



Audit Report



OIG-09-027

Management Letter for Fiscal Year 2008 Audit of the
Office of the Comptroller of the Currency's Financial Statements

January 8, 2009

Office of
Inspector General

Department of the Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

January 8, 2009

**MEMORANDUM FOR JOHN C. DUGAN
COMPTROLLER OF THE CURRENCY**

FROM: Michael Fitzgerald /s/
Director, Financial Audits

SUBJECT: Management Letter for Fiscal Year 2008 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 2008 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, 2008 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, GKA issued and is responsible for the accompanying management letter that discusses 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 audit 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 2008**

October 31, 2008

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

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

Phone: 202-857-1777
Fax: 202-857-1778
Website: www.gkacpa.com

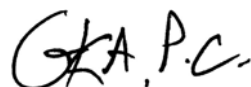
Inspector General, Department of the Treasury, and
the Comptroller of the Currency:

We have audited the balance sheet as of September 30, 2008 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, 2008. 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.

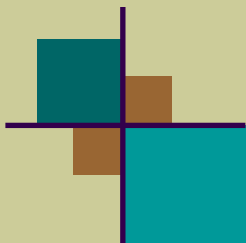
During our audit we noted certain matters involving OCC's information technology general controls that are presented in this letter for your consideration. The comments and recommendations, all of which have been discussed with the appropriate members of OCC management, are intended to improve OCC's 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 31, 2008



Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

Improvements Needed in Information Technology General Controls over OCC's Financial Systems (Prior Year Significant Deficiency).

In our fiscal year (FY) 2007 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 our report on internal control over financial reporting. In FY 2008, 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 two (2) out of 15 issues identified in FY 2007 remain open or are partially resolved. We noted five (5) new areas for improvement in FY 2008. The weaknesses noted in OCC's IT general controls are noted and discussed below.

(A) Entity-Wide Security Program Planning and Management

Entity-wide security program planning and management provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

In the FY 2008 audit, we noted that OCC strengthened its controls over requiring new contractors to complete and sign all access agreements before given access to OCC information systems; the administration of the security awareness training; recordkeeping of users' access agreements; completion of exit process for terminated employees; and testing and updating its Computer Incident Response Capability; as we recommended in our FY 2007 audit report. None of the findings noted in FY 2007 related to the entity-wide security program planning and management were repeated in FY 2008. However, we noted a new finding in this area which is detailed below together with our recommendation, and management's response.

1. OCC did not ensure that background investigations had been performed prior to allowing employees access to sensitive information.

Two (2) out of the ten (10) new hires selected for testing did not have completed background investigations. According to OCC management, the two individuals are temporary interns that did not work for more than 180 days and therefore do not require background investigations. However, *OCC Information Security Program: Policies Standards and Required Controls*, states "The OCC limits access to its information and information resources strictly to those individuals who have demonstrated very high levels of professional competence and personal conduct. It screens its workforce members to ensure they are qualified to accept their information security responsibilities and to perform reliably in positions of public trust...The OCC requires the completion of suitable background investigations and signed acknowledgements of information security responsibility prior to allowing its employees and contractors access to its sensitive information and supporting technology."

The lack of adequate background investigations increases the risk that unqualified or

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

untrustworthy individuals may have access to OCC data and systems. This puts OCC data at risk of inadvertent or deliberate misuse, modification, destruction, or disclosure of sensitive information.

Recommendation:

We recommend that OCC management institute a process to screen temporary interns based on the risk designation of their position and complete a background investigation, if necessary.

Management's Response:

The Critical Infrastructure Protection and Security Office of the OCC concurs that two (2) of the new hires tested did not have background information due to the fact that they were temporary student interns assigned to low risk, non-sensitive, non-Public Trust positions that did not require a suitability investigation or a Homeland Security Presidential Directive (HSPD) -12 investigation under current regulations.

To address the perceived risk and remediate this finding the OCC will change the procedures for student interns requiring a minimal background investigation be completed by OPM in the form of a Special Agreement Check for all interns. This new procedure will be completed by November 1, 2008 due to necessary consultation with Human Resources and District Offices.

(B) Access Controls

Access controls limit and/or detect access to computer resources (data, programs, equipment and facilities), thereby protecting these resources against unauthorized modification, loss and disclosure.

We noted that OCC has implemented our FY 2007 audit recommendations pertaining to strengthening access controls pertaining to the password configuration setting for C-Cure System and revoking unnecessary access accounts. However, we noted that one FY 2007 audit finding pertaining to recordkeeping of management approval and recertification for access to SQL server database has not been addressed. This is included in finding No. 2 below. In addition, we noted two new findings in this area. Our findings and recommendations, and management's responses are detailed below.

2. OCC should document and maintain approved authorization and recertification forms for access to SQL Server database related to the Financial Management applications (Repeat Finding).

OCC was unable to provide evidence of management authorization and recertification of access to SQL Server database for \$SMART for six (6) out of 10 users selected for testing. Although, *OCC Information Security Program: Policies Standards and Required Controls*, states "The OCC manages information system account, including establishing, activating, modifying, reviewing and disabling accounts. It reviews user information system accounts at least annually

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

and privileged accounts at least semi-annually...Only OCC-authorized users are allowed to access sensitive information and OCC information resources...System access controls shall deny access by default, and grant access only as authorized by appropriate authority...OCC limits system privileges to that functionality for which a user has a demonstrated need in the course of performing his or her work. This access allocation practice is called least privilege...The OCC requires access control lists to be reviewed monthly to reconfirm the need for continued access at the assigned access level for each user. It shall have access termination processes that ensure access is removed promptly when an authorized user is terminated, transferred or otherwise no longer requires access."

Without the strict requirement for management authorization, users may have unauthorized access rights to the SQL Server database that supports \$SMART, thus putting OCC systems at increased risk for inappropriate modification or disclosure of data.

Recommendations:

We recommend that OCC management: (1) document and maintain on file approved database authorization forms for individuals with access to the SQL Server database supporting \$SMART, and (2) dedicate resources to complete its on-going efforts to recertify roles and privileges of users with SQL database access.

Management's Response:

Management concurs with the finding. OCC will enhance its current process of managing requests for access, and recertification of access to the SQL Server database supporting \$SMART. The existing process will be evolved to use Remedy as its repository for the management of all \$SMART access requests. The \$SMART system administrator will work with the Database Administrator (DBA) team to create and periodically review a report of all users (general and system administrators) who have SQL Server accounts with roles that offer access to query \$SMART tables, views, and reports as part of a standard recertification process. The DBA team will update its standard processes to ensure steps associated with granting access to \$SMART SQL Server tables are clearly articulated, and all such actions are documented in Remedy. All remediation work will be completed by February 2009.

3. Database access permissions are not always granted in accordance with the principle of least privilege.

Database access permissions are not always granted in accordance with the principle of least privilege. Specifically, the BUILTIN\Administrators group, which is the Windows Administrators group, is added to the SQL Server System Administrator role. Therefore Windows Administrators have full control over the SQL database of \$SMART, which is a major application with a security categorization of Moderate. However, Windows Administrators are not required to manage databases and, therefore, should be removed from this role. Per OCC's management, when the \$SMART SQL database was initially setup, the BUILTIN\Administrators group was automatically added to the SQL Server System Administrator role by default.

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

However, OCC did not remove database administrator privileges from the BUILTIN\Administrators group because it is used to run the SQL Services and could cause potential issues with recovering the database in disaster situations. Nonetheless, *OCC Information Security Program, Policies Standards and Required Controls*, states “Information systems having a security categorization of MODERATE or HIGH shall enforce the most restrictive set of rights/privileges or access needed by users, or processes acting on behalf of users, for the performance of specified tasks.”

Granting full control of database objects to Windows Administrators increases the risk that non-privileged users can take full control of the \$SMART SQL database. This puts OCC systems and data at risk of inadvertent or deliberate modification, destruction and disclosure.

Recommendation:

We recommend that OCC management create a separate account to run the SQL Server Services prior to removing the BUILTIN\Administrators group from the SQL Server System Administrator role or establish alternate mechanisms to restrict Windows Administrators from obtaining full control over the \$SMART database.

Management’s Response:

Management concurs with the finding. OCC has contacted Microsoft concerning the removal of the BUILTIN\Administrators group from the SQL Server Administration role. Microsoft has responded by providing instructions for safely removing the account.

The OCC will remove the BUILTIN\Administrators group from the SQL Server Administration role before December 31, 2008.

4. OCC does not currently monitor and review actions performed by database administrators within the \$SMART database.

OCC does not currently monitor and review actions performed by database administrators within the \$SMART database. The lack of active monitoring of OCC database administrators increases the risk of unauthorized modification, destruction, or disclosure of \$SMART data stored within the database.

OCC has procured and is currently in the process of implementing a COTS tool called Guardium which will enable OCC to log and review database administrator activities. The *OCC Information Security Program, Policies Standards and Required Controls*, states “OCC ensures that its information systems produce audit logs that record user and processing activity related to system security, and that these logs are regularly reviewed.”

Recommendation:

We recommend that OCC management complete the implementation of the Guardium tool and implement a process to periodically review database administrator actions.

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

Management's Response:

OCC Management concurs with the finding. OCC has procured the Guardium Security Suite 7.0 product. This tool will allow the OCC to actively monitor the actions of privileged users such as Database Administrators. The product will also allow for automatic alerts when privileged users (such as Database Administrators) access or attempt to access data they should not access. The tool will be installed by end of October, 2008. The capability to monitor database administrator actions, send alerts on unauthorized actions, and retain logs on actions involving data OCC has classified as sensitive for a minimum of 1 year, will be in place by February 28, 2009. At that point the OCC Computer Center Incident Response will add Guardium logs to the standard operating procedures for monitoring, review and reporting of logs. The Incident Response team reviews unusual activity throughout the day.

(C) Service Continuity

Service continuity controls ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

During our audit, we noted that OCC has implemented our FY 2007 recommendations to strengthen its service continuity controls pertaining to the performance of a cost-benefit analysis to support its selection of an off-site storage facility close to the Data Center; maintenance of consistency between Contingency Planning documents; finalizing the Information Technology Recovery Plan; development of a formal emergency response training program for Data Center personnel; and mitigation of risk associated with overheating due to the absence of an air conditioner in the Data Center telecommunication room. None of the findings noted in FY 2007 were repeated in FY 2008. However, we noted two (2) new findings in this area which are detailed below together with our recommendations, and management's response.

5. Lessons Learned from the disaster recovery testing have not been incorporated in the Disaster Recovery Plan.

The SMART Disaster Recovery Plan (DRP) was tested in February 2008. However, weaknesses identified during the disaster recovery testing have not been incorporated into the DRP. *OCC Information Security Program, Policies Standards and Required Controls*, states "The OCC reviews its contingency plans at least annually, and revises its plans to address system/organizational changes or problems encountered during plan implementation, execution, or testing."

OCC may not be able to fully recover and restore SMART systems and data in a disaster situation without an updated contingency plan.

Recommendation:

We recommend that OCC management institute a process to update the SMART DRP to address

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

weaknesses identified during disaster recovery testing.

Management Response:

Management concurs with the finding.

The template for the *Disaster Recovery (DR) Post Exercise* document will be revised to explicitly indicate that follow-through is required on lessons learned. Specifically, the lessons learned section of the document will be updated to specify that the lessons learned must be incorporated in the \$SMART Contingency Plan. Further, the format of this section will be updated to include owner and delivery date columns for each conclusion. This delineation of responsibility for each conclusion will allow for a more efficient process to track the status and close-out of each item.

The cross-functional team that participated in the \$SMART DR testing will reconvene to address the specific lessons learned from this exercise. Updates will be tracked and documented until conclusion. A memo will be drafted upon close-out and submitted to the Chief Information Officer detailing each remediation accompanied by appropriate artifacts.

All remediation work will be completed by February 2009.

6. The OCC network failover capacity has not been fully tested.

The OCC network failover capacity has not been fully tested to ensure that network operations can be restored at an alternate site in disaster situations. According to OCC management, funding issues and the potential risk impacting OCC business functions have prevented full testing of the failover capability. However, *OCC Information Security Program, Policies Standards and Required Controls*, states “The OCC tests at least annually the contingency plans for its information systems having security categorizations of MODERATE or HIGH to determine the plans’ effectiveness and its organizational readiness... For its information systems with MODERATE and HIGH security categorizations, the OCC identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions when the primary processing capabilities are unavailable. The OCC ensures that the timeframes for resumption of information systems operations are consistent with its recovery time objectives.”

If OCC failover capability is not fully tested, OCC may not be able to restore its financial management systems (including \$SMART) in a disaster situation.

Recommendation:

We recommend that OCC management institute a process to fully test the network failover capability.

Management Response:

OCC Management Concurs - As noted in the findings, all non-disruptive elements of the

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

\$SMART DRP have been tested. OCC will complete a risk-based cost-benefit analysis associated with conducting a full failover test of the components of the OCC network associated with \$SMART. The results of the risk assessment will be presented to the OCC Executive Committee by April 2009.

(D) Application Software Development and Change Control

Application Software Development and Change Control prevents unauthorized programs or modifications to an existing program from being implemented. During our audit, we identified one finding in this area that is being repeated for FY 2008. Our finding, related recommendation, and management's response are detailed below.

7. OCC has not fully implemented the necessary capabilities to automatically and promptly detect and remove unauthorized personal and public domain software from OCC systems (workstations) (Repeat Finding).

OCC users have local administrator privileges on their individual workstations and can install software at will. Additionally, even though OCC has implemented the Microsoft System Management Server (SMS) system, OCC has not fully implemented a process to detect and remove unauthorized software. The implementation of SMS, which provides patch management, software distribution, and hardware and software inventory capabilities for OCC systems; is in the piloting phase of the process to detect and remove unauthorized software from OCC systems. However, *National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, User Installed Software* states "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." Further, *OCC Information Security Program, Policies Standards and Required Controls*, states: "The OCC identifies which types of software downloads and installations shall be (1) Permitted (e.g., updates and security patches to existing software); or (2) Prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect); and (3) Enforces this accordingly."

The lack of active monitoring of OCC systems for the use of unauthorized software could result in the introduction of unapproved software in OCC's networking environment, which could negatively impact processing operations, introduce harmful viruses, and/or cause the loss of data.

Recommendation:

We recommend that OCC management continue to dedicate resources to fully implement the necessary SMS process automatically and promptly detect and remove unauthorized personal and public domain software from OCC systems (workstations) and implement controls to restrict users from downloading and installing unapproved software.

Office of the Comptroller of the Currency
Management Letter Comments and Recommendations
Year Ended September 30, 2008

Management's Responses:

Management concurs with the finding.

(1) The OCC will formalize its management controls over the prohibition of installing software that has not been officially approved, supported, and controlled by the OCC. These management controls consist of policy (PPM 4000-3), procedures, and annual security awareness training that are made available to all OCC computer users.

(2) Operational controls are also being used to provide additional safeguards. OCC's Information Technology Services (ITS) department has established a full accounting of all software currently found on its workstations and laptops. This inventory is cross referenced against the OCC standard operating system build, application suites, and non-standard but OCC sanctioned third party software. In February 2008, ITS began a pilot of this process with two Business Units. The pilot will continue through December of 2008, after which the remaining Business Units will be scheduled to implement and follow the process. This process will remain in place until OCC completes its full implementation of the Federal Desktop Core Configuration (FDCC) by December 2009.

(3) Technical controls are also being utilized to establish a secure operating system image that complies with the FDCC settings. Given the significant impact that the FDCC will have on OCC's mission capabilities, OCC is implementing FDCC in a phased manner with low impact, low risk settings being deployed by January 2009; moderate impact, moderate risk settings being deployed by June 2009; and high impact, high risk settings (which includes revocation of administrative privileges from general uses) scheduled for December 2009. Lastly, given the age, complexity, and impact to OCC's core mission support systems, not all high impact, high risk settings may be implemented. Final disposition of this finding will not be fully enacted until OCC completes its impact analysis for removal of administrative privileges on its core mission applications. If it is determined that administrative privileges cannot be removed, OCC will have to accept the risk until its core mission systems can be upgraded, reengineered, and/or retired.