating environment. Page Seven of the plan states that $MART is a commercial off the shelf (COTS) application customized for the OCC and is based on PeopleSoft Financials version 8.49. However $MART currently uses PeopleSoft Financials version 8.9.

- The Network Infrastructure (NI) General Support System (GSS) Systems Security Plan (SSP) has not been updated to reflect the OCC's current operating environment or the NIST 800-53 Revision 3 controls.

Specifically, we noted the following:

  - Several NIST 800-53 Revision 3 controls are not accurately reflected in the NI GSS SSP. For example, the AC-12, *Session Termination*, and AC-13, *Supervision and Review—Access Control*, have been withdrawn from 800-53 Revision 3, but are still documented within the SSP.
  - The "organizationally-defined" frequencies and values defined by NIST 800-53 Revision 3 have not been documented within the NI GSS SSP. Additionally, the Compliance descriptions do not address whether the "organizationally-defined" controls are in place or planned. For example the RA-5 control does not address the organizationally-defined timeframe for remediating security vulnerabilities
  - Section 1.6.2, *System Interconnections/Information Sharing*, has not been updated to reflect accurate agreement dates for the Memorandum of Understanding and Interconnection Security Agreements in place.
  - Section 1.8, *Privacy Impact Assessment*, states that, the NI GSS Privacy Impact Assessment (PIA) was revised and reviewed in October 2008, but has not been approved as of the date of this document. However, we noted that the NI GSS PIA was actually completed and approved.
  - Section 2.3.4, *Risk Assessment (RA-3)*, has not been updated with the current Risk Management Framework information such as the October 2009 Certification and Accreditation information.
  - Section 3.4.2, *Contingency Plan (CP-2)*, states that the OCC Information Technology Disaster Recovery Plan (ITRP), dated April 4, 2008, serves as the Contingency Plan for the Network Infrastructure GSS; however there is an updated version of the ITRP currently in place.

- The $MART Contingency Plan has not been updated to reflect the current $MART environment or NIST 800-34 Requirements. Specifically, we noted the following:
  - The $MART Contingency Plan does not contain procedures for recovering the $MART system in a disaster situation. Additionally, the recovery procedures are not documented in the ITRP.
  - The $MART Contingency Plan has not been updated to reflect the upgrade from PeopleSoft 8.4 to PeopleSoft 8.9.

- Network Infrastructure (NI) General Support System (GSS) Contingency Plan has not been updated to reflect the NI environment or NIST 800-34 Requirements. Specifically, we noted the following:
  - The NI GSS Contingency Plan does not contain procedures for recovering the NI system in a disaster situation. Additionally, the recovery procedures are not documented in the ITRP.

  - NI GSS Contingency Plan states, "IBM Compatible 2013 Amdahl Mellenium Mainframe running ZOS .14 Operating System is planned for decommission by 2008"; however there was no evidence available to show that this had actually occurred.
  - The NI GSS Contingency Plan states that the planned migration to Dell EMC Storage Area Network (SAN) is set for 2007; however, the Dell EMC migration has been completed and the NI GSS Contingency Plan has not been updated to reflect the migration.

- The $MART Security Assessment Report was not updated to reflect the upgrade from PeopleSoft 8.4 to PeopleSoft 8.9

The current process for updating certification and accreditation documentation as changes occur in the OCC environment is not effective. As a part of the update of the $MART SSP, details were taken out that made the plan inconsistent with NIST 800-18 requirements. Also, OCC has not updated the system security plans for its major application and general support system to address the NIST 800-53 Revision 3 controls. Additionally, OCC created a database to house its procedures for recovering information systems in disaster situations; however the procedures were not incorporated into the contingency plans for the $MART system or the Network Infrastructure.

The Planning Section of NIST 800-18 *Guide for Developing Security Plans for Federal Information Systems* Revision 1, states the following:

- "The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system."
- "The system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan also may reference other key security-related documents for the information system such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, security configuration checklists, and system interconnection agreements as appropriate."
- "An agency must meet the minimum security requirements in this standard by applying security controls selected in accordance with NIST SP 800-53 and the designated impact levels of the information systems. An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include: (i) the application of scoping guidance; (ii) the specification of compensating controls; and (iii) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities."

- "For efficiency in developing system security plans, common security controls should be documented once and then inserted or imported into each system security plan for the information systems within the agency. The individual responsible for implementing the common control should be listed in the security plan."
- "System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made. The application of scoping guidance must be reviewed and approved by the authorizing official for the information system."

The Planning Section of NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, states the following:

> "Control: The organization:
> a. Develops a security plan for the information system that:
> - Is consistent with the organization's enterprise architecture;
> - Explicitly defines the authorization boundary for the system;
> - Describes the operational context of the information system in terms of missions and business processes;
> - Provides the security category and impact level of the information system including supporting rationale;
> - Describes the operational environment for the information system;
> - Describes relationships with or connections to other information systems;
> - Provides an overview of the security requirements for the system;
> - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
> - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
>
> b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and
> c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments."

The Contingency Planning Section of NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, states the following:

> "Control: The organization:
> a. Develops a contingency plan for the information system that:
> - Identifies essential missions and business functions and associated contingency requirements;
> - Provides recovery objectives, restoration priorities, and metrics;
> - Addresses contingency roles, responsibilities, assigned individuals with contact information;
> - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
- Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*];
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];
e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and
f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]."

The Security Assessment and Authorization Section of NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, states the following:

"Control: The organization:
a. Develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;"

Over time, policies and procedures may become inadequate because of changes in threats, changes in operations or deterioration in the degree of compliance. Failure to update certification and accreditation documentation increases the probability that OCC management may not be aware of how system and environmental changes impact the OCC's ability to recover from disaster situations. Additionally, risks may not be adequately identified and corresponding controls implemented to address those risks.

RECOMMENDATIONS:

We recommend the following:

1. OCC management implement a process to ensure that C&A documentation is updated timely in accordance with OCC policy and ensure that approvals are documented on file.
2. Additionally, OCC should ensure that the information contained in the C&A documentation is accurate and reflects the current system operating and organizational environment.

3. OCC management should ensure that the $MART SSP is consistent with NIST 800-18 requirements

MANAGEMENT RESPONSE:

Management concurs with the Finding and Recommendations. OCC management is in the process of taking corrective action, reincorporating control implementation into the current $MART System Security Plan, in order to bring it back into compliance with NIST *Special Publication 800-18: Guide for Developing Security Plans for Federal Information Systems*.

1) OCC management ensured that all noted updates to the Network Infrastructure (NI)-General Support System (GSS) operating environment were incorporated in the annual System Security Plan review completed on October 29, 2011.

Additionally, OCC management will:

2) Evaluate the NI-GSS documents and ensure that documentation utilizes controls outlined in NIST *Special Publication 800-53 Revision 3: Recommended Security Controls for Federal Information Systems and Organizations*, to include documented "organizationally-defined" frequencies and values;
3) Review the $MART System Security Plan, Contingency Plan, and Security Assessment Report to ensure that the current system operating environment is documented to reflect the upgrade of PeopleSoft to version 8.9; and
4) Update the NI-GSS Contingency Plan and $MART Contingency Plans to reflect the accurate operating environments of each system and to ensure they reference the correct procedures for recovering the system in the event of a disaster.

(B) Access Controls

Weaknesses in the OCC's process for managing service accounts.

Specifically, we noted the following:

- Seventy-seven service accounts on the OCC network had never logged on to the network or had not logged on for more than one year; however there was no evidence that these accounts had been reviewed to determine whether or not they were still necessary.
- Twenty-five active service accounts on the OCC network whose passwords have been set to Never Expire; however, there was no evidence that their passwords had been changed on an annual basis in accordance with OCC requirements.
- There was no evidence that service accounts on the SQL Server database supporting the $MART application had been reviewed to determine whether or not they were still necessary.
- One service account on the SQL Server database supporting $MART was identified as having database administrator privileges. OCC policy states that service accounts must not be granted administrator privileges.

OCC currently does not have a process in place for periodically reviewing service accounts for appropriateness. Additionally, network passwords are not being changed for service accounts in accordance with OCC policy.

The *OCC Master Security Controls Catalog*, states the following:

- ”The OCC manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [monthly].”
- “The information system automatically disables inactive accounts after no more than [90 days].”

OCC Information Technology Services Directive, *AC: Account Management, 01-02, version 090707*, states

- Information Technology Services (ITS) is solely responsible for the issuance and control of all Service Accounts that permit access to OCC information systems and databases. ITS shall designate appropriate individuals within ITS (FTEs as well as contractors) to manage the appropriate Service Accounts (such SQL server, Sybase Server, SIS Application Services, WISDM Application Services).
- OCC Service Accounts must be dedicated to a specific, documented task, and are not issued for general purposes

- OCC Service Accounts must be granted the minimum necessary privileges to perform the specific, documented task. ITS holds and maintains documentation on the requirements for every Service Account.
- OCC Service Accounts must not be granted administrator privileges
- ITS shall maintain a current list of all OCC Service Accounts. This list will be made available only on a need-to-know basis to authorized personnel. A list of accounts will be made available to the OCC Computer Incident Response Center (CIRC) so that compliance with the password standard can be monitored monthly.
- Service Account passwords must be reset after one year, at the departure of any staff member with knowledge of the password, or when an application is moved into the production environment.

Without an adequate process for periodic review of service accounts and passwords, unauthorized or unnecessary users may have access permissions to OCC systems and data.

RECOMMENDATIONS:

We recommend the following:

1. OCC management ensure that service accounts are periodically reviewed for appropriateness.
2. OCC ensure that passwords for service accounts are changed in accordance with OCC policy.

MANAGEMENT RESPONSE:

Management concurs with the Finding and Recommendations. OCC management will update policies and procedures related to the management of Service Accounts, ensuring alignment with relevant guidance and best practices. Additionally, OCC management will train appropriate staff in policies and procedures associated with Service Account management and will enhance the current account management program to more closely monitor Service Account compliance with applicable policies.

(C) Contingency Planning

Backup tapes have not been tested on a quarterly basis for $MART and the Network Infrastructure to ensure their viability, reliability and integrity in the event of a disaster.

OCC informed us that backup tapes are tested on a semi-annual basis as a part of the functional disaster recovery testing. However, testing had not occurred this year as of August 31, 2011 because of contract negotiations with the alternate site provider IBM. OCC conducted a backup tape test as a part of a disaster recovery test in late September.

The *OCC Master Security Controls Catalog*, states the following:

- "OCC tests backup information on a quarterly basis to verify media reliability and information integrity."

Lack of adequate testing of backups increases the risk that OCC may not be able to recover backup data in a disaster situation.

RECOMMENDATION:

1. We recommend that OCC periodically test backup tapes in accordance with OCC policy.

MANAGEMENT RESPONSE:

Management concurs with the Finding and Recommendation, noting exception with elements of the condition. OCC Server and Storage Operations (SSO) conducts regular restoration of servers that comprise the Network Infrastructure-General Support System. Since the beginning of the calendar year, SSO has conducted ninety nine server recoveries, without failure. As noted in the Notification of Finding and Recommendation, OCC conducted a disaster recovery exercise, to include testing of the reliability of $MART backup media, prior to the end of the fiscal year. Management will evaluate current OCC media testing procedures and policy to ensure compliance with NIST guidance and Treasury Department directives, and will take prudent steps to ensure the reliability of backup media.

(D) Configuration Management

OCC's controls for configuring information systems in accordance with documented baseline configurations need improvement.

Specifically, we noted the following:

- $MART MS SQL Server 2005 TCP port is set to 1433. However, the MS SQL Server 2005 baseline configuration states that SQL Server TCP Ports should be set to something other than 1433 and 1434.

- The Default Domain Policy settings are not consistent with the Baseline Configuration Settings for the Windows Server 2003. Specifically, the following settings were not consistent with the documented baseline:
  - Minimum Password Length
  - Maximum password Age
  - Enforce Password History
  - Account lockout duration
  - Audit Logon Events
  - Audit Privilege Use
  - Audit Object Access

OCC had not updated its system configurations and documented baselines to ensure that system settings are consistent with the approved baselines

The *OCC Master Security Controls Catalog*, states the following:

- The OCC develops, documents, and maintains a current baseline configuration of the information system.
- The OCC updates the baseline configuration of the information system as an integral part of information system component installations.

The Configuration Management Section of NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, states the following:

"Control: The organization:

a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;

c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures."

Due to these weaknesses, system security configurations may not be adequately configured to mitigate risks to OCC's environment. This increases the risk that individuals may exploit vulnerabilities to obtain inappropriate access to OCC systems and data thus putting OCC systems at risk of inadvertent or deliberate disclosure, modification, or destruction.

RECOMMENDATION:

1. We recommend that OCC management ensure that OCC system configurations are consistent with the approved baselines.

MANAGEMENT RESPONSE:

Management concurs with the Finding and Recommendation, noting exception with elements of the condition. Based on internal review of policy compliance scans of $MART servers, OCC management notes that several policy deviations referenced in the condition do not exist on $MART servers. OCC management will review current configurations and documented baselines to ensure compliance with relevant industry best practices and standards, and applicable agency policy. OCC management will also evaluate the process for identifying, documenting, and approving deviations from documented baseline configurations.

Users have administrative rights to install personal or public domain software on their desktops. (Repeat Condition).

As noted during the prior year audit, although a process for removing and detecting unauthorized software is implemented as compensating controls, the controls do not fully mitigate the weakness. Users still have administrative rights to install personal or public domain software on their desktops.

OCC suspended the implementation of the Beyond Trust (BT) Project in anticipation of migrating all user workstations to Windows 7. According to OCC, Windows 7 will allow OCC to remove administrative privileges while still giving applications the necessary permissions to execute. OCC also plans to establish a software white list to prevent the installation of unauthorized software.

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Revision 3 states:

"Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect)."

The use of unapproved software by employees could negatively impact processing operations, introduce harmful viruses, and/or cause the loss of data.

RECOMMENDATION:

1. We recommend that OCC management continue with its plan to implement a software solution to restrict users from installing and executing unauthorized software on OCC workstations.

MANAGEMENT RESPONSE:

Management concurs with the Finding and Recommendation. The OCC has elected to address this issue as a part of upcoming technology refresh activities that are scheduled for FY2012. OCC management has elected to deploy a United States Government Configuration Baseline (USGCB) compliant Windows 7 desktop image with an enterprise application control solution and standard user rights, replacing the current Windows XP image with local administrator rights. This strategy will leverage existing large-scale projects to address this weakness, and will limit identified risks associated with such a far reaching project. Until such time that this image is deployed, OCC management will continue to dedicate resources to enhance the detective compensating controls in place to limit risk associated with the install of unauthorized software.