Audit Report

OIG-14-025

Management Letter for the Audit of the Office of the Comptroller of the Currency's Fiscal Years 2013 and 2012 Financial Statements

February 4, 2014

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

February 4, 2014

MEMORANDUM FOR THOMAS J. CURRY
COMPTROLLER OF THE CURRENCY

FROM: Michael Fitzgerald
Director, Financial Audit

SUBJECT: Management Letter for the Audit of the Office of the Comptroller of the Currency's Fiscal Years 2013 and 2012 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 (OCC) financial statements for fiscal years 2013 and 2012. Under a contract monitored by the Office of Inspector General, Williams, Adley & Company-DC, LLP (Williams Adley) an independent certified public accounting firm (IPA), performed an audit of the OCC's financial statements as of September 30, 2013 and for the year then ended. Another IPA audited the OCC's financial statements as of September 30, 2012 and for the year then ended and expressed an unmodified opinion on those financial statements. The contract required that the audit be performed in accordance with generally accepted government auditing standards and applicable provisions of Office of Management and Budget Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*.

As part of its audit, Williams Adley issued, and is responsible for, the accompanying management letter that discusses certain matters involving internal control over financial reporting that were identified during the audit, but were not required to be included in the auditors' reports.

In connection with the contract, we reviewed Williams Adley's letter and related documentation and inquired of its representatives. Our review disclosed no instances where Williams Adley 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 Audit at (202) 927-5329.

Attachment

MANAGEMENT LETTER

Comptroller of the Currency
Office of the Comptroller of the Currency

Inspector General
Department of the Treasury

We have audited the balance sheet as of September 30, 2013, 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 unmodified opinion thereon dated November 20, 2013. The financial statements of OCC as of September 30, 2012 were audited by other auditors who issued an unmodified opinion dated October 31, 2012.

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.

In our fiscal year 2013 audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. Although not considered to be material weaknesses or significant deficiencies, we noted certain matters involving internal control over information technology operations and the financial institution assessment process that are presented in Appendix I to this letter for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of OCC management, are intended to improve internal control. Also, we noted one management letter comment that is carried over from the prior year, as discussed in Appendix II. Additionally, we have provided the status of all prior year management letter comments in the same appendix.

We appreciate the cooperation and courtesies extended to us during the conduct of the audit. We will be pleased to meet with you or your staff, at your convenience, to discuss issues in this letter or furnish any additional information you may require.

Williams, Adley & Company-DC, LLP

Washington, D.C.
November 20, 2013

Information Technology Operations

Although the OCC performed weekly scans, had a process of identifying vulnerabilities within the information systems, and developed configuration baseline requirements, weaknesses continued to exist in the financial system. OCC had identified certain vulnerabilities during its routine scans but considered them as low to moderate risks. Since only high risk vulnerabilities are addressed as part of the Plan of Actions and Milestones (POA&M) process, OCC did not address these identified vulnerabilities.

The OCC Master Security Control Catalog (MSCC) Risk Assessment Section, Control RA-5 states: *"The OCC remediates legitimate vulnerabilities as specified in associated POA&Ms or corrective actions plans in accordance with an organizational assessment of risk." However,* the MSCC catalog does not specify what type/level of risk is a legitimate vulnerability and how each category of risk is to be addressed.

Also, for one vulnerability identified, the software vendor confirmed that a conflict exists between the application and the scanning tool which the vendor states the current setting is necessary as a security feature.

System weaknesses increase the potential for unauthorized activities to occur without being detected thus leading to potential theft, destruction, and misuse of agency data both from internal and external threats.

Recommendations: We recommend that OCC Security & Compliance Services (SCS):

1. Update the MSCC procedures to:
    a. Define the risk level associated with a legitimate vulnerability, and
    b. Address the handling of identified low to moderate risks vulnerabilities.

2. Remediate the identified vulnerabilities.

Management Response:

The OCC concurs with recommendation #1 and stated that they will update its policy to better define risk levels and legitimate vulnerabilities. The OCC stated that they will also update its procedures to provide direction on evaluating and remediating low and moderate vulnerabilities based on a risk assessment. The OCC estimates completing the corrective actions for this recommendation by January 31, 2014.

OCC stated that they had remediated all the vulnerabilities identified by the auditor related to that recommendation prior to completion of the audit.

Auditor Analysis:

Based on management's response, we determined that the proposed approach is sufficient to close the recommendations if properly implemented.

OCC's response has not been subjected to the auditing procedures applied in the audit of the financial statements and accordingly, we express no opinion on it.

Underassessment of Financial Institutions

From March 2009 through March 2013, five financial institutions were under-assessed by a total of $4,886,926. In September 2013, six financial institutions (including the five mentioned above) were under-assessed by a total of $863,885. During the periods mentioned above, the financial institutions were assessed as commercial banks instead of independent trust banks. Independent trust banks are assessed a surcharge above the commercial bank assessment.

The Licensing Department (within the Office of Chief Counsel) is in charge of providing Financial Management (FM) with the list of banks and each bank's assessment category (i.e. commercial bank, credit card bank, and/or independent trust bank). Each bank is categorized based on the type of assets they hold. In order for a financial institution to qualify as a commercial bank, a bank's assets must be less than 50% trusts. If the bank's assets exceed 50% trusts, the bank is classified as an Independent Trust Bank and is therefore subject to a surcharge.

The under-assessed banks were comprised of less than 50% assets in trust when originally evaluated, however in subsequent assessments periods the trust asset percentage crossed the 50% threshold. Since, the Licensing Department did not regularly re-evaluate bank classifications, the commercial bank designation was not revised accordingly.

GAO's Standards for Internal Control in the Federal Government states that:

> "Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation."
>
> "Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded. Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination."

Under-assessment of financial institutions occurred because OCC does not have policies and procedures for periodically reevaluating banks to determine whether their current categorization and thus the assessment is appropriate.

In October 2013, the Comptroller of the Currency decided to waive the assessment and collection of the $4,886,296. The September 2013 under-assessment was collected in October 2013 and was

appropriately included in the FY13 financial statements. Due to this error, assessment fees amounting to $4,886,926 were not collected that could have been used to fund OCC's operations.

Recommendation:

We recommend that OCC develop policies and procedures for determining assessment fees including an annual re-evaluation of banks to confirm or correct their classifications.

Management Response:

The OCC concurs with this recommendation. They stated that they have already established a cross-disciplinary team with experts to develop a streamlined process for determining assessment fees and validating the bank assessment classification. Financial Management (FM) will develop the policies and procedures documenting the process. In addition, FM's Internal Controls team will test the new process to determine if controls are working as designed. The estimated completion date for the streamlined process is March 31, 2014 and the estimated completion date for the policies and procedures is April 30, 2014.

Auditor Analysis:

Based on management's response, we determined that the proposed approach is sufficient to close the recommendation if properly implemented.

OCC's response has not been subjected to the auditing procedures applied in the audit of the financial statements and accordingly, we express no opinion on it.

The following is the status of the remediation of weaknesses noted during the Fiscal Year 2012 audit. For the purposes of this letter, we included only a summarized version of each issue and the recommendations made.

12-06 OCC Needs To Strengthen Its Contingency Planning Controls (Repeat Condition)

There were weaknesses in *OCC's* contingency planning controls. Specifically, (1) an executable disaster recovery strategy solution did not exist for a general support system (GSS), (2) the contingency plan for this GSS did not contain detailed procedures for recovering the system in a disaster situation or detailed procedures for reconstituting the system after a disaster, (3) the contingency plan for an application did not contain detailed procedures for recovering that application in a disaster situation or detailed procedures for reconstituting the application after a disaster, and (4) the contingency plans for the application and the GSS included several links to documents stored on the organizations share site. This increases the risk that the referenced documents may not be accessible during a disruption that impacts the network.

Recommendations: OCC management should:

18. Continue with its existing corrective action to develop an executable recovery strategy for its network. Once a strategy is developed, it should be tested to ensure that it can be executed
19. Update the Business Impact Assessments for the general support system to establish a RPO for the system.
20. Update the system Contingency Plan to incorporate detailed recovery and reconstitution procedures
21. Update the system Contingency Plan to incorporate all necessary documents stored on the share site needed to facilitate system recovery.
22. Update the Business Impact Assessments for the application to establish a RPO for the system.
23. Update the application Contingency Plan to incorporate detailed recovery and reconstitution procedures.
24. Update the application Contingency Plan to incorporate all necessary documents stored on the share site needed to facilitate system recovery.

Status: Partially Closed. OCC addressed the prior year recommendations 22, 23, and 24, which included updating the contingency plan and the Business Impact Assessments for the application. However, weaknesses continue in OCC's general support system contingency planning controls. As a result, recommendations numbers 18, 19, 20, and 21 remain open.

Management Response:

The OCC concurs with these recommendations. The OCC stated that they are continuing to improve OCC's ability to recover the network general support system through their enterprise disaster recovery modernization initiative. They stated that the OCC's Technology Solutions Subcommittee approved this initiative on July 30, 2013 and that Information Technology Services developed a multi-year project plan to support modernizing OCC's disaster recovery capability that is contingent on allocation of necessary funding in future periods. OCC stated that management approved the plan and provided the auditors a copy during the audit. Further, the OCC estimates corrective actions will be completed no later than September 30, 2016 for recommendation 18; July 30, 2014 for recommendation 20; August 30, 2014 for recommendation 21; and January 31, 2014 for recommendation 19.

Auditor Analysis:

Based on management's response, we determined that the proposed approach is sufficient to close the recommendations if properly implemented.

Prior Year Findings		**Current Year Status**
12-01	OCC should ensure that its Information System Security Plans (SSP) are consistent with Federal requirements	This finding has been closed.
12-02	OCC should strengthen its role based training controls	This finding has been closed.
12-03	OCC should ensure that appropriate agreements are in place to ensure that data is adequately protected	This finding has been closed.
12-04	OCC needs to strengthen its identification and authentication controls	This finding has been closed.
12-05	OCC needs to strengthen its account management controls	This finding has been closed.
12-06	OCC needs to strengthen its contingency planning controls (Repeat Condition)	Partially Closed. See repeat condition above.
12-07	OCC should test the offsite disaster recovery backup tapes on a semi-annual basis	This finding has been closed.
12-08	OCC should update its virus definition to the current version	This finding has been closed.
12-09	OCC needs to strengthen its controls for configuring information systems	This finding has been closed.
12-10	OCC should maintain current patches and remove unnecessary services from application servers	This finding has been closed.
12-11	OCC needs to strengthen its configuration management controls	This finding has been closed.

OCC's response has not been subjected to the auditing procedures applied in the audit of the financial statements and accordingly, we express no opinion on it.