U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

# Audit Report

## Security and Application Controls - Rural Development's Dedicated Loan Origination and Servicing System

Report No. 85501-1-FM
February 2007

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington DC 20250

February 12, 2007

REPLY TO
ATTN OF: 85501-1-FM

TO: Russell Davis
Administrator
Rural Housing Service

THROUGH: John Dunsmuir
Audit Liaison
Financial Management Division

FROM: Robert W. Young /s/
Assistant Inspector General
for Audit

SUBJECT: Security and Application Controls - Rural Development's Dedicated Loan Origination and Servicing System

This report presents the results of our audit of security and application controls in Rural Development's Dedicated Loan Origination and Servicing (DLOS) system. The report identifies improvements needed in the security program relating to oversight, documentation, and access. The report also discusses the need to strengthen the management of change controls.

Your response to our draft report is included in its entirety in exhibit B, with excerpts in the Findings and Recommendations sections of the report. Based on information provided in the response, we have reached management decision on Recommendations 1, 3, 5, 6, 7, 8, 11, and 13. For the remaining recommendations, please refer to the OIG Position section of the report for specific details as to the information needed to reach management decision. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer for the recommendations for which management decision has been reached.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendations noted above. Please note that the

regulation requires management decision to be reached on all findings and recommendations within 6 months from report issuance.

We appreciate the courtesies and cooperation extended to us during the audit.

# *Executive Summary*

***Security and Application Controls - Rural Development's Dedicated Loan Origination and Servicing System (Audit Report No. 85501-1-FM)***

## Results in Brief

Rural Development uses the Dedicated Loan Origination and Servicing (DLOS) system to originate and service direct Single Family Housing (SFH) loans, which accounted for over 378,000 loans with an outstanding principal balance of over $13 billion as of the end of fiscal year 2005. Servicing activities included payments received of over $1.1 billion. Our objectives were to evaluate whether Rural Development had adequate and effective controls to ensure transactions were properly authorized and processed, and proper segregation of duties was maintained. Overall, we found that Rural Development had not implemented adequate controls to adequately protect the integrity of the data. Ultimately, this may affect Rural Development's ability to adequately manage its SFH direct loan portfolio.

Management is responsible for developing, implementing, and maintaining effective internal controls. The three objectives of internal control are to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Appropriate internal control should be integrated into each system established by agency management to direct and guide its operations.[1] While Rural Development had implemented significant controls within the DLOS system, we noted that further improvements were needed. Rural Development had not established an effective security program that adequately documented its security plans, risk assessments, and disaster recovery/contingency plans. Rural Development had not conducted a thorough certification and accreditation (C&A) and appropriately established interconnection security agreements for its interconnecting systems. Rural Development had hired contractors to prepare the documentation supporting the certification of the system; however, it did not adequately monitor their compliance with the guidance provided by OMB and the National Institute of Standards and Technology. As a result, all security controls may not have been identified and tested. In addition, there was ineffective management and oversight of information technology resources that unnecessarily exposed critical loan portfolio information to the risk of disclosure, modification, or deletion.

Material weaknesses existed in Rural Development's ability to effectively control access to sensitive data within the DLOS system. Rural Development had not established and implemented effective internal controls to ensure that (1) access to system software and hardware was adequately limited, (2) user identifications belonging to former employees were timely removed, (3)

[1] Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004.

users had only the access needed to perform their job functions, and (4) monthly verification of user access was correctly performed. For example, the monthly monitoring reports were poorly designed in that they only provided who had access and not the type of access (e.g., "Read," "Write," etc.). As a result, Rural Development had not adequately restricted access based on job responsibilities, monitored access for all its employees, and/or conducted the agreed-upon review of access rules.

Material weaknesses continued to exist within Rural Development's processes to effectively control system software changes. Rural Development had not established and implemented effective internal controls to ensure that system software changes were properly (1) authorized, (2) supported by change request documents, (3) tested, and/or (4) monitored when migrated into production. We noted that Rural Development had a configuration management control system in place; however, personnel were circumventing the policies and procedures for using the system, rendering the controls ineffective. Without proper software change controls, Rural Development could not be assured that DLOS system functions were performing as intended. As a result, there was increased risk that data may become unreliable and that malicious programs may be introduced and/or security features may be inadvertently or deliberately omitted or rendered inoperable.

We believe that the findings in this report, taken as a whole, constitute a material internal control weakness and should be reported in the agency's Federal Managers' Financial Integrity Act report.

## Recommendations In Brief

We recommend that Rural Development:

- Ensure that the DLOS system security plan accurately references Information Technology Services (ITS) and National Information Technology Center (NITC) documents, and that adequate documentation is maintained to verify that all controls in the security plan were implemented.

- Perform a C&A which fulfills the requirements of full system accreditation by establishing effective configuration management and continuous control monitoring. Additionally, ensure that the C&A includes adequate Security Testing and Evaluation testing and appropriate supporting documentation.

- Establish agreements with all entities with systems connecting with the DLOS system, NITC, and ITS general support systems that

include rules of behavior and controls that must be maintained by the interconnecting systems.

- Remove all inappropriate "Write" accesses to the DLOS system production libraries that were identified by the audit. Establish controls to ensure excessive permissions are not assigned.

- Establish controls to ensure staff and contractors do not exceed assigned levels of authority by modifying dataset rules to elevate privileges within production libraries. Ensure all testing of dataset rules is completed within the test libraries.

- Enable logging through Access Control Facility 2 (ACF2) of all "Write" accesses to production libraries. Establish controls to ensure the logging report is reviewed on a daily basis.

- Establish controls to ensure system software changes are properly authorized, tested, and documented prior to migration to the production environment.

**Agency Response.** Rural Development generally agreed with the findings and recommendations in this report. Its response is provided in its entirety in exhibit B. However, Rural Development did not agree with Recommendation 4, to revise its Disaster Recovery Plan (DRP). Rural Development notes that mainframe recovery is more crucial to restoring operations and the mainframe component can be used in lieu of the web-based component to collect loan data.

**OIG Position.** We were able to reach management decision on Recommendations 1, 3, 5, 6, 7, 8, 11, and 13. Our position on what is needed to reach management decision on the remaining recommendations is included in the Findings and Recommendations section of the report. Regarding Recommendation 4, the DRP needs revision to document usage of the mainframe system to record data normally recorded in the web-based component.

## *Abbreviations Used in This Report*

| | |
|---|---|
| ACF2 | Access Control Facility 2 |
| ASSERT | Automated Security Self-Evaluation and Remediation Tracking |
| C&A | certification and accreditation |
| CCB | Configuration Control Board |
| CS | Cyber Security |
| CSC | Centralized Servicing Center |
| DLOS | Dedicated Loan Origination and Servicing |
| DM | Departmental Manual |
| DRP | Disaster Recovery Plan |
| FTP | File Transfer Protocol |
| ISA | interconnection security agreement |
| ID | identification |
| ISSS | Information Systems Security Staff |
| IT | information technology |
| ITS | Information Technology Services |
| MOU | memorandum of understanding |
| NIST | National Institute of Standards and Technology |
| NITC | National Information Technology Center |
| OCIO | Office of the Chief Information Officer |
| ODCFO | Office of the Deputy Chief Financial Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| SFH | Single Family Housing |
| SLA | service level agreement |
| SP | Special Publication |
| SRB | System Review Board |
| SSP | System Security Plan |
| USDA | U.S. Department of Agriculture |

# Table of Contents

# Background and Objectives

## Background

One of the goals of Rural Development is to improve the quality of life through the U.S. Department of Agriculture (USDA) financing of affordable, quality housing. The Rural Development Single Family Housing (SFH) program has traditionally served as a source of financing for borrowers who could not obtain credit elsewhere, or could not afford to pay commercial interest rates.

The Dedicated Loan Origination and Servicing (DLOS) system is used by Rural Development to originate and service direct SFH loans for the Centralized Servicing Center (CSC) located in St. Louis, Missouri. This system, which consists of the UniFi loan origination and the MortgageServ loan servicing components, was significantly enhanced to accommodate the unique requirements of SFH loan programs. Implementation of the system brought new servicing capabilities to the agency such as escrowing, forced-placed insurance, pre-determined amortization schedules, and default management.

Borrower loan application data is input into the web-enabled UniFi system at local Rural Development servicing offices located throughout the United States. The data is uploaded to the MortgageServ system on the National Information Technology Center (NITC) mainframe during the nightly update. Loan servicing data is input into the MortgageServ system from personal computers located at the CSC.

The SFH system includes an online transaction entry and inquiry capability accessed by about 800 field offices, CSC, the national office, and the Office of the Deputy Chief Financial Officer (ODCFO). Updates are done both online real-time and through nightly batch processes. CSC is the primary user and ODCFO has overall financial and accounting responsibility. SFH operations include online inquiry and transaction input, pre-application and application processing, loan making and servicing transaction updates, portfolio management, daily register, balancing, program reporting, and financial reporting.

As of the end of fiscal year 2005, DLOS accounted for over 378,000 loans with an outstanding principal balance of over $13 billion. Servicing activities recorded in DLOS during fiscal year 2005 included payments received of over $1.1 billion.

Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer. They are commonly categorized into three phases of a processing cycle as follows.

- Input data are authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner.

- Processing data are properly processed by the computer and files are updated correctly.

- Output files and reports generated by the application accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

## Objectives

Our objective was to determine whether selected security and application system controls (manual or automated) were in place and functioning effectively to ensure transactions were properly authorized and processed, and proper segregation of duties was maintained.

# Findings and Recommendations

## Finding 1 — Management Oversight and Documentation Need Improvement

Management is responsible for developing, implementing, and maintaining effective internal controls. The three objectives of internal control are to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Appropriate internal control should be integrated into each system established by agency management to direct and guide its operations.[2] While Rural Development had implemented significant controls within the DLOS system, we noted that further improvements were needed. Rural Development had not established an effective security program that adequately documented its security plans, risk assessments, and disaster recovery/contingency plans. Rural Development had not conducted a thorough certification and accreditation (C&A) and appropriately established interconnection security agreements (ISA) for its interconnecting systems. Rural Development had hired contractors to prepare the documentation supporting the certification of the system; however, it did not adequately monitor their compliance with the guidance provided by OMB and the National Institute of Standards and Technology (NIST). As a result, all security controls may not have been identified and tested. In addition, there was ineffective management and oversight of information technology (IT) resources that unnecessarily exposed critical loan portfolio information to the risk of disclosure, modification, or deletion.

Although Rural Development had taken some actions since our last audit[3] to comply with security requirements, our review disclosed that additional actions were needed in the following areas.

Risk Assessments

Risk assessments, as defined by NIST, are a systematic approach to assessing the vulnerability of information system assets; identifying threats, quantifying the potential losses from threat realization; and developing countermeasures to eliminate or reduce the threat or amount of potential loss.

[2] Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004.
[3] Audit Report No. 85099-4-FM, *Review of Rural Development's Information Technology Resources Security*, dated March 2004.

The risk assessment for the DLOS system contained a detailed description of the physical security controls that were tested (including observation of network distribution closets stationed within the open working environment). However, the description of physical controls and the observation was for the Goodfellow facility, not the Market Street facility where the Web farm[4] hosting UniFi was located. In addition, the threat and impact analyses were inadequate. For example, the risk assessment defined what a threat and impact analyses was, but did not describe how the definition was applied.

Rural Development personnel stated the risk assessment was completed using Office of the Chief Information Officer-Cyber Security (OCIO-CS) guidance available at that time; however, the risk assessment was dated February 12, 2004, while USDA Risk Methodology issued by OCIO-CS was dated February 11, 2003, a full year earlier. Our comparison of USDA Risk Methodology to NIST requirements indicated that the OCIO-CS document included guidance for the same requirements we noted as missing in the DLOS system risk assessment. As a result, Rural Development could not be assured that all risks attributable to this mission-critical system had been considered and that appropriate steps had been taken to mitigate those risks.

System Security Plan

OMB Circular No. A-130[5] requires agencies to plan for the adequate security of each major application, taking into account the security of all systems in which the application operates. The security plan is to be consistent with guidance issued by NIST. In addition, both NIST[6] and OCIO[7] provide guidance on the preparation of security plans.

Specifically, we noted:

- Inconsistencies between the security plan and other system documentation;

- references to NITC and Information Technology Services' (ITS) documentation for explanation of controls, but those explanations were not included in the NITC or ITS documents; and

[4] A Web farm is a company that provides infrastructure, management, content, and sometimes even fulfillment for their clients' e-business applications. Typically the Web farm will comprise at least two servers.
[5] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000.
[6] NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems*, dated December 1998, was used in our review of the DLOS system security plan. NIST issued a revised SP 800-18 in February 2006 that requires agencies to document their security controls related to NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, dated February 2005, and Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006.
[7] Departmental Manual (DM) 3565-001, *Annual Security Plans for Information Technology Systems*, dated February 17, 2005.

- limited documentation to verify that all controls in the security plan were implemented.

Disaster Recovery/Contingency Planning

We noted that Rural Development used multiple plans for contingency/disaster recovery for the DLOS system. However, because DLOS consists of both a mainframe and webserver component that reside on the general support systems owned by NITC and ITS, recovery planning must be coordinated with those agencies. Depending on the location and type of event, NITC's and/or ITS' Disaster Recovery Plans (DRP) would be executed first, in order to provide the application IT infrastructure required to recover the DLOS system.

According to NIST,[8] recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. In addition, teams should be sufficient in size to remain viable if some members are unavailable to respond or alternate team members may be designated. Also, the contingency planning coordinator should consider that a disaster could occur that would render a majority or all personnel unavailable to respond. In this situation, executing the plan may be possible only by using personnel from another geographic area of the organization or by hiring contractors or vendors.

We reviewed the DRPs for the NITC mainframe and ITS Web farm as they relate to the recovery of the DLOS system. While the NITC mainframe DRP appeared adequate to restore the mainframe application, Rural Development needs to ensure that ITS has the necessary information to restore the web-based DLOS system application. For example, Rural Development had not supplied ITS with system software and documentation needed in order for ITS to restore the DLOS system. Additionally, Rural Development's DRP indicated DLOS must be recovered within 5 days; however, the ITS DRP showed that 5 or more weeks might be needed to recover the system. Lastly, Rural Development's IT Contingency Plan differed from the ITS DRP as to the alternate site for restoring the DLOS system web-based application.

We also noted the following during our review of the DLOS system DRP.

- Team members for both the DLOS system mainframe and Web farm recovery and reconstitution activities were all located in the St. Louis, Missouri office. The plans did not take into consideration a disaster that might occur rendering a majority or all personnel unavailable to respond, and the need for personnel from

[8] NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, dated June 2002.

another geographic area to execute the plan. In addition, some teams contained only one or two members and did not provide sufficient team size to remain viable if some members are unavailable to respond.

- Recovery procedures were not presented in a straightforward step-by-step style. For example, one step for the functional support team was to verify that internal security controls were in place and that user access controls were working properly; however, the plan did not identify internal security controls or user access controls or the steps to take to verify those controls.

Certification and Accreditation

Although the DLOS system underwent a C&A as required by OMB and NIST, the process was inadequate.

- In a prior audit report,[9] we noted that (1) supporting documentation did not meet NIST and Department guidelines; (2) agencies and their contractors had not conducted adequate Security Testing and Evaluations; and (3) agencies had not fulfilled the requirements of full system accreditation by establishing effective configuration management or continuous control monitoring.

Our review disclosed the same weaknesses for the DLOS system C&A effort.

Interconnecting Systems

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data stored, processed, and/or transmitted on those systems.

OMB Circular No. A-130 requires that written management authorization, often in the form of a memorandum of understanding (MOU) or an ISA, be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems.

The DLOS system security plan identified 11 interconnecting systems for which an ISA is needed between Rural Development and the owner of the

[9] Audit Report No. 50501-4-FM, *Review of the USDA's Certification and Accreditation Efforts*, dated October 2005.

interconnecting system. We obtained copies of the ISAs for seven of those interconnecting systems, and found the ISAs had not been finalized.[10]

Also, the security plan identified an additional nine interconnecting systems where Rural Development documented that NITC was responsible for the ISA. NITC security personnel indicated that there were two ISAs with the U.S. Department of the Treasury for services provided across its customer base; however, the other seven agreements are unique to Rural Development and not NITC's responsibility.

NITC Security Directive 1.2, *NITC Customer Security Boundaries and Responsibilities*, dated March 26, 2003, established security boundaries and responsibilities of NITC and its customers. It states that application owners have security management responsibility for their application systems while NITC will provide security administration for customer computer platforms only as specified by a MOU or service level agreement (SLA).

The Rural Development security plan stated that a SLA existed for the general support systems used by the DLOS system, including NITC, ITS, and the ITS Web farm. The NITC SLA was a generic document, not specific to Rural Development or to the DLOS system. The SLA did not outline the management, operation, and use of the interconnection as required by NIST.

In addition, Rural Development maintains only one ISA with ITS and the ITS Web farm. OMB requires the interconnection agreement to define the rules of behavior and controls that must be maintained for the system interconnection. We noted that the ISA limited security services to patch management, vulnerability scanning, logical access control, and incident response. The ISA further stated that the remainder of the security services provided would be defined in the future.

## Recommendation 1

Revise the DLOS system risk assessment to accurately describe controls and sites tested and adequately addresses threat and impact analyses.

**Agency Response.** Rural Development's Information Systems Security Staff (ISSS) utilized the USDA OCIO mandated Automated Security Self-Evaluation and Remediation Tracking (ASSERT) automated tool to document compliance with security controls to identify vulnerabilities, and to build remediation plans for the DLOS system. In addition, Rural Development recently performed the annual detailed risk assessment which addresses threat identification and impact analysis. Risks identified are tracked and reported

[10] Of the 11 interconnecting systems identified in the security plan, 2 systems no longer connected with DLOS, 2 systems were owned by the same entity requiring only 1 ISA, and an ISA did not exist for 1 entity.

via the ASSERT reporting tool. The risk assessment, a living document, was updated in August 2006 and is available for review.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

### Recommendation 2

Ensure that the DLOS system security plan accurately references ITS and NITC documents, and that adequate documentation is maintained to verify that all controls in the security plan were implemented.

**Agency Response.** Rural Development received updated draft C&A condensed guidance and templates from OCIO-CS in October and November 2006. OCIO-CS continues to modify its guidance and templates and will distribute new versions to the agencies as the drafts are approved for release. The draft documents state that the guidance is the result of a review of the USDA C&A policy and guidance to bring it closer to standardized NIST and OMB recommendations. A goal of the new C&A strategy is to standardize the base C&A process with NIST SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems,* and clearly distinguish where additional USDA processes, oversight, concurrency, or demands are required. Increased efficiency, enhanced clarification of expectations, and reduced investments of cost and time are the intended results. As always, Rural Development will ensure that the C&A is accomplished in compliance with existing Federal and Departmental guidance. The security controls are tested and vulnerabilities tracked in the OCIO-CS mandated ASSERT tool and the Security Test and Evaluation process.

Rural Development, NITC, and ITS are in the process of revising Systems Security Plans (SSP) to comply with the updated draft OCIO-CS C&A guidance and templates. The OCIO-CS revised policy requires a concurrency review by OCIO-CS after security certification, but before accreditation takes place. This concurrency review provides an additional and independent level of review to help ensure that Departmental and NIST guidelines are followed. Rural Development will validate NITC and ITS SSP references prior to forwarding C&A documentation to the designated accrediting authority.

The SSP is a living document and is constantly being updated to reflect the most recent data available.

**OIG Position.** In order to reach management decision, Rural Development needs to establish policies and procedures to ensure controls identified in the security plan are effectively implemented. Further, Rural Development needs to provide a date when the controls are put in place, and when the DLOS

system security plan will be updated to accurately reference ITS and NITC documents.

### Recommendation 3

Provide ITS with appropriate system software and documentation to restore the DLOS system, and eliminate inconsistencies between the ITS and DLOS system DRPs.

**Agency Response.** Rural Development is tracking and managing a reported vulnerability with the ASSERT tool regarding providing ITS with current updated UniFi documentation. This documentation will be provided to ITS by January 31, 2007. The DRP will be updated and provided to ITS by the end of the second quarter of fiscal year 2007. ITS' recovery time objectives are not current with those identified by the agency. ITS has committed to updating its DRP documentation and bringing it into agreement with Rural Development's by March 31, 2007.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

### Recommendation 4

Revise the DLOS system DRP to assign sufficient personnel to recovery teams and present recovery procedures in a straightforward step-by-step style.

**Agency Response.** The Office of Inspector General (OIG) does not recognize the two major system components of the DLOS system and the different degree of risk associated with these two components which result in them having different disaster recovery criteria. The DLOS system has a mainframe component (MortgageServ) and a web-based component (UniFi). The mainframe component is used to service all consumer loans and provides all supporting detail for amounts reported for these loan programs in the financial reports. The web-based component supports only the loan application process for these loan programs and does not contain any financial information. Therefore, the criticality for restoring these systems in a disaster recovery scenario is different. Further supporting this differentiation in criticality is the fact that the mainframe component has the capability to collect data on loan applications in the event the web-based component is disabled. In terms of business continuity and the need to recover critical systems, the web-based component recovery timeframe is longer than the mainframe component timeframe. This is by design to minimize the significant cost of maintaining redundant hardware in a separate location to support the recovery of the less critical web-based component.

The recovery of the DLOS system mainframe component is tested twice each year as part of the NITC disaster recovery exercise. The mainframe component has been successfully restored to the NITC hot-site multiple times. Following the completion of each disaster recovery exercise, an assessment is made as to the success of the test and any problems or issues that surfaced during the test are evaluated and corrective actions are taken prior to the next test. This is an ongoing process and the disaster recovery plan is continually being updated to incorporate any enhancements needed as identified through these tests.

Rural Development can find no guidance in Federal or Department publications that identifies a specific number of personnel required to recover software applications in a declared disaster. Rural Development believes it has exercised good judgment in identifying the appropriate personnel sufficient to recover the DLOS system.

**OIG Position.** OIG recognizes the two major system components of the DLOS system and the different degree of risk associated with these two components. Although Rural Development states that it does not need the web-based component to record loan information into the mainframe component, system documentation did not include procedures for recording loan application information into the mainframe component instead of the web-based component. In addition, field personnel had not been trained on those procedures. Therefore, procedures need to be established and included in the DRP, and training given to field personnel to provide knowledge for using the mainframe system to input data in the case of a disaster.

Additionally, although Federal or Department publications do not identify a specific number of personnel required to recover software applications in a declared disaster, as stated in our report, NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, provides that teams should be sufficient in size to remain viable if some members are unavailable to respond. We found that some teams contained only one or two members and did not provide sufficient team size to remain viable if some members are unavailable to respond.

We continue to believe our recommendation is appropriate and Rural Development needs to provide information that addresses the assignment of recovery teams of appropriate size, as well as, enhancing the DRP documentation to present procedures in a straight forward step-by-step style, including procedures for recording loan information into the mainframe component.

## Recommendation 5

Perform a C&A which fulfills the requirements of full system accreditation by establishing effective configuration management and continuous control monitoring. Additionally, ensure that the C&A includes adequate Security Testing and Evaluation testing and appropriate supporting documentation.

**Agency Response.** Rural Development has documented responses to specific C&A related recommendations outlined in OIG's report, specifically relative to risk assessments, SSPs, DRPs, interconnection security agreement, logical access controls, etc.

Rural Development received updated draft C&A condensed guidance and templates from OCIO-CS in October and November 2006. OCIO-CS continues to modify its guidance and templates and will distribute new versions to the agencies as the drafts are approved for release. Configuration management, continuous control monitoring, Security Test and Evaluation, and appropriate supporting documentation are included in the OCIO-CS guidance. The OCIO revised policy requires a concurrency review by OCIO-CS after security certification, but before accreditation takes place. This concurrency review provides an additional and independent level of review to help ensure that Departmental and NIST guidelines are followed.

The recertification is scheduled for completion by June 30, 2007.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

## Recommendation 6

Establish agreements with all systems connecting with the DLOS system, NITC, and ITS general support systems that include rules of behavior and controls that must be maintained by the interconnecting systems.

**Agency Response.** NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, sets forth guidelines for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by different organizations. Rural Development believes that all interconnections between systems maintained by the agency and support systems maintained by different organizations are adequately secured and meet the requirements for encryption of data and for establishing the connections between systems. We recognize that not all interconnections are documented by a written agreement and we are working on establishing these agreements. Draft revised guidelines and templates for

establishing these agreements were recently received from OCIO-CS. OCIO-CS continues to modify their C&A guidance and templates.

As the DLOS system is recertified, Rural Development will ensure compliance with all Federal and Departmental regulations relative to interconnecting systems. Recertification is scheduled to be completed by June 30, 2007.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

## Finding 2 Weaknesses Over DLOS System Access Controls

Material weaknesses continued to exist in Rural Development's ability to effectively control access to sensitive data within the DLOS system. Rural Development had not established and implemented effective internal controls to ensure that (1) access to system software and hardware was adequately limited, (2) user identifications (ID) belonging to former employees were timely removed, (3) users had only the access needed to perform their job functions, and (4) monthly verification of user access was correctly performed. The monthly monitoring reports were poorly designed in that they only provided who had access and not the type of access (e.g., "Read," "Write," etc.). As a result, Rural Development had not adequately restricted access based on job responsibilities, monitored access for all its employees, and/or conducted the agreed-upon review of access rules.[11] Without effective logical access controls, Rural Development's critical loan data is at risk of disclosure, modification, or deletion.

DM 3140-1[12] requires agencies to use individual user IDs and passwords to control access to systems processing personnel, financial, market-related, or other sensitive data. Further, Section 6c, requires staff to remove employee user accounts and passwords when the employee is no longer employed by the agency. OMB Circular No. A-130 lists individual accountability as a primary mechanism for personnel security. It recognizes that accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them.

[11] Based on weaknesses identified in Audit Report No. 85099-4-FM, Rural Development agreed to conduct an analysis of security software ACF2 rules for access to mainframe applications and general support systems.
[12] DM 3140-1, *Management ADP Security Manual*, Appendix D, Section 4.a.

Finally, Rural Development's *Data Security Manual*, dated February 16, 2000, states that user accounts must be disabled immediately when a user leaves Rural Development, when a user will be away from the office for 1 month or more, or when accounts are found to be inactive for longer than 90 days.

Despite raising this issue in our prior audits,[13] we continued to find that Rural Development had not complied with OMB, Departmental, or its own policies regarding user IDs and passwords. Rural Development had established a process of circulating user access lists to appropriate management; however, the process was not effective because the lists did not include the level of access granted to each user, and field personnel did not properly review the lists to identify users who no longer required the assigned system access. In addition, Rural Development had not performed the agreed-upon analysis of Access Control Facility 2 (ACF2)[14] rules for access to mainframe applications and the general support system. We also noted that security personnel did not have sufficient knowledge of ACF2 dataset rules to correctly grant access within the mainframe environment. The following illustrate the types of weaknesses we found.

- Although Rural Development indicated that it had removed "Write" access from the production libraries as a result of our prior audit, we found that of the 47 individual IDs with "Write" access to the production libraries including source code for MortgageServ, 24 did not need the access to perform their duties. In addition, we identified 9 IDs, not currently assigned to an individual user that still had access to production libraries. Finally, we identified 1 user that had left the agency over 1 year ago.

- We also identified 58 users with administrative access to UniFi. In addition to providing update access to production libraries, this access provides the ability to update and/or delete source code. Based on our review, Rural Development immediately deleted the administrative access for 46 of the 58 users, and restricted the access for an additional 8 users.

- We also identified a dataset that contained NITC IDs and passwords used for submitting batch File Transfer Protocol (FTP) jobs. The dataset name identified that this dataset contained passwords. We found that 47 users had "Read" and "Write" access to this dataset. Rural Development advised that the renaming and restriction of

[13] Audit Report No. 85099-4-FM, *Review of Rural Development's Information Technology Resources Security*, dated March 2004, and Audit Report No. 85099-2-FM, *Security Over Rural Development's Information Technology Resources Needs Improvement*, dated August 5, 2002.
[14] ACF2 is a program that enables security on mainframes. Access to a system is controlled by rules set up within the program.

access to this file was to be included in the scope of the ACF2 cleanup project.

- We noted that a contractor exceeded the authorized level of access. The contractor modified the dataset rule granting "Read," "Write," "Allocate," and "Execute" access to the DLOS system production libraries, including the source code. Three days later, the contractor again modified the dataset rule to remove the excessive access. In response to our questions, Rural Development explained that the contractor granted himself access to run and test a utility and subsequently removed the access.

The above instances could have been avoided if Rural Development had (1) adequately maintained access profiles based on job functions and separation of duties principles and (2) established an effective mechanism to periodically review the level of access granted to employees to ensure that it remains consistent with job functions and separation of duties principles.

Rural Development began taking steps during our audit to correct the material weaknesses identified. Rural Development had added a contract resource to support the ACF2 cleanup project.

### Recommendation 7

Remove all inappropriate "Write" accesses to the DLOS system production libraries that were identified by the audit. Establish controls to ensure excessive permissions are not reassigned.

**Agency Response.** Rural Development removed "Write" access to the DLOS system production libraries for all development personnel identified during the audit and during subsequent reviews. Physical evidence is available for review upon request.

Rural Development is developing documentation advising the user community of the revised procedures/controls requiring Information Technology Program Manager approval prior to granting ACF2 access. The documentation is scheduled to be issued by January 31, 2007.

In addition, DLOS production library access will be included in the quarterly verification report and procedures by April 30, 2007. The reports will be issued to the system owners to verify and sign the certification attesting to the accuracy and need for the access commensurate with employee job responsibilities.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

### Recommendation 8

Ensure the dataset that contained NITC IDs and passwords used for submitting batch FTP jobs is renamed and that access to this dataset is appropriately limited.

**Agency Response.** The dataset was renamed and access is very restricted. Final turnover to eliminate all references to the former name is scheduled for December 31, 2006.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

### Recommendation 9

Establish controls to review administrative accesses to the UniFi webserver to ensure that access is not granted to individuals who do not need the access to perform their job responsibilities.

**Agency Response.** Rural Development requested ITS to provide the agency with quarterly reports relevant to all software applications hosted by the ITS web farm. When received, these reports will be distributed to agency management staff consistent with procedures currently established to ensure the continued validation of access privileges to all agency web-based applications.

**OIG Position.** In order to reach management decision, please provide the date of implementation of the planned action for quarterly report distribution.

### Recommendation 10

Establish controls to ensure staff and contractors do not exceed assigned levels of authority by modifying dataset rules to elevate privileges within production libraries. Ensure all testing of dataset rules is completed within the test libraries.

**Agency Response.** Rural Development reemphasized the policy applicable to contractors with authority and responsibility to grant access privileges to agency personnel and especially in the granting of access privileges to themselves. ISSS established controls to test any changes to data set rules prior to deployment to production. Procedures have been updated to reinforce this policy and are available for review upon request.

Other actions that support resolution of this recommendation includes the recent recompetition of the ISSS support contract which resulted in the award of the contract to a new commercial vendor. In addition, recent hiring control

authority approval has allowed Rural Development to increase the staffing to provide the capability for more day-to-day monitoring and management of contractor support staff.

**OIG Position.** We concur with the corrective actions. However, in order to reach management decision, please provide the dates that these actions were taken.

### Recommendation 11

Modify verification reports to include the identification of authorities associated with all production libraries.

**Agency Response.** DLOS production library access will be included in the quarterly verification report and procedures by April 30, 2007. The reports will be issued to the system owners to verify and sign a certification attesting to the accuracy and need for the access commensurate with employee job responsibilities.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

### Recommendation 12

Document and implement access profiles based on job responsibilities and separation of duties principles.

**Agency Response.** A joint Information Resources Management and Centralized Servicing Center initiative was completed in March 2006 to create and implement role-based templates to be used to establish the appropriate access authority for each teller ID within the Centralized Servicing Center based on branch, section, unit, position, and template number. The instructions for completing the automated log book form for national office program staff and for Centralized Servicing Center employees currently instruct staff to specify the template number when requesting changes to a teller ID or when establishing a new teller ID.

The automated log book form used by field office staff has been modified to distinguish between roles that require obligation authority within MortgageServ and those that do not require obligation authority.

In addition, ISSS updated desk procedures over a year ago to cease copying access privileges from one user to another by not allowing the requesting agency official to request ISSS to provide an employee with the same authorities given to a current employee. Forms and desk procedures were updated throughout the year to fully document and support the cessation of

this procedure, but the practice itself was stopped over a year ago. Managers must now specify exact MortgageServ access authorities requested for individual MortgageServ users.

Physical evidence is available for review upon request.

**OIG Position.** We concur with the actions outlined in Rural Development's response. However, please provide implementation dates in order to reach management decision.

## Finding 3 Application Change Controls Need Strengthening

Material weaknesses continued to exist within Rural Development's processes to effectively control system software changes. Rural Development had not established and implemented effective internal controls to ensure that system software changes were properly (1) authorized, (2) supported by change request documents, (3) tested, and/or (4) monitored when migrated into production. We noted that Rural Development had a configuration management control system in place; however, personnel were circumventing the policies and procedures for using the system, rendering the controls ineffective. Without proper software change controls, Rural Development could not be assured that DLOS system functions were performing as intended. As a result, there was increased risk that data may become unreliable and that malicious programs may be introduced and/or security features may be inadvertently or deliberately omitted or rendered inoperable.

DM 3575-001[15] states that changes to an information system can have a significant impact on the security of the system. The manual stresses that documenting changes to information systems is an essential aspect of maintaining the security accreditation. In addition, an effective configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, dated October 1995, recognizes that computer systems and environments in which they operate change continually. For both major and minor changes, the manual mandates system testing and appropriate documentation. According to NIST SP 800-37,[16] *Guide for the Security Certification and Accreditation of Federal Information Systems,* it is important to document the

[15] DM 3575-001, *Security Controls in the System Life Cycle/System Development Life Cycle*, dated May 27, 2005.
[16] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004.

proposed or actual changes to the information system and to subsequently determine the impact of those proposed or actual changes on the security of the system.

Further, OMB Circular No. A-130[17] emphasizes:

> Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Finally, DM 3520-001[18] requires a board be established to approve the baseline configuration management documentation; ascertain all of the benefits, risks, and impacts of changes before a decision is made to implement; defer or reject a change; and schedule new releases of systems. The scope of authority of the board is derived by a written charter approved by agency management. Rural Development's change control procedures require the System Review Board (SRB) to review all requests for change, determine the applicability, accept the request, and establish the priority sequence of change requests.

Rural Development procedures required a user to use Form RD 2006-15, "Request for Automation," to document and justify a request to modify a system. That form, when used correctly, guides the request through Rural Development's change control process including (1) prioritization and approval by the SRB, (2) unit level testing, (3) user acceptance testing, and (4) release of the change into the production environment.

Despite raising this issue in our prior audit, we continued to find that Rural Development had not complied with existing guidance. We noted that Rural Development had not performed the agreed-upon comprehensive review of the change control process for all major applications and the general support system.

Our review of 16 completed DLOS system changes disclosed that the changes were not properly authorized or approved before implementation. The following describes some of the system change weaknesses identified.

- None of 16 system changes used the correct change request form (Form RD 2006-15). As a result of our review, Rural Development indicated that it would require the use of the form for all future

[17] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 30, 2000.
[18] DM 3520-001, *Configuration Management Policy and Responsibilities*, dated July 15, 2004.

change requests.

- Only one change had test plans and results to demonstrate that the change was tested and approved before placed into production.

- Two changes were requested and approved by the same person.

- One change was migrated into production before user acceptance; another was migrated into production without testing.

- None of the 16 changes included evidence that the change was reviewed, accepted, or prioritized by the SRB. In addition, Rural Development was unable to provide a sample of the minutes where a request for change was actually approved by a majority of the voting members of the board, or where the actual priority of a newly accepted change request was accepted.

We also noted that unauthorized changes continued to be made within the DLOS system.[19] These changes were not made by the Rural Development configuration management staff or processed through its change management software.[20] Further, these unauthorized changes can rarely be traced back to the individual who made the change.

Based on our review, the configuration management staff indicated that it would prepare a daily report of changes to the DLOS system job control language and source codes that were not made by them or through its change management software. In addition, independent staff would share a daily log of production changes with configuration management who in turn would review the log and ensure that procedures were followed.

## Recommendation 13

Enable logging through ACF2 of all "Write" access to the production libraries of the DLOS system. Establish controls to ensure the logging report is reviewed on a daily basis.

**Agency Response.** The cost and systems impact of activating the ACF2 logging facility for the system production libraries was evaluated and appropriate logging identified. Implementation, including desk procedures for generation and review, tracking, reporting, and mitigation of the daily ACF2 logging report will be completed by December 31, 2006. Rural Development will then conduct an analysis to determine if the reports provide

[19] Audit Report No. 85099-4-FM, *Review of Rural Development's Information Technology Resources Security*, dated March 31, 2004.
[20] When unauthorized changes are made directly to the production libraries without going through the change management software, the baseline configuration maintained by the software has been compromised, known as a "footprint compromise," requiring the baseline to be rebuilt.

the level of detail data needed to be a useful management tool to monitor effective security controls, and will adjust the reports accordingly.

In addition, the compensating control previously implemented provides a report directly to the Deputy Chief Information Officer when there are any differences identified within the Endevor configuration management software between certification libraries. While already implemented, Rural Development is in the process of documenting the desk procedures for the review, tracking, reporting, and mitigation of the daily report.

**OIG Position.** We concur with Rural Development's management decision on this recommendation.

### Recommendation 14

Establish controls to ensure system software changes are properly authorized, tested, and documented prior to migration to the production environment.

**Agency Response.** Rural Development has implemented policies and procedures to better formalize and document the system software change control process. These steps include:

- Documenting a formal Configuration Control Board (CCB) Charter specifically outlining the duties, responsibilities, membership, change request approval process, etc., of each board. CCB Charters are sent to OCIO-CS for review and evaluation as part of the monthly OCIO-CS scorecard oversight and review process.

- Mandating the use of the specific "Request for Automation," and problem report forms as specified in Rural Development instructions. While already implemented, the Rural Development Systems Development Life Cycle guidance is being updated to strengthen these requirements.

- Requiring that the agenda and minutes for all CCB meetings be appropriately documented and distributed including a copy to ISSS for review and action. Minutes from the CCB meetings are sent to the OCIO-CS for review and evaluation as part of the monthly OCIO-CS scorecard oversight and review process.

- Restricting and limiting access to production libraries to a fewer number of staff specifically identified as requiring access to provide emergency off-hours support.

- Incorporating testing to ensure the documented policies and procedures for review, tracking, reporting, and mitigation of the daily

ACF2 and Endevor reports are working effectively into the periodic Configuration Management and Standards Compliance Branch Management Control Review.

- Requiring appropriate physical evidence of user acceptance testing of software modifications prior to implementation to the production environment.

**OIG Position.** We concur with the planned actions, but in order to reach management decision, please provide the dates of implementation.

# Scope and Methodology

We reviewed management oversight, security, and application controls over the DLOS system established by Rural Development to ensure the confidentiality, integrity, and availability of information in that system. The review was conducted at Rural Development's CSC office located in St. Louis, Missouri, one State office, and one local office. The State and county office were judgmentally selected based on the program dollars and location.

Fieldwork was performed from January through April 2006.

To accomplish our audit objectives, we performed the following audit steps and procedures:

- We reviewed policies and procedures relating to the DLOS system.
- We interviewed Rural Development officials responsible for the development, management, and data input of the DLOS system.
- We interviewed Rural Development State and field staff responsible for data authorization, completeness, and accuracy at selected State and local offices.
- We analyzed user account information in regards to accessing the DLOS system data.
- We reviewed system documentation and data records to verify the integrity of the DLOS system data.

This audit was performed in accordance with *Government Auditing Standards*.

# Exhibit A – DLOS System Application Controls Matrix



| Control Objective (Based on U.S. General Accountability Office Federal Information System Control Audit Manual) | DLOS System Control Technique(s)[21] | OIG Evaluation |
|---|---|---|
| All data are authorized before entering the application system. | • Data entered by field office technician.<br>• Field office specialist reviews data entered by technician. | • Sixty loan sample files were reviewed. Information in the files were properly input into the DLOS system.<br>• For the loan files reviewed, we determined that loan information was reviewed and approved. |
| Restrict data entry terminals to authorized users for authorized purposes. | • User IDs and passwords are required to gain access into the DLOS system and data maintained on computers.<br>• Monthly user ID verification reports are sent to validate the currency of user information and that all users have appropriate access.<br>• ACF2 is installed at USDA NITC to prevent unauthorized access to mainframe systems, files, and resources.<br>• Access to UniFi is assigned based on groups.<br>• UniFi access is limited to specific menus. | • Access to system software and hardware was not adequately limited. Of the 47 individual IDs with "Write" access to the production libraries, including source code for MortgageServ, 24 did not need the access to perform their duties.<br>• Forty-six of the 58 users had administrative access to UniFi that was not needed. Another 8 users had their access restricted.<br>• A contractor exceeded his authorized level of access by granting himself "Read," "Write," "Allocate," and "Execute" access to the DLOS system production libraries.<br>• Monthly verification lists did not include the level of access granted to each user, and field personnel did not properly review the lists to identify users who no longer required the system access assigned. |
| Master files and exception reporting help ensure all data processed are authorized. | • Master files and exception reporting is available within MortgageServ. | • MortgageServ prepared reports to detect any out-of-balance conditions, and to reconcile any reported errors. The reports were automatically produced daily when balance errors occurred. |

[21] DLOS system control techniques as reported to us by Rural Development officials. Only limited system documentation existed outlining the controls established.

| | | |
|---|---|---|
| All authorized transactions (data) are entered into and processed by the computer. | • File headers and transmitting reports ensure all transactions are processed by the computer. | • File header labels were used. Transaction Set 203, Outbound Transmission identified Header label information contained in different types of files. In addition, a Posting File Transmit report provides a control report explaining errors identified during production runs when header and trailer record labels do not match. |
| Reconciliations are performed to verify data completeness. | • Daily reconciliation and data integrity routines used by the system include a variety of reports verified by servicing offices at the start of each business day and data edit checks of online data entry screens and batch programs. | • The Posting File Transmit file documents, by batch number, whether the detail records for each batch equaled the totals in the trailer record for that batch (number of accounts and total dollars.)<br>• A loan origination interface file was passed nightly from UniFi to the Servicing System. The file contained records for both new and changed loans, which tracked out-of-sync account information for loans receiving appropriated funds.<br>• The Daily Processing Summary Balancing Error Report was divided into five separate sections that showed balancing, cross foot, and missing transaction errors. |
| Data entry design features contribute to data accuracy. | • UniFi screens were user-friendly. | • Although the terminal screens guide data, had unique identifiers, and prompted the terminal operator for next data to be entered, the source documentation and data entry screens were not adequately designed to minimize errors. The borrowers' data that had been input was not brought forward as the technician moved through the various screens.<br>• The terminal screens were not in order of data input. The same screens must be revisited for additional input.<br>• Computer terminal screens do not use key verification. Rural Development had controls in place where data is checked and verified multiple times by staff. |

| | | |
|---|---|---|
| Data validation and editing are performed to identify erroneous data. | • DLOS system data fields programmed to accept certain values. | • The mortgage account number included a self-check digit, which must be supplied as a part of the account number on each screen.<br>• Each night the system reviews the transaction log's balance after posting to the master file's balance for Principal, Escrow, and Unapplied Funds Balances. If a discrepancy was noted, an error message was generated.<br>• Online DLOS system documentation included information on the Payment and Interest Payment Calculation.<br>• Over-riding or bypassing data validation and editing was restricted. |
| Erroneous data are captured, reported, investigated, and corrected. | • Reconciliation reports are produced. | • Reconciliation procedures existed to review and correct erroneous data.<br>• Various spreadsheets existed to capture, report, and correct out-of-balance conditions. |
| Review of output reports helps maintain data accuracy and validity. | • Various reports produced by the DLOS system help maintain data accuracy and validity. | • State office personnel used Brio reports and spreadsheets to track loan data because the system did not provide adequate reports for verifying certain data.<br><br>Inter-office spreadsheets of amount funded, the balance, and amounts broken out in very low, low, 504 loans, 504 grants, and new allocations were kept at the local office we visited. |

USDA Rural Development

**United States Department of Agriculture**
**Rural Development**

NOV 30 2006

SUBJECT: Office of Inspector General Report 85501-1-FM

TO: John Dunsmuir
Acting Director, Financial Management Division

THROUGH: Sherie Hinton Henry Sherie Hinton Henry 11/30/06
Deputy Administrator
for Operations and Management

Following are our comments concerning the recommendations in the official draft of Office of Inspector General (OIG) Report 85501-1-FM, Security and Application Controls – Rural Development's Dedicated Loan Origination and Servicing System (DLOS).

Recommendation 1

Revise the DLOS system risk assessment to accurately describe controls and sites tested and adequately addresses threat and impact analyses.

**Comments**

Rural Development's Information Systems Security Staff (ISSS) utilized the United States Department of Agriculture (USDA) Office of the Chief Information Officer (OCIO) mandated ASSERT automated tool to document compliance with security controls, to identify vulnerabilities, and to build remediation plans for the Consumer system. In addition, Rural Development recently performed the annual detailed risk assessment which addresses threat identification and impact analysis. Risks identified are tracked and reported via the ASSERT reporting tool.


1400 Independence Ave, S.W. • Washington, DC 20250-0700
Web: http://www.rurdev.usda.gov


Committed to the future of rural communities.



received 12/1/06 Del

The recommendation does not state that controls were not present, just that they were not documented sufficiently in the risk assessment. The Consumer risk assessment, a living document, was updated in August 2006 and is available for review upon request.

Rural Development does not believe this is material since the conditions noted do not result in more than a remote likelihood of a material misstatement of the financial statements or other significant financial reports.

This recommendation should be closed.

Recommendation 2

Ensure that the DLOS system security plan accurately references Information Technology Service (ITS) and National Information Technology Center (NITC) documents, and that adequate documentation is maintained to verify that all controls in the security plan were implemented.

**Comments**

Rural Development received updated draft certification and accreditation (C&A) condensed guidance and templates dated October 2006 from the Office of the Chief Information Officer–Cyber Security (OCIO-CS). Subsequent updated draft guidance and templates was received in November 2006 from OCIO-CS. OCIO-CS continues to modify its guidance and templates and will distribute new versions to the agencies as the drafts are approved for release. The draft documents state that the guidance is the result of a review of the USDA C&A policy and guidance to bring it closer to standardized National Institute of Standards and Technology (NIST) guidance and Office of Management and Budget recommendations. A goal of the new C&A strategy is to standardize the base C&A process with NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems, and clearly distinguish where additional USDA processes, oversight, concurrency, or demands are required. Increased efficiency, enhanced clarification of expectations, and reduced investments of cost and time are the intended results. As always, Rural Development will ensure that the C&A is accomplished in compliance with existing Federal and Departmental guidance. The security controls are tested and vulnerabilities tracked in the OCIO-CS mandated ASSERT tool and the security test and evaluation process.

Rural Development, NITC, and ITS are in the process of revising Systems Security Plans (SSP) to comply with the updated draft OCIO-CS C&A guidance and templates. The OCIO-CS revised policy requires a concurrency review by OCIO-CS after security certification, but before accreditation takes place. This concurrency review provides an additional and independent level of review to help ensure that Departmental and NIST guidelines are followed. Rural Development will validate NITC and ITS SSP references prior to forwarding C&A documentation to the designated accrediting authority.

The SSP is a living document and is being constantly updated to reflect the most recent data available.

Rural Development does not believe this is material since the conditions noted do not result in more than a remote likelihood of a material misstatement of the financial statements or other significant financial reports.

This recommendation should be closed.

Recommendation 3

Provide ITS with appropriate system software and documentation to restore the DLOS system, and eliminate inconsistencies between the ITS and DLOS system Disaster Recovery Plans (DRP).

**Comments**

This recommendation is related to Recommendation 4 and is addressed in this joint assessment.

These recommendations indicate that OIG does not recognize the two major system components of the Consumer system and the different degree of risk associated with these two components which result in them having different disaster recovery criteria. The DLOS system has a mainframe component (MortgageServ) and a web-based component (UniFi). The mainframe component is used to service all consumer loans and provides all supporting detail for amounts reported for these loan programs in the financial reports. The web-based component supports only the loan application process for these loan programs and does not contain any financial information. Therefore, the criticality for restoring these systems in a disaster recovery scenario is different. Further supporting this differentiation in criticality is the fact that the mainframe component has the capability to collect data on loan applications in the event the web-based component is disabled. In terms of business continuity and the need to recover critical systems, the web-based component recovery timeframe is longer than the mainframe component timeframe. This is by design to minimize the significant cost of maintaining redundant hardware in a separate location to support the recovery of the less critical web-based component.

The recovery of the Consumer system mainframe component is tested twice each year as part of the NITC disaster recovery exercise. The mainframe component has been successfully restored to the NITC hot-site multiple times. Following the completion of each disaster recovery exercise, an assessment is made as to the success of the test and any problems or issues that surfaced during the test are evaluated and corrective actions are taken prior to the next test. This is an ongoing process and the disaster recovery plan is continually being updated to incorporate any enhancements needed as identified through these tests.

Rural Development does not agree with these two recommendations as stated nor do we agree there are any material weaknesses in our existing disaster recovery strategy and plan for the Consumer's system. OIG has not indicated that they found we are unable to recover the critical financial component of the Consumer system. The update of the disaster recovery plan is an ongoing process and it continues to improve with each test conducted.

However, Rural Development is tracking and managing a reported vulnerability with the ASSERT tool regarding providing ITS with current updated UniFi documentation. This documentation will be provided to ITS by January 31, 2007. The Consumer disaster recovery plan will be updated and provided to ITS by the end of the second quarter of Fiscal Year 2007. ITS's recovery time objectives are not current with those identified by the Agency. ITS has committed to updating their DRP documentation and bringing it into agreement with Rural Development's by March 31, 2007.

Rural Development can find no guidance in Federal or Department publications that identifies a specific number of personnel required to recover software applications in a declared disaster. Rural Development believes it has exercised good judgment in identifying the appropriate personnel sufficient to recover the Consumer system.

Recommendations 3 and 4 should be closed.

Recommendation 4

Revise the DLOS system DRP to assign sufficient personnel to recovery teams and present recovery procedures in a straightforward step-by-step style.

**Comments**

See the comments for Recommendation 3.

Recommendation 5

Perform a C&A which fulfills the requirements of full system accreditation by establishing effective configuration management and continuous control monitoring. Additionally, ensure that the C&A includes adequate Security Testing and Evaluation testing and appropriate supporting documentation.

**Comments**

Rural Development has documented responses to specific C&A related recommendations outlined in OIG's report, specifically relative to Risk Assessments, SSP's, DRP's, Interconnection Security Agreement, logical access controls, etc. At the time the OIG report was received, and subsequently, Rural Development requested additional details from OIG relative to non-fulfillment of C&A requirements. When additional details are provided, Rural Development will address them.

In the interim, Rural Development received updated draft C&A condensed guidance and templates dated October 2006 from OCIO-CS. Subsequent updated draft guidance and templates was received in November 2006 from OCIO-CS. OCIO-CS continues to modify its guidance and templates and will distribute new versions to the agencies as the drafts are approved for release. Configuration management, continuous control monitoring, security test and evaluation and appropriate supporting documentation are included in the OCIO-CS guidance. The OCIO revised policy requires a concurrency review by OCIO-CS after security certification, but before accreditation takes place. This concurrency review provides an additional and independent level of review to help ensure that Departmental and NIST guidelines are followed.

See the comments for Recommendation 13 for additional details specific to configuration management and continuous control monitoring.

This recommendation should be closed.

Recommendation 6

Establish agreements with all systems connecting with the DLOS system, NITC, and ITS general support systems that include rules of behavior and controls that must be maintained by the interconnecting systems.

**Comments**

NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, sets forth guidelines for planning, establishing, maintaining, and terminating interconnections between information technology systems that are owned and operated by different organizations. Rural Development believes that all interconnections between systems maintained by the Agency and support systems maintained by different organizations are adequately secured and meet the requirements for encryption of data and for establishing the connections between systems. We recognize that not all interconnections are documented by a written agreement and we are working on establishing these agreements. Draft revised guidelines and templates for establishing these agreements were recently received from OCIO-CS. OCIO-CS continues to modify their C&A guidance and templates.

As the Consumer system is re-certified, Rural Development will ensure compliance with all Federal and Departmental regulations relative to interconnecting systems. Recertification is scheduled to be completed by June 30, 2007.

Rural Development believes that all interconnections have been securely established and do not represent a vulnerability to the Agency. We do not concur that the absence of a documented agreement represents a material weakness.

This recommendation should be closed.

Recommendation 7

Remove all inappropriate "Write" accesses to the DLOS system production libraries that were identified by the audit. Establish controls to ensure excessive permissions are not reassigned.

**Comments**

Rural Development removed "Write" access to the Consumer system production libraries for all development personnel identified during the audit and during subsequent reviews. Physical evidence is available for review upon request.

Rural Development is developing documentation advising the user community of the revised procedures/controls requiring Information Technology Program Manager approval prior to granting Access Control Facility 2 (ACF2) access. The documentation is scheduled to be issued by January 31, 2007.

In addition, Consumer production library access will be included in the quarterly verification report and procedures by April 30, 2007. The reports will be issued to the system owners to verify and sign the certification attesting to the accuracy and need for the access commensurate with employee job responsibilities.

Recommendation 8

Ensure the dataset that contained NITC ID's and passwords used for submitting batch FTP jobs is renamed and that access to this dataset is appropriately limited.

**Comments**

Request for Automation (RFA) CS-9193 was initiated and approved through the Consumer Configuration Control Board (CCB) to modify the file name for .
RFA CS-9193 includes modification to all jobs and procedures that reference to now utilize the data set name . Data set has very restricted access.

RFA CS-9193 has had two turnovers to date to correct this problem. Final turnover to eliminate all references to is scheduled to occur by December 31, 2006.

Physical evidence is available for review upon request.

This recommendation should be closed.

Recommendation 9

Establish controls to review administrative accesses to the UniFi webserver to ensure that access is not granted to individuals who do not need the access to perform their job responsibilities.

**Comments**

Rural Development ISSS staff requested ITS to provide the Agency with quarterly reports relevant to all software applications hosted by the ITS web farm. When received, these reports will be distributed to Agency management staff consistent with procedures currently established to ensure the continued validation of access privileges to all Agency web-based applications.

This recommendation should be closed.

Recommendation 10

Establish controls to ensure staff and contractors do not exceed assigned levels of authority by modifying dataset rules to elevate privileges within production libraries. Ensure all testing of dataset rules is completed within the test libraries.

**Comments**

Rural Development ISSS management has re-emphasized the policy applicable to contractors with authority and responsibility to grant access privileges to Agency personnel and especially in the granting of access privileges to themselves. ISSS established controls to test any changes to data set rules prior to deployment to production. ISSS desk procedures have been updated to reinforce this policy and are available for review upon request.

Other actions that support resolution of this recommendation includes the recent re-compete of the ISSS support contract which resulted in the award of this contract to a new commercial vendor. In addition, recent hiring control authority approval has allowed Rural Development to increase the staffing in ISSS to provide the capability for more day-to-day monitoring and management of contractor support staff.

This recommendation should be closed.

Recommendation 11

Modify verification reports to include the identification of authorities associated with all production libraries.

**Comments**

See the comments for Recommendation 7.

Recommendation 12

Document and implement access profiles based on job responsibilities and separation of duties principles.

**Comments**

A joint Information Resources Management and Centralized Servicing Center initiative was completed in March 2006 to create and implement role-based templates to be used to establish the appropriate access authority for each teller identification (ID) within the Centralized Servicing Center based on Branch, Section, Unit, Position, and Template Number. The instructions for completing the automated Log Book form for National Office program staff and for Centralized Servicing Center employees currently instructs staff to specify the template number when requesting changes to a teller ID or when establishing a new teller ID.

The automated Log Book form used by field office staff has been modified to distinguish between roles that require obligation authority within MortgageServ and those that do not require obligation authority.

In addition, ISSS updated desk procedures over a year ago to cease copying access privileges from one user to another by not allowing the requesting Agency official to request ISSS to provide an employee with the same authorities given to a current employee. Forms and desk procedures were updated throughout the year to fully document and support the cessation of this procedure, but the practice itself was stopped over a year ago. Managers must now specify exact MortgageServ access authorities requested for individual MortgageServ users.

Physical evidence is available for review upon request.

This recommendation should be closed.

Recommendation 13

Enable logging through ACF2 of all "Write" access to the production libraries of the DLOS system. Establish controls to ensure the logging report is reviewed on a daily basis.

**Comments**

This recommendation is related to Recommendation 14 and is addressed in this joint assessment.

The cost and systems impact of activating the ACF2 logging facility for the Consumer system production libraries was evaluated and appropriate logging identified. Implementation, including desk procedures for generation and review, tracking, reporting, and mitigation of the daily ACF2 logging report will be completed by December 31, 2006. Rural Development will then conduct an analysis to determine if the reports provide the level of detail data needed to be a useful management tool to monitor effective security controls, and will adjust the reports accordingly.

In addition, the compensating control previously implemented provides a report directly to the Deputy Chief Information Officer when there are any differences identified within the Endevor configuration management software between certification libraries. While already implemented, Rural Development is in the process of documenting the desk procedures for the review, tracking, reporting, and mitigation of the daily report.

Rural Development has implemented policies and procedures to better formalize and document the system software change control process. These steps include:

--Documenting a formal CCB Charter specifically outlining the duties, responsibilities, membership, change request approval process, etc., of each board. CCB Charters are sent to OCIO-CS for review and evaluation as part of the monthly OCIO-CS scorecard oversight and review process.

--Mandating the use of the specific RFA and Problem Report forms as specified in Rural Development instructions. While already implemented, the Rural Development Systems Development Life Cycle guidance is being updated to strengthen these requirements.

--Requiring that the agenda and minutes for all CCB meetings be appropriately documented and distributed including a copy to ISSS for review and any necessary action. Minutes from the CCB meetings are sent to the OCIO-CS for review and evaluation as part of the monthly OCIO-CS scorecard oversight and review process.

--Restricting and limiting access to production libraries to a fewer number of staff specifically identified as requiring access to provide emergency off-hours support.

--Incorporating testing to ensure the documented policies and procedures for review, tracking, reporting, and mitigation of the daily ACF2 and Endevor reports are working effectively into the periodic Configuration Management and Standards Compliance Branch (CMSCB) Management Control Review (MCR). The next CMSCB MCR is scheduled for 2008.

--Requiring appropriate physical evidence of user acceptance testing of software modifications prior to implementation to the production environment.

Physical evidence is available for review upon request.

This recommendation should be closed.

Recommendation 14

Establish controls to ensure system software changes are properly authorized, tested, and documented prior to migration to the production environment.

**Comments**

See the comments for Recommendation 13.

This recommendation should be closed.

If you have any questions, please contact Bill Morff at 314-335-8847.

DALE ALLING
Acting Chief Information Officer

F:\Common\AFD\Jewel's Folder\85501-01-FM\8550101FM OD DLOS 1-30-07.doc

Auth_____DD_____DAIG_____AIG_____