Audit Report

OIG-10-025

Management Letter for Fiscal Year 2009 Audit of the
Office of the Comptroller of the Currency's Financial Statements

December 22, 2009

Office of
Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

December 22, 2009

MEMORANDUM FOR JOHN C. DUGAN
COMPTROLLER OF THE CURRENCY

FROM: Michael Fitzgerald
Director, Financial Audits

SUBJECT: Management Letter for Fiscal Year 2009 Audit of the Office of the Comptroller of the Currency's 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 Year 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, 2009 and for the year then ended. The contract required that the audit be performed in accordance with generally accepted government auditing standards; applicable provisions of Office of Management and Budget Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements,* as amended*;* and the *GAO/PCIE Financial Audit Manual*.

As part of its audit, 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 | Management Consultants

OFFICE OF THE COMPTROLLER OF THE CURRENCY
MANAGEMENT LETTER
FISCAL YEAR 2009

October 30, 2009

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

gka, P.C.

Certified Public Accountants | Management Consultants

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

Phone: 202-857-1777
Fax: 202-857-1778
Website: 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, 2009 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 30, 2009. 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 30, 2009

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2009

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

In our fiscal year (FY) 2008 audit, we identified weaknesses in the areas of entity-wide security program planning and management, access controls, service continuity, and application software development and change controls**.** We reported these weaknesses to management in a management letter. In FY 2009, 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. Only one (1) out of six (6) issues identified in FY 2008 remains partially unresolved (see Finding 5 below). The remediation work on this issue included a phased implementation of Federal Desktop Core Configuration (FDCC) and the implementation of a management control to detect and remove unauthorized software. During the FDCC implementation, OCC determined that administrative rights could not be removed without significant impact to OCC mission production systems. Treasury has since granted a waiver to OCC for removing administrator privileges. To mitigate the risk impact associated with local administrator privileges, the OCC is currently in an on-going process to research alternate methods for preventing the installation of unauthorized software.

We noted four (4) new areas for improvement in FY 2009. 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.

In the FY 2009 audit, we noted that OCC has updated its hiring procedures to require the completion of an Office of Personnel Management (OPM) Special Agreement Check (SAC) for all temporary interns who will be at OCC for less than 6 months as was recommended in our FY 2008 management letter. None of the findings noted in FY 2008 related to security management and contingency planning were repeated in FY 2009. However, we noted a new finding in this area which is detailed below together with our recommendation, and management's response.

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

   Specifically, we noted the following:

- The $MART Risk Assessment has not been updated to reflect changes to the $MART operating environment. Specifically, the upgrade from SQL Server 2000 to SQL Server 2005.
- There was no signature page or documentation provided to show that the July 2008 $MART Security Plan was approved.
- The $MART Security Plan has not been updated to reflect changes to the $MART operating environment. Specifically, the upgrade from SQL Server 2000 to SQL Server 2005.
- The $MART Security Plan does not accurately describe the system's interconnections. The plan states that there is a peer to peer connection used to transfer data between the OCC and Citibank, and the OCC and the Department of Defense - Central Contractor Registration (CCR). However, there are no direct connections between the OCC and these outside entities.
- The $MART Business Impact Analysis has not been updated to reflect changes to the $MART operating environment. Specifically, the upgrade from SQL Server 2000 to SQL Server 2005.
- The $MART Contingency Plan has not been updated to reflect changes to the $MART operating environment. Specifically, the upgrade from SQL Server 2000 to SQL Server 2005.
- The Network Infrastructure General Support System Security Plan identifies Jackie Fletcher as the Authorizing Official. However, Jackie Fletcher was replaced by Bajinder Paul as the Authorizing Official and the document was not updated to reflect the change.
- The Network Infrastructure General Support System Contingency Plan was not updated to reflect testing and lessons learned from the March 2009 testing.

The OCC does not have a formal process in place to ensure that all C&A documentation is updated to reflect system changes, changes in the operating environment or organizational changes. Additionally OCC is still in the process of updating the network contingency plan to incorporate the lessons learned from the last recovery test. However, the *OCC Master Security Controls Catalog*, states the following:

- "The OCC updates the risk assessment [every three (3) years] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system."
- "The OCC reviews the security plan for the information system [annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments."

- "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. Periodic assessments are important means of ensuring the effectiveness of policies and controls to reduce risk on an ongoing basis. Failure to update risk assessments, security plans and contingency plans increases the probability that OCC management may not be aware of how system changes impact the confidentiality, integrity and availability of system data. This may impact OCC's ability to recover from disaster situations. This increases the risk that OCC management may not have all of the appropriate information to ensure that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

Recommendations:
We recommend that OCC management: (1) implement a process to ensure that C&A documentation is updated timely in accordance with OCC policy, (2) ensure that approvals of C&A documentation are retained, and (3) ensure that the information contained in the documentation is accurate and reflects the current system operating and organizational environment.

Management's Response:
The OCC will document and implement a process to ensure that C&A documentation is reviewed on a periodic basis and updated when major changes occur, or as needed. The resulting agreed upon process will then be implemented and disseminated to all appropriate stakeholders. Stakeholders will be trained on their newly defined responsibilities. The C&A documentation will be updated to address the specific examples identified above.

(B) Access Controls

Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment.

We noted that OCC has implemented our FY 2008 audit recommendations to document and maintain approved authorization and recertification forms for access to SQL Server database related to the Financial Management applications; grant database access permissions in accordance with the principle of least privilege; and implementing a process, including implementing the Guardium tool, and standard operating procedures (SOP) to periodically review actions performed by database administrators within the $MART database.

None of the findings noted in FY 2008 related to access controls were repeated in FY 2009. However, we noted two new findings in this area. Our findings and recommendations, and management’s responses are detailed below.

2. **There are weaknesses in the OCC’s process for periodically reviewing network accounts and disabling access permissions that are no longer required.**

   Specifically, we noted the following:

   a. The number of days requirement for disabling inactive accounts in the $MART and Network Infrastructure Security plans were not consistent with the Master Security Controls Catalog and the Account Management Standard of Operating Procedures.

   b. There was no evidence to show that unnecessary System Administrator accounts were adequately disabled after the last account recertification.

   c. OCC network accounts are not being recertified on a monthly basis in accordance with the Master Security Controls Catalog.

   d. We identified 650 active network accounts that had been inactive for more than 60 days.

   e. We identified 295 active network accounts that have been configured with passwords that never expire.

We noted the following causes of the conditions stated above:

- OCC did not ensure that the “number of days” requirement for disabling inactive accounts was consistent in its procedures and security plans in accordance with agency requirements. Once OCC was notified of this issue, management revised the security artifacts with a requirement of no more than 90 days to bring all 4 documents into alignment. Therefore, we did not make any further recommendations.
- OCC currently does not perform monthly reviews of network accounts. OCC performed a review of system administrator accounts in March 2009 and identified accounts that needed to be removed; however the accounts had not been removed at the time of our audit. OCC is still in the process of removing these accounts.
- OCC does not have a process in place to identify service accounts, exchange accounts and other accounts that are exempt from the requirement to disable inactive accounts. Therefore, some inactive accounts are not appropriately disabled as a part of the weekly review process. Once OCC was notified of the 650 inactive accounts, OCC did its own analysis and determined that only 47 of the accounts were questionable. OCC then disabled the account or validated that it needed to be active.
- OCC does not have a process in place to identify the network accounts that must be configured with a password that never expires. Therefore, some network accounts were erroneously configured with passwords that do not expire. Once OCC was notified of these 295 accounts, OCC did its own analysis and determined that only 82 of the accounts were questionable. OCC then disabled the accounts or validated that they needed to be configured with a password that do not expire.

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]."
- "The OCC manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [90 days] of inactivity; and (vi) archiving user identifiers."
- "The OCC manages information system authenticators by: (i) defining initial authenticator content;(ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically."

Weaknesses in access controls increase the risk of inadvertent or deliberate disclosure, modification and destruction of OCC data. Users may have unauthorized or unnecessary access permissions to OCC systems and data.

Recommendations:
We recommend the following:

1. OCC should recertify network access permissions on a monthly basis in accordance with the Master Security Controls Catalog and remove access for individuals that no longer require the access.
2. OCC should disable unnecessary network accounts after 90 days of inactivity in accordance with OCC requirements.
3. OCC should implement a process to identify, document and approve all network accounts that are exempt from the 90 day inactivity requirement and periodically review these accounts for appropriateness.
4. OCC should implement a process to identify, document and approve all network accounts that are exempt from having to automatically enforce password changes and periodically review these accounts for appropriateness.

Management's Response:
The access controls weaknesses will be addressed as noted below:

Response to Condition "a" – Number of Days Requirement for Disabling Inactive Accounts: As noted by GKA, the OCC has updated documentation related to access controls to consistently reflect the requirement to disable accounts after 90 days of inactivity. No further action is required.

Response to Condition "b" – System Administrator Account Management: The OCC initiated a Task Order to address the issue of defining and implementing a process over the management of privileged accounts (i.e. creation, deletion, and review/recertification of accounts). The task order, which was awarded in September 2009, will focus on analyzing the current state process and either improving it or re-engineering it based upon the current state analysis findings. The resulting agreed upon procedures will then be implemented and disseminated to all appropriate stakeholders. Stakeholders will be trained upon their newly defined responsibilities.

Response to Condition "c" – Network Accounts Management/Network Account Recertification: The OCC will implement a process to periodically review/recertify network accounts in accordance with established OCC requirements. This process will be disseminated to all appropriate stakeholders. Stakeholders will be trained on their newly defined responsibilities.

Response to Condition "d" - Disabling Inactive Network Accounts: In FY 2007, a process was established to review inactive user accounts and disable accounts that reached the 90 day mark on a weekly basis. The number of inactive user accounts was significantly reduced as a result of this function. In recent months, the review and removal of inactive user accounts occurred with less frequency. We intend to reestablish a capability to periodically review all network accounts and disable accounts after 90 days of inactivity in accordance with the established requirements.

Response to Condition "e" – Identify and review Network Accounts Exempt from Inactive and Password Expire Requirements: The OCC will implement a process to identify and periodically review all accounts (e.g. service accounts, exchange accounts, etc.) which are exempt from: (a) the 90 day inactivity requirement, and (b) having to automatically enforce password changes. . This process will be disseminated to all appropriate stakeholders. Stakeholders will be trained on their newly defined responsibilities.

3. **There is currently no process in place to periodically review logs of system administrator activity for the OCC network.**

OCC maintains a log of all additions and deletions from the administrator groups on its network. The OCC Incident Response Team reviews these logs to determine if there are any user accounts that do not conform to OCC naming conventions. However, the operations group does not periodically review the logs to ensure that the individuals being added to the administrator groups are actual system administrators who have been authorized to have those access permissions.

The OCC Master Security Controls Catalog, states the following:

- “The OCC supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.”
- “The OCC regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.”

Failure to periodically review audit logs increases the risk that unauthorized individuals may access, modify or destroy data without detection. Additionally, management may not be able to identify suspicious or unusual actions that could help detect potential security breaches.

Recommendation:
We recommend that OCC implement a process to periodically review logs of system administrator activity on the network.

Management’s Response:
As part of their regular weekly duties, the OCC’s *Computer Incident Response Capability* (CIRC) staff maintains surveillance of privileged account activity looking for non-compliance to standards, add and remove actions and other suspicious activity (based on trends) that would present a risk of unauthorized access. Any issue with suspicious activity is escalated to the Information Resource Management (IRM) Lead for Incident Response. While this responsibility is defined in the CIRC Procedures Manual (v4.5 Appendix A), the CIRC’s review criteria and procedures are not formally documented. The OCC will formally document these procedures, in addition to developing and implementing a process to provide evidence of the periodic reviews currently taking place over system administrator activity by CIRC staff.

It should be noted that an additional layer of system administrator activity review is currently in place to monitor and review actions of database administrators in the $MART database. This database logging capability (and associated review process) was implemented in February of 2009 to address a prior year (FY 2008) finding.

<u>(C) Configuration Management</u>

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.

During the prior year, we recommended that OCC management continue to dedicate resources to fully implement the necessary Microsoft System Management Server (SMS) process to automatically and promptly detect and remove unauthorized personal and public domain software from OCC systems (desktops) and implement controls to restrict users from downloading and installing unapproved software. The remediation work on this issue included a phased implementation of the Federal Desktop Core Configuration (FDCC) and the implementation of a management control to detect and remove unauthorized software. During the FDCC implementation, OCC determined that administrative rights could not be removed without significant impact to OCC mission production systems. Treasury has since granted a waiver to OCC for removing administrator privileges. To mitigate the risk impact associated with local administrator privileges, the OCC is currently in an on-going process to research alternate methods for preventing the installation of unauthorized software. We also noted a new finding in this area. Our findings and recommendations, and management's responses are detailed below.

4. **The OCC consolidated inventory of systems was not up-to-date. Specifically, we observed that the C-Cure physical security management system was not included in the inventory.**

At the time of our review, the OCC was not reviewing and updating the consolidated system inventory. However, in July 2009, the OCC instituted a quarterly process to review and update the consolidated system inventory and performed the first initial review. Therefore we did not make any further recommendations.

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

- "The OCC develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information."
- "The OCC updates the inventory of information system components as an integral part of component installations."

Effective configuration management includes the implementation of processes to maintain and keep current an accurate comprehensive baseline inventory of hardware, software, and firmware. Failure to incorporate components in the inventory increases the risk that sensitive components may not be adequately identified and monitored for patch levels. Additionally, if sensitive components are not on management's radar, then they may not have adequate security controls in place to ensure that they are not targeted to exploit vulnerabilities

Recommendations:
Before the end of our fieldwork, the OCC reviewed and updated the consolidated system inventory in order to remediate this deficiency. Therefore we did not make any further recommendations.

Management's Response:

As part of the continuous improvement process, in mid 2009, ITS identified an opportunity to increase the accuracy and reliability of information contained in the Application System Inventory (ASI) portion of the OCC's Agency Metadata Repository (AMR). Specifically, ITS reviewed the current fields/attributes of the ASI and identified several fields/attributes as critical elements of the change, configuration and release management decision-making process. The critical fields and associated information were baselined and used as a reference during the first of ongoing quarterly audits. The first quarterly audit was completed on September 16, 2009. Preliminary audit numbers indicate that an average of 11 attributes (26%) of each of the 135 applications were either updated or added as a result of the audit process. ITS recognizes the need for accurate and timely information, and proactively seeks to reduce risks and increase reliability of services through continuous review and improvement process.

5. **Although, the OCC has implemented a process to detect unauthorized software, OCC users still have local administrator privileges on their individual workstations without any mitigating controls to prevent them from installing software at will.**

OCC has currently implemented the Microsoft System Management Server (SMS) system, which provides patch management, software distribution, and hardware and software inventory capabilities for OCC systems. OCC piloted a process for detecting and removing all unauthorized software from OCC systems and determined that the process was too time consuming. Therefore, OCC implemented a scaled down version of the process where they identify, detect and work to remove 5 to 10 unauthorized software versions on a quarterly basis. However this process does not detect all versions of unauthorized software. Additionally, users have local administrator privileges on their workstations which would allow them to re-install the software at will. OCC plans to fully address this issue by implementing a software solution, as a part of the technology refresh that allows management to "white list" authorized software and prevent any unauthorized software from running.

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:

Although this is a repeat finding, it should be noted that the remediation work outlined in the management response for the prior year finding (FY2008 IT-02) was completed and reviewed by the GKA auditors during the FY 2009 cycle. Remediation work included a phased implementation of Federal Desktop Core Configuration (FDCC) and the implementation of a management control to detect and remove unauthorized software.

As a result of rigorous testing conducted by the OCC's Enterprise Test Lab during the FDCC implementation, it was determined that administrative rights could not be removed without significant impact to OCC mission production systems. Due to this, the OCC submitted a request to Treasury for 11 FDCC deviations, one of which was a waiver for removing administrator privileges. Treasury reviewed and approved this request in their July 1, 2009 FDCC Deviation Approval memo to the OCC, which was provided to the GKA auditors.

To mitigate the risk impact associated with local administrative privileges, the OCC is currently in an on-going process to research alternate methods for preventing the installation of unauthorized software; including the use of special software that enables white-listing of installations. If a technical solution is not feasible in FY 2010, ITS will conduct a risk assessment that will be the basis of a risk acceptance memo should Business units choose to accept the residual risk associated with this issue.