DATE: July 7, 2010

REPLY TO
ATTN OF: 04703-2-KC (4)

TO: Dallas Tonsager
Under Secretary
Rural Development

FROM: Gil H. Harden /s/
Assistant Inspector General
for Audit

SUBJECT: Weaknesses in Controls that Segregate Key Duties Single Family Housing Direct Loans Recovery Act Controls – Phase II

The American Recovery and Reinvestment Act of 2009 (Recovery Act) included $1 billion for the Rural Housing Service (RHS) to provide single-family housing direct loans to borrowers.[1] Congress, in enacting the Recovery Act, emphasized the need for accountability and transparency in the expenditure of funds. The Office of Management and Budget (OMB) subsequently issued guidance that required Federal agencies to establish rigorous internal controls, oversight mechanisms, and other approaches to meet the accountability objectives of the Recovery Act.[2]

RHS, an agency within the Rural Development mission area, is responsible for distributing Recovery Act funds through the Section 502 Single-Family Housing (SFH) Direct Loan Program.[3] These loans are available for very-low and low income households that cannot qualify for other credit to obtain homeownership. Applicants may obtain 100 percent financing to purchase an existing dwelling, purchase a site and construct a dwelling, or purchase newly constructed dwellings located in rural areas. As of June 29, 2010, RHS has obligated approximately $1.1 billion in direct loans to about 8,400 very-low and low income borrowers.

Our role, as mandated by the Recovery Act, is to oversee agency activities and to ensure agencies expend funds in a manner that minimizes the risk of improper use. We identified weaknesses in controls involving authorizations to initiate, approve, obligate, and disburse loans that could allow possible fraudulent activity. This Fast Report is the fourth in a series that will report on our oversight activities regarding SFH direct loans. Issues identified in these Fast Reports will be compiled into a final report at the conclusion of our audit.

---

[1] The American Recovery and Reinvestment Act, Public Law 111-5, was signed into law on February 17, 2009. The program level subsequently increased to about $1.56 billion due to changes in the subsidy rate for fiscal year 2010.
[2] *Initial Implementing Guidance for the American Recovery and Reinvestment Act of 2009*, February 18, 2009, and *Updated Implementing Guidance for the American Recovery and Reinvestment Act of 2009*, April 3, 2009.
[3] SFH Direct Loans are authorized by Title V of the Housing Act of 1949 under Section 502. 7 Code of Federal Regulations Part 3550 provides the policies for the SFH Direct Loan Program.

The audit objectives are to test the effectiveness of the management controls for the Recovery Act-funded Section 502 SFH Direct Loan Program. To accomplish our overall objective, we tested the effectiveness of Rural Development's separation of duties controls over access authorities to initiate, approve, obligate, and disburse loans in its loan origination system (LOS)[4] and its mortgage servicing system (MSS).[5]

We reviewed information obtained from Rural Development's Information Technology Internal Control Office (IT-ICO), located in St. Louis, Missouri, listing all LOS and MSS users, including their MSS Profile IDs.[6] We analyzed these data listings obtained to identify Rural Development personnel assigned special MSS Profile IDs. We then cross-referenced these IDs to determine their access authorities in LOS. We also obtained and reviewed the unnumbered letters dated July 2, 2008, and September 18, 2008, issued by Rural Development's national office to States.[7] These letters outlined justifications needed for making special Profile IDs available to MSS users.

In addition, we interviewed officials in Rural Development's Centralized Servicing Center (CSC), Missouri and Kansas State offices, and Rural Development's national office and the IT-ICO to discuss the number of Rural Development staff approved for the special Profile IDs. We discussed how Rural Development monitors individual usage of the authorizations provided by the special MSS Profile IDs to ensure they are not being abused.

Based on our review, we identified 149 Rural Development personnel that were given multiple access authorities; this significantly increased the risk that improper activities and errors may go undetected in the SFH Direct Loan Program. Specifically, we found 88 Rural Development personnel with an MSS Profile ID (Profile ID A) in 38 States, which identifies employees with loan approval authority that are also authorized to obligate and disburse Section 502 Direct SFH loans.[8] Of these 88 employees, we identified 70 that also have access to the LOS, which allows them to initiate the loan making process. In addition, we identified 108 Rural Development personnel with an MSS Profile ID (Profile ID B), which gives these employees multiple authorities to obligate and disburse Section 502 Direct SFH loans in 42 States, but who do not have loan approval authority.[9] We found 79 of these users also have access to the LOS. Although personnel with MSS Profile ID B are not delegated loan approval authority, like Profile ID A, according to Rural Development's IT- ICO officials, nothing in either system prevents individuals, given both access to LOS and the authority in MSS to obligate and disburse, from solely processing an entire loan from application to disbursement.

---

[4] A personal computer-based application used by loan originators in each Rural Development field office. LOS retains application information, calculates maximum loan amounts, and generates loan approval and closing forms. It is part of Rural Development's Dedicated Loan Origination System (DLOS).

[5] The mainframe-based computer application that is used by Rural Development field offices to electronically communicate with, and transmit information to, the Centralized Servicing Center (CSC), and by CSC to service and track borrower's loans. MSS is also part of DLOS.

[6] The MSS ID defines the "level of authority" a user has in the DLOS to approve, obligate, and/or disburse a loan.

[7] Unnumbered Letter, dated September 18, 2008, described the authorities associated with a new MSS Profile ID. These were RHCDS/Check Request or Cancel and RHCDS/Obligation Request Validation. This unnumbered letter also provided guidelines concerning the assignment of this Profile ID. This Profile ID was developed to identify MSS users that also have been granted loan approval authority by their respective State offices. Unnumbered Letter, dated July 2, 2008, describes the authorities associated with another new MSS Profile ID. These were also RHCDS/Check Request or Cancel and RHCDS/Obligation Request Validation, but identified users without loan approval authority.

[8] The analysis identified a total of 95 users with MSS Profile ID A. Of these 95, we identified 7 duplicate users, based on name, resulting in the 88 individuals.

[9] Our analysis identified a total of 120 users with MSS Profile ID B. Of these 120, we identified 12 duplicate users, based on name, resulting in the 108 individuals.

Our analysis of the user information provided by the IT-ICO identified 17 State offices where there were a high number of users (4 or more) with MSS Profile IDs A and B distributed between the State and Area Office employees (see table below). The high number of users with these elevated authorities presents a risk for potential improper activities. Broad accesses to initiate, approve, obligate, and disburse loans creates potential for misdirecting loans or funds for personal use, to personal friends or family members, or to particular realtors and/or contractors, among many other possibilities.

National Institute of Standards and Technology (NIST) defines that an organization separate duties of individuals as necessary to prevent malevolent activity without collusion through assigned information system access authorizations.[10] NIST also defines that an organization employ the concept of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.[11] When access authorizations do not adequately separate assigned duties, we believe other compensating controls should be implemented to monitor the activity of the users with multiple accesses to ensure authorities are not abused and no improper activity has occurred.

Rural Development officials acknowledged the increased risk of improper activities and errors that may go undetected with the use of these special MSS Profile IDs. However, they justified giving these MSS Profile IDs in some States because, in many field offices, there may be only one or two employees who work on SFH direct program loans. If one person is on leave or sick, the loan processing, closing, or disbursement of loan funds could be unreasonably delayed or halted.

The Table that follows lists the 17 State offices with a high number of users with MSS Profile ID A or Profile ID B that also have access to the LOS.

No.	State Office	ID A SO Users with LOS Access	ID A AO Users with LOS Access	ID B SO Users with LOS Access	ID B AO Users with LOS Access	Total MSS Users with LOS Access
1	GA	0	0	3	1	4
2	HI/GU/WP	1	1	1	1	4
3	ID	2	5	1	1	9
4	IL	0	0	5	0	5
5	IN	1	1	0	3	5
6	LA	0	0	3	1	4

[10] NIST Special Publication 800-53, Revision 3, Information Security, Access Control-5 (AC-5).
[11] NIST Special Publication 800-53, Revisions 3, AC-6, Least Privilege.

No.	State Office	ID A SO Users with LOS Access	ID A AO Users with LOS Access	ID B SO Users with LOS Access	ID B AO Users with LOS Access	Total MSS Users with LOS Access
7	MO	2	5	1	0	8
8	MT	2	0	2	0	4
9	NV	2	0	1	2	5
10	NJ	2	1	0	2	5
11	NY	2	2	1	0	5
12	NC	0	0	2	2	4
13	OR	2	0	2	0	4
14	PA	2	0	1	2	5
15	UT	2	2	0	0	4
16	VT/NH	1	0	3	2	6
17	WY	1	3	1	0	5

Effective controls to mitigate the risk for the authorities granted in MSS Profile IDs like Profile ID A and Profile ID B generally require, at a minimum, automated logging of the on-line activities of employees with these IDs and particularly loan obligations and check requests. Additionally, the log(s) of these employees' activities should be independently reviewed and monitored on a frequent basis to ensure the authorities are not abused and no improper activity has occurred.

We met with the IT-ICO staff to discuss automated or manual controls implemented to monitor usage of authorities granted by Profile IDs A and B. Our review disclosed that there were no automated controls in place in the LOS or MSS that would identify instances where users with these authorities exercised initiation, approval, and/or disbursement authorities on the same loan. Rural Development officials stated they did not generate any specific reports or logs or perform any other special procedures to monitor activity by users with these profile IDs. When we asked if the system had the capabilities to generate logs or other reports that could be used to monitor the activity of staff with multiple authorities, Rural Development officials stated that they could generate such reports if requested. However, they said that the only control currently implemented was that the security officer who assigned these profile IDs was to make sure that State or national office officials requesting these authorities provided justification for initializing the access privileges.

In more recent discussions, we learned that Rural Development first became aware during its Fiscal Year 2007 annual OMB Circular No. A-123, Appendix A, tests that the threat of not logging the employees' activities for the MSS created vulnerability, that suspicious activity was not being reviewed, and the opportunity of detection was lost. As part of the process to complete the auditing and monitoring milestones identified in the Agency's plan of action, a cost-benefit and risk mitigation analysis was conducted on the MSS application. The cost-benefit analysis described manual and automated compensating controls that the Agency maintains reduced the risk of program dollars lost (or risk value) to a level less than the cost of implementing the automated logging controls.[12] Consequently, Rural Development's Chief Information Officer signed a document forgoing the implementation of these automated logging controls.

We agree that it is senior management's responsibility to implement the most appropriate controls to decrease risk to an acceptable level at the least cost. Although we did not audit all the controls listed in Rural Development's cost-benefit analysis in this review, we found one of the compensating controls listed that would be effective to address multiple access authorizations was only partially in place, and Rural Development relied on this control in the cost-benefit analysis to significantly reduce the risk value. The control requires the national office to monitor the activity of all employees who approve loans and concurrently access the system to obligate loans and/or disburse checks. Rural Development implemented a control to ensure that any such access must be approved by national office program staff before granting the authorities. We agree with this control, but believe the activities of these employees must also be monitored periodically, either manually or automated, to significantly reduce the risk of improper activity in the SFH Direct Loan Program. This additional control, however, is not being performed at the national office level.

In a subsequent discussion with Rural Development national office officials on March 26, 2010, we were told that the responsibility for monitoring separation of duties for the authorities granted by these profile IDs was delegated to the States. They further stated that no monitoring procedures or guidance had been issued to the States, outside of the unnumbered letters. They did state, however, that on Form RD 3550-25, Loan Closing Instructions and Loan Closing Statement, there is a separation of duties certification where the Loan Approving Official enters the names of staff members who verified the borrower's income and credit, obligated the funds in the MSS, and activated the loan in the MSS. However, procedures do not require an independent verification as to the accuracy and completeness of this information or to determine that the same official did not perform all actions on the same loan. Rural Development officials added that this certification is routinely reviewed during their State Internal Reviews (SIR). However, from our analysis of the SIRs, we found these reviews are only performed once every 5 years at field offices in each State and only require looking at whether the Separation of Duties certification on Form RD 3550-25 was completed.

In our follow-up discussion with Rural Development officials on March 26, 2010, they agreed with our concern with the broad authorities granted by the MSS Profile IDs. They commented

[12] Rural Development's Risk Mitigation Analysis described the compensating controls as: 1) Physical Security, 2) Firewalls, 3) LAN Access to Network Activity Directory, 4) LOGBOOK Controls for Elevated Access, 5) Limited State Access, 6) Separation of Duties within MSS, 7) National Monitoring of Loan Approval Authority, 8) Transaction Level Thresholds, 9) MSS Access Limited to Roles Established, 10) DCFO/Treasury Controls.

that in the case of field offices with few staff who work on SFH direct loans, it is difficult, and in some cases, not possible to attain true separation of duties. They reemphasized that controls monitoring usage of the MSS Profile IDs should be at the State office level and automated logging controls would be costly to implement. Further conversations confirmed that there is no formal guidance requiring monitoring of the usage of these MSS Profile IDs. Follow up with State office officials in Missouri and Kansas confirmed that there was no monitoring requirement; therefore, no control is currently in place.

We recommend that the Rural Development national office:

1. Develop procedures and controls, utilizing existing capabilities, to monitor loan approval, obligation and disbursement activities of users with MSS Profile IDs A or B. These monitoring activities should be documented and readily identify when a user exercises multiple authorities on the same loan. The monitoring process should be reviewed frequently by Rural Development officials at an appropriate level to investigate the circumstances surrounding the suspicious use of these authorities and determine whether concurrent use of these authorities on a single loan was justified.

2. Require each State to reevaluate the current authorizations to determine whether the individuals assigned these multiple authorities have an absolute need for them, based on the concept of least privilege. Also, determine whether LOS access is necessary for those staff members granted these multiple authorizations.

Please provide a written response within 5 days outlining your proposed corrective action for this issue, including timeframes for implementation of those actions. If you have any questions, please contact me at (202) 720-6945, or have a member of your staff contact Steve Rickrode, Director, Rural Development and Natural Resources Division, at (202) 690-4483.

USDA'S

RURAL DEVELOPMENT

RESPONSE TO AUDIT REPORT

United States Department of Agriculture
Rural Development
Office of the Under Secretary

TO: Gil H. Harden
Assistant Inspector General for Audit

July 15, 2010

FROM: Dallas Tonsager /S/
Under Secretary
Rural Development

SUBJECT: Single Family Housing Direct Loans Recovery Act Controls – Phase II
04703-2-KC (4)

This is in response to your memorandum, dated July 7, 2010, in which you requested a response to your recommendations contained in the subject report. The recommendations resulted from your audit of the controls associated with the Section 502 Single Family Housing (SFH) Direct Loan Program.

In this review, OIG looked at the effectiveness of Rural Development's separation of duty controls over access authorities to initiate, approve, obligate, and disburse loans in its loan origination and mortgage servicing systems. The review identified 149 users with multiple system access authorities (70 of which have loan approval authority) which OIG indicated posed an increased risk that improper activities and errors may go undetected.

Considerable discussion was held regarding the following control identified in the Rural Development Chief Information Officer's memorandum:

> **National Monitoring of Loan Approval Authority** – all employees that can approve a loan are monitored and their access to the obligation and/or check disbursement template is monitored and must be approved by National Office Program staff.

This control was implemented through the unnumbered letters dated July 2, 2008 and September 18, 2008; both of which were titled, "MortgageServ Access/Separation of Duties."

Rural Development expended significant effort in reviewing system access for each user. Every user with multiple access authority was recommended for such access by the State Office based on demonstrated need and each case was approved by the National Office. OIG is interpreting this control to mean that there should be ongoing National Office monitoring of the activity of all employees who approve loans and concurrently access the system to obligate loans or disburse checks. This is not the intent of this control.

While we agree that additional monitoring of activities such as those recommended in your report would further strengthen our internal controls, we do not believe that the National Office is the appropriate place to undertake such activities. As such, we will develop and implement a manual process to require State Office monitoring of loan approval, obligation and disbursement activities for users with MortgageServ Profile IDs [redacted] within 90 days. At the same time, we will continue to explore automated alternatives should a viable option be identified. In addition, we will require each State to reevaluate the current authorizations for those with multiple authorities on an annual basis to assure there is an absolute need for these authorities including access to the UniFi system.

If you have any questions regarding this memorandum, please contact the Single Family Housing Direct Loan Division at (202) 720-1474.