



# Audit Report



OIG-11-046

Management Letter for the Audit of the Office of the Comptroller of the Currency's Fiscal Years 2010 and 2009 Financial Statements

December 07, 2010

## Office of Inspector General

### Department of the Treasury

This report has been reviewed for public dissemination by the Office of Counsel to the Inspector General. Information on pages 2 through 4 requiring protection from public dissemination has been redacted from this report in accordance with Exemption 2 of the Freedom of Information Act, 5 U.S.C. Section 552.



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

OFFICE OF  
INSPECTOR GENERAL

December 07, 2010

**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 2010 and 2009  
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 2010 and 2009 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, 2010 and 2009 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



Certified Public Accountants | Management Consultants

**OFFICE OF THE COMPTROLLER OF THE CURRENCY  
MANAGEMENT LETTER  
FISCAL YEAR 2010**

**October 29, 2010**

*Member of the American Institute of Certified Public Accountants*

*1015 18th Street, NW · Suite 200 · Washington, DC 20036 · Phone: 202-857-1777 · Fax: 202-857-1778 · [WWW.gkacpa.com](http://WWW.gkacpa.com)*

1015 18th Street, NW  
Suite 200  
Washington, DC  
20036

Phone: 202-857-1777  
Fax: 202-857-1778  
Website: [www.gkacpa.com](http://www.gkacpa.com)

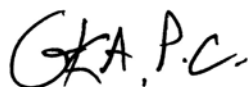
Inspector General, Department of the Treasury, and  
the Comptroller of the Currency:

We have audited the balance sheet as of September 30, 2010 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 29, 2010. 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.

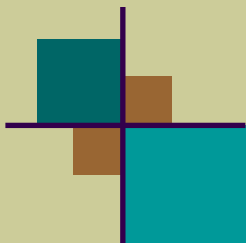
During our audit we noted certain matters involving OCC's information technology general controls that are presented in this letter for your consideration. The comments and recommendations, all of which have been discussed with the appropriate members of OCC management, are intended to improve OCC's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



October 29, 2010



**Office of the Comptroller of the Currency**  
**Management Letter Comments and Recommendations**  
**Year Ended September 30, 2010**

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

In our fiscal year (FY) 2009 audit, we identified weaknesses in the areas of entity-wide security management and contingency planning, access controls, and configuration management. We reported these weaknesses to management in a management letter. In FY 2010, OCC made significant progress in resolving these weaknesses, as evidenced in OCC's Plan of Actions and Milestones (POA&M) and our verification of correction of many of the prior year issues. Two (2) out of five (5) issues identified in the prior years remain partially unresolved. There were no new findings for FY 2010.

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

**(A) Security Management and Contingency Planning**

An entity wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks.

Contingency planning safeguards against losing the capacity to process, retrieve, and protect information maintained electronically, which significantly affect an agency's ability to accomplish its mission.

**1. There are weaknesses in the OCC's process for updating its Certification and Accreditation (C&A) documentation.**

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

- The Network Infrastructure General Support System (NI GSS) Information Technology Recovery Plan (ITRP) dated July 21, 2008 has not been updated to reflect the current NI GSS environment. Specifically, we noted the following:
  - There is no evidence that the NI GSS ITRP has been updated to reflect the lessons learned from the recent ITRP disaster recovery tests that was performed in August 2009.
  - The NI GSS ITRP, July 21, 2008, Pg. 17, paragraph 1, states that planned migration to [REDACTED] is planned for 2007. However, the [REDACTED] migration has been completed and the ITRP has not been updated.
  - NI GSS ITRP states that, pg. 17 states, "IBM Compatible [REDACTED] Mainframe running [REDACTED] Operating System is planned for decommission by 2008". However, it is not clear from our review of the ITRP if this has occurred.

**Office of the Comptroller of the Currency**  
**Management Letter Comments and Recommendations**  
**Year Ended September 30, 2010**

- NI GSS ITRP: Section 6.32: Pg. 74 states that, “an updated copy of the ITRP is distributed quarterly to key personnel including 2 Resident Technical Support Specialist in the Southern and Western Districts”. However, we could not confirm that this is being done.
- The \$SMART IT Contingency Plan (ITCP or CP) has not been updated to reflect changes to the \$SMART operating environment. Although the \$SMART critical applications were listed, one application the [REDACTED] does not reflect the current \$SMART computing environment. [REDACTED] was upgraded to [REDACTED] in FY 2009.

While the \$SMART ITCP was updated to incorporate reference to [REDACTED] in Section 6 (System Description), it still had outdated references to [REDACTED] in the context of references to team representation (page 18, table 7-3), recovery goals (page 25, table 15-1), application support team (page A-1, table A-3), required applications (page I-4, table I-2), and strategic recovery objectives (page I-20, table I-11). Once notified of this issue, OCC management updated the \$SMART ITCP before the end of our field work. Additionally, we noted that OCC was in the process of reviewing and updating the NI GSS ITRP.

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

“The OCC reviews the contingency plan for information systems (annually) and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.”

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 contingency plans increases the probability that OCC management may not be aware of how system changes impact the OCC’s ability to recover from disaster situations.

**Recommendations:**

We recommend that OCC management:

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

**Management’s Response:**

Management concurs with the finding and recommendations. IRM will ensure timely and accurate updates to C&A documentation by implementing a documented process to review the status of C&A documentation in TAF (Trusted Agent FISMA). Quarterly artifacts reports will be

**Office of the Comptroller of the Currency**  
**Management Letter Comments and Recommendations**  
**Year Ended September 30, 2010**

generated from TAF and reviewed by the C&A team to ensure all approved versions of the documentation are posted in TAF.

As described below, the OCC has made or will be making corrections to the two documents noted by the auditors, NI GSS ITRP and \$SMART CP.

Issues with the NI GSS ITRP:

- a. The NI GSS ITRP is not currently up to date due to the departure of the ITRP Manager. The NI GSS ITRP is currently being updated. The updated version will include lessons learned from this years test. Scheduled completion date: October 31, 2010.
- b. The planned migration to the [REDACTED] has been completed. The updated ITRP will note the completion of this upgrade and include ITRP-related SAN information.
- c. An OCC management decision was made to delay the decommissioning of the IBM Compatible [REDACTED] Mainframe running [REDACTED] Operating System. The updated ITRP will note the current operational status of the mainframe and the updated ITRP will include other mainframe ITRP information.
- d. The ITRP has not been distributed quarterly to key personnel including 2 Resident Technical Support Specialist in the Southern and Western Districts due to the departure of the ITRP Manager. The ITRP will be updated annually and will be distributed quarterly to key personnel including 2 Resident Technical Support Specialist in the Southern and Western Districts.

Issues with the \$SMART CP:

The C&A program approved a new ITCP template in January 2010. As recommended by our C&A vendor, this template combined the Business Impact Analysis (BIA) into the ITCP. As part of the \$SMART 2010 Recertification, the \$SMART ITCP was updated in April 2010 (Version 4.01, dated 4/21/2010) and has been uploaded to the Audit Fix SharePoint site. The BIA is included as Appendix I in the ITCP. The latest information on the \$SMART environment is included in section 6, General System Description/Purpose, page 8 and states the use of [REDACTED].

**Office of the Comptroller of the Currency  
Management Letter Comments and Recommendations  
Year Ended September 30, 2010**

**(B) Configuration Management**

Configuration management policies, plans, and procedures should be developed, documented, and implemented at the entity wide, system, and application levels to ensure an effective configuration management process.

**2. Users have administrative rights to install personal or public domain software on their desktops.**

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 have administrative rights to install personal or public domain software on their desktops.

The OCC is in the process of implementing a software tool to remediate this weakness. The Beyond Trust (BT) Implementation project is currently in testing and is scheduled for complete implementation by April 2011.

*NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, User Installed Software 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 download and install software. The organization identifies what types of software downloads and installations are permitted (e.g., updates and security patches to existing software) and what types of downloads and installations are prohibited (e.g., software that is free only for personal, not government, use). The organization also restricts the use of install-on-demand software.”

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

**Recommendation:**

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

**Management’s Response:**

Management concurs with the finding and recommendation. The OCC has chosen to address this issue by using Beyond Trust application control software (ACS) to control elevation of privileges.



**Office of the Comptroller of the Currency**  
**Management Letter Comments and Recommendations**  
**Year Ended September 30, 2010**

The present OCC user desktop configuration allows local administrator privileges for all users. This means that users are not blocked from installing or downloading unauthorized or potentially malicious software which can harm computers and networks. OCC is currently implementing an industry-proven COTS solution, called Beyond Trust Privilege Manager, to provide minimally-needed privileges for about 95% of the typical users to fully execute their mission applications. The Beyond Trust tactic will establish a control method and an approval process to prevent these users from downloading, installing, or executing un-approved software.

At the same time, Beyond Trust will allow the remaining 5% of the Designated IT Specialists (e.g. Administrators, System Developers, Trained Technical Support Personnel, and Computer Security Analysts) to have full administrative rights to perform their official duties in supporting user desktop configurations or protecting application infrastructure.

BeyondTrust is currently undergoing two rounds of testing in the OCC Enterprise Testing Lab from August 24, 2010 to October 24, 2010. The control application is being readied for field testing among a group of about 40 pilot users starting in mid-October 2010. If pilot testing is successful, full implementation of Beyond Trust will expand by phases for all OCC users in accordance with the following schedule estimates:

<u>Southern District:</u>	November 15, 2010 to December 15, 2010
<u>Western District:</u>	December 15, 2010 to January 15, 2011
<u>Central District:</u>	January 15, 2011 to February 15, 2011
<u>Northern District:</u>	February 15, 2011 to March 15, 2011
<u>HQ:</u>	March 15, 2011 to April 15, 2011