Audit Report

OIG-15-009

Management Letter for the Audit of the Community Development Financial Institutions Fund's Fiscal Years 2014 and 2013 Financial Statements

November 14, 2014

Office of Inspector General

Department of the Treasury

November 14, 2014

**MEMORANDUM FOR DENNIS NOLAN, ACTING DIRECTOR
COMMUNITY DEVELOPMENT FINANCIAL
INSTITUTIONS FUND**

FROM: Michael Fitzgerald
              Director, Financial Audit

SUBJECT: Management Letter for the Audit of the Community
              Development Financial Institutions Fund's Fiscal Years 2014
              and 2013 Financial Statements

I am pleased to transmit the attached management letter in connection with the audit of the Community Development Financial Institutions (CDFI) Fund's Fiscal Years 2014 and 2013 financial statements. Under a contract monitored by the Office of Inspector General, KPMG LLP (KPMG), an independent certified public accounting firm, performed an audit of the CDFI Fund's financial statements as of September 30, 2014 and 2013, and for the years then ended. The contract required that the audit be performed in accordance with generally accepted government auditing standards and Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*.

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

In connection with the contract, we reviewed KPMG's letter and related documentation and inquired of its representatives. Our review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted government auditing standards and OMB Bulletin No. 14-02.

Should you have any questions, please contact me at (202) 927-5789, or a member of your staff may contact Catherine Yi, Manager, Financial Audit at (202) 927-5591.

Attachment

November 12, 2014

Inspector General
U.S. Department of the Treasury
Washington, DC

Acting Director
Community Development Financial Institutions Fund
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of U.S. Department of the Treasury's Community Development Financial Institutions Fund (the CDFI Fund), as of and for the year ended September 30, 2014, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, we considered the CDFI Fund's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the CDFI Fund's internal control. Accordingly, we do not express an opinion on the effectiveness of the CDFI Fund's internal control.

During our audit we noted an item involving internal control and other operational matters that is presented for your consideration. This comment and related recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in the attached Appendix A.

The CDFI Fund's written response to our comment and recommendations (also in Appendix A) has not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the CDFI Fund's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss this comment and related recommendations with you at any time.

This communication is intended solely for the information and use of the addressees, OMB, the U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Improvements Needed in Controls Surrounding the CDFI Fund's Disbursement System

Improvements are needed in controls surrounding the CDFI Fund's Disbursement System (System) to prevent or detect and correct unauthorized changes to production data or the application environment as neither the System nor database are structurally designed or coded to enforce segregation of duties.

Management contracted with a third party for development and system support to maintain the System and its databases. Management assigned a third party as the administrator, and permitted the development team to have update privileges within the System production environment.

Once management approves a system change request (SCR), the development team follows Standard Operating Procedures, which require segregation of duties by assigning a team member to each of the four roles within the change management function (developing, testing, quality control, and deployment). The system first assigns the SCR to the SCR Manager, who then assigns it to a Developer. The Developer identifies and notates on the SCR ticket respective roles. Due to the small size of the third-party system, contractor team members can perform different roles on different SCRs. However, neither the System nor the database structure enforces any segregation of duties controls (restricted user provisioning) to prevent a contractor team member from performing all roles within the change management function. Management further stated that the contractors performing the change management function have database roles/privileges that allow them the ability to access and modify the application logs.

Segregation of duties of the contractors is not enforced through the system which results in the potential for unauthorized system changes to a disbursement in certain scenarios.

Management may not detect and correct unauthorized changes within the System tables on a timely basis, which could lead to unauthorized access, modification, and/or disclosure of the System's production data and application environment.

Recommendations

We recommend that management:

1. Evaluate the existing privileges of the System development team members, including the SCR Manager, and reassign privileges that enforce segregation of duties at the application and database levels; and

2. As appropriate, document the risk assessment and acceptance of any incompatible duties, and implement an effective control to mitigate the risk of unauthorized access and activity (e.g., the implementation of a mechanism and process to log incompatible activities, and independently review the logs on a periodic basis and resolve any violations).

Management's Response

CDFI Fund Management appreciates the opportunity to review and respond to this finding and recommendations. The CDFI Fund continuously seeks to improve our business applications, and CDFI Fund Management concurs with both the finding and recommendations.

1. The CDFI Fund will evaluate existing privileges of the Application Administration team to determine if segregation of duties can be enforced by the system without significantly impacting ongoing operations and maintenance of CDFI Fund business applications.

2. The CDFI Fund will document the risk assessment and acceptance of not having the system enforce segregation of duties, and implement effective controls to mitigate the risk of unauthorized access and activity.